Jacqueline Sievers

Dr. iur., LL.M., Rechtsanwältin, CIPP/E
Walder Wyss AG, Zürich
www.walderwyss.com

David Vasella

Dr. iur., Rechtsanwalt, CIPP/E
Walder Wyss AG, Zürich
www.walderwyss.com

Datenschutzrecht

Bedeutung der DSGVO für die Treuhandbranche

Europaweit wird das Datenschutzrecht an veränderte Rahmenbedingungen angepasst. Am 25. Mai 2018 bzw. am 1. Juli 2018 ist die Datenschutzgrundverordnung (DSGVO) in der EU bzw. im EWR in Kraft getreten, welche auch Auswirkungen auf Schweizer Unternehmen haben kann. Die Autoren gehen in diesem Beitrag auf die Anwendbarkeit der DSGVO für Treuhänderinnen und Treuhänder sowie deren Kunden in der Schweiz ein und stellen die daraus entstehenden Pflichten und die organisatorischen Anforderungen dar.

Wer Personendaten bearbeitet, hatte schon lange[1] eine Reihe datenschutzrechtlicher Grundsätze einzuhalten, u.a. die folgenden:[2]

- Rechtmässigkeit (Art. 4 Abs. 1 DSG)
- Bearbeitung nach Treu und Glauben (Art. 4 Abs. 2 DSG)
- Verhältnismässigkeit (Art. 4 Abs. 2 DSG)
- Erkennbarkeit und Zweckbindung (Art. 4 Abs. 3 und 4 DSG)
- Datenrichtigkeit (Art. 5 DSG)
- Datensicherheit (Art. 7 DSG)
- Beschränkung der Bekanntgabe von Personendaten ins Ausland (Art. 6 DSG)

Der Datenschutz muss also keineswegs neu erfunden werden. Es ist allerdings kein Geheimnis, dass beim Datenschutz ein gewisses Vollzugsdefizit besteht oder bestand,[3] in der Schweiz ebenso wie im übrigen Europa.

Die Europäische Datenschutzgrundverordnung (DSGVO)[4] sieht daher Sanktionen vor, die «wirksam, verhältnismässig und abschreckend» sein sollen (Art. 83 Abs. 1 DSGVO), und begleitet die **materiellen Pflichten** der Datenverarbeiter mit **flankierenden Dokumentations- und Organisationspflichten** (Art. 5 Abs. 2 DSGVO, «Rechenschaftspflicht»; aber auch Bestimmungen über den Datenschutzbeauftragten, den EU-Vertreter, die Datenschutz-Folgenabschätzung, den Umgang mit Verletzungen des Schutzes von Personendaten, die Einbindung von Auftragsverarbeitern usw.). Die Schweiz tut es der DSGVO gleich und revidiert derzeit ihr Datenschutzgesetz (DSG).[5] Auch wenn sich der **Entwurf des DSG** (E-DSG) noch in der Beratung befindet,[6] darf man annehmen, dass das neue DSG der DSGVO ähnlich sehen wird, wenn auch mit Abstufungen und – so ist zu hoffen – einem wesentlich pragmatischeren Ansatz.[7]

Im Vordergrund der Debatte steht allerdings weiterhin die DSGVO, die am 25. Mai 2018 in der EU und am 20. Juli 2018 im übrigen EWR[8] in Kraft getreten ist: Hier vor allem die **extraterritoriale Anwendung** der DSGVO[9] und die dadurch ausgelösten – und von der Beratungsindustrie genährten – Ängste, vor allem vor hohen Bussen (die bei Unternehmen ohne Niederlassung im EWR allerdings übertrieben sind), vor Abmahnungen aus Deutschland (wobei nur wenige Abmahnungen wegen Verletzungen der DSGVO bekannt sind und offen ist, ob sie überhaupt abmahnfähig sind)[10] und vor dem bürokratischen Aufwand bei der Umsetzung der DSGVO. Vor diesem Hintergrund fragt sich zunächst, ob bzw. wann die DSGVO auf Treuhänderinnen und Treuhänder der Schweiz und auf ihre Kunden anwendbar ist.

1. Ist die DSGVO auf schweizerische Treuhänder und ihre Kunden anwendbar?

1.1 Allgemeines

Dass Treuhänder in den sachlichen Anwendungsbereich der DSGVO fallen, liegt auf der Hand. Sie bearbeiten Informationen, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen, und damit Personendaten (Art. 4 Nr. 1 und 2 DSGVO). Dasselbe gilt für ihre Kunden. Weniger klar ist die Frage, unter welchen Umständen der räumliche Anwendungsbereich der DSGVO eröffnet ist. Hier ist zwischen zwei Konstellationen zu unterscheiden:

- Wenn sich ein **Gericht oder eine Behörde im EWR** mit dieser Frage beschäftigt, ist Art. 3 DSGVO anwendbar (dazu Punkt 1.2 ff.), der die räumliche Anwendbarkeit der DSGVO regelt. Ebenfalls anwendbar sind die kollisionsrechtlichen Bestimmungen des lokalen Rechts im Gerichtsstaat, die den räumlichen Anwendungsbereich des Umsetzungsrechts bestimmen (also beispielsweise darüber entscheiden, welches nationale materielle Recht die Beschränkungen der Rechte und Pflichten aus Art. 12 ff. DSGVO gestützt auf Art. 23 DSGVO regelt).[11]
- Wenn ein **schweizerisches Gericht oder eine schweizerische Behörde** über die Anwen-

dung der DSGVO zu befinden hat, ist demgegenüber nicht Art. 3 DSGVO, sondern das schweizerische Kollisionsrecht anwendbar; bei aus einer angeblichen Verletzung des Datenschutzrechts abgeleiteten Ansprüchen also Art. 139 IPRG.[12] Eine direkte Berufung auf Art. 3 zur Begründung der Anwendbarkeit der DSGVO vor einem schweizerischen Gericht scheidet daher aus (auch wenn den Autoren eine erste Klage vorliegt, die Ansprüche direkt auf Art. 3 DSGVO stützen will).

Im Vordergrund steht gleichwohl Art. 3 DSGVO, weil die Risiken einer Busse als höher eingeschätzt werden als die Risiken zivilrechtlicher Ansprüche vor schweizerischen Gerichten. Art. 3 DSGVO regelt drei Fälle, in denen die DSGVO auf eine Datenbearbeitung durch eine Person oder ein Unternehmen ausserhalb des EWR Anwendung findet. Bei allen Fällen bestehen noch erhebliche Unklarheiten. Eine gewisse Klärung wird vom **Europäischen Datenschutzausschuss** erwartet, einem Gremium der Aufsichtsbehörden der Mitgliedstaaten (die frühere Artikel-29-Datenschutzgruppe), der u.a. die Aufgabe hat, auf die einheitliche Anwendung der DSGVO hinzuwirken (Art. 67 ff. DSGVO). Es ist bekannt, dass der Ausschuss am 25. September 2018 Leitlinien zu Art. 3 DSGVO zuhanden einer öffentlichen Konsultation verabschiedet hat, doch sind diese bei Drucklegung dieses Beitrags noch nicht veröffentlicht worden.

1.2 Niederlassung im EWR

Betreibt ein Unternehmen eine Niederlassung im EWR, so ist die DSGVO auf Datenbearbeitungen «im Zusammenhang» mit dieser Niederlassung anwendbar (Art. 3 Abs. 1 DSGVO). Hier sind zahlreiche Fragen offen, z.B. welche Verbindung zwischen einer Niederlassung und dem schweizerischen Unternehmen genügt, um die DSGVO auch auf Letzteres zur Anwendung zu bringen und was überhaupt eine «Niederlassung» im datenschutzrechtlichen Sinne ist. Hier soll die Feststellung genügen, dass schweizerische Unternehmen mit **Töchtern, Zweigniederlassungen und anderen dauerhaften Strukturen in einem EWR-Staat** zumindest Gefahr laufen, die DSGVO auch bei eigenen Tätigkeiten beachten zu müssen.

1.3 Angebot von Waren oder Dienstleistungen

Die DSGVO kann ihre Anwendbarkeit allerdings nicht auf Unternehmen beschränken, die im EWR niedergelassen sind. Zum Schutz betroffener Personen im EWR muss sie vielmehr auch Datenbearbeitungen ausserhalb des EWR erfassen. Art. 3 Abs. 2 lit. a DSGVO verankert vor diesem Hintergrund das aus anderen Rechtsgebieten bekannte Marktortprinzip.[13] Danach findet die DSGVO Anwendung auf Datenbearbeitungen «im Zusammenhang» mit «Angeboten» an betroffene Personen in der Union (d.h. im EWR). Richtet ein Treuhandunternehmen ein Angebot an Personen im EWR, kann die DSGVO auf entsprechende Angebote anwendbar sein.

Als «Angebot» gilt dabei jedes entgeltliche oder unentgeltliche **Angebot von Leistungen**, unabhängig davon, ob auf das Angebot ein Vertragsschluss folgt.[14] Da ausweislich des Wortlauts nur Angebote und nicht auch die Nachfrage von Leistungen erfasst ist, sollte die Datenbearbeitung im Zusammenhang mit der Rekrutierung, Anstellung und Beschäftigung von Personen im Ausland (z.B. von Grenzgängern) nicht unter die DSGVO fallen.[15] Erfasst sind sodann Angebote an Personen, die sich physisch im EWR aufhalten; auf Wohnsitz und Nationalität kommt es nicht an, auch nicht auf den gewöhnlichen Aufenthalt (vgl. Erwägungsgrund 2). Demgegenüber sind Angebote **nicht erfasst, die sich an juristische Personen richten**, da nur Menschen betroffene Personen im Sinne der DSGVO sind (Art. 4 Nr. 1 DSGVO). Das Angebot einer Mehrwertsteuervertretung in der Schweiz für ein ausländisches Unternehmen etwa fällt nicht unter Art. 3 Abs. 2 lit. a DSGVO. Es spielt allerdings keine Rolle, ob die angesprochene natürliche Person als Konsument oder gewerblich tätig ist, sodass insoweit auch B2B-Geschäft erfasst sein kann. Ein Treuhandunternehmen, das Einzelunternehmen Leistungen anbietet, kann daher durchaus unter die DSGVO fallen.

Sehr wichtig ist allerdings die folgende Einschränkung: Art. 3 Abs. 2 lit. a DSGVO erfasst nur Angebote, die sich **offensichtlich an natürliche Personen im EWR richten** (Erwägungsgrund 23; «offensichtlich beabsichtigt»). Ob dies der Fall ist, ist im Einzelfall anhand objektiver Kriterien zu bestimmen. Erwägungsgrund 23 nennt einige Indizien, und weitere ergeben sich aus der einschlägigen Rechtsprechung des EuGH.[16] Für Treuhänder ohne Niederlassung im EWR dürfte vor allem die Gestaltung der Website von Bedeutung sein. Hier deuten insbesondere folgende Indizien auf eine offensichtliche Absicht hin:

- Verwendung einer Domain eines EWR-Staats wie «.de» oder «.fr»
- Verwendung einer im EWR gesprochenen Sprache, die keine schweizerische Landessprache ist, z.B. Polnisch
- Beschreibung von Leistungen spezifisch für Personen aus dem EWR (etwa Beratungsangebote bei der Besteuerung von schweizerisch-französischen Grenzgängern oder Hinweise auf Beratungsangebote für Private gemeinsam mit einem deutschen Partner)
- Preisangaben in EUR oder anderen europäischen Währungen
- Wegbeschreibungen aus dem EWR-Ausland in die Schweiz
- Erwähnung von Kundschaft im EWR, z.B. in Testimonials
- Ausgaben z.B. für Google AdWords, damit die Webseite im Ausland gefunden wird

Nicht erfasst sind daher Zufallskunden aus dem EWR, die zwar bedient werden, aber ohne dass eine entsprechende Absicht manifest wäre – es sei denn, man werte die Tatsache des Vertragsschlusses bereits als genügendes Indiz für eine solche Absicht, was u.E. aber nicht gerechtfertigt ist.[17]

Ungeklärt ist die Situation bei **nicht aktiv akquirierten Dauerbeziehungen**, beispielsweise einer Beziehung mit einem deutschen Kunden, der auf dem Gebiet der Schweiz geworben wurde, aber in Deutschland wohnt und nach seiner Heimkehr weiter betreut wird. Hier stellt sich die Frage, wie weitere Angebote im Rahmen dieser Betreuung zu behandeln sind, z.B. bei der Verlängerung oder dem Ausbau der Kundenbeziehung. Nach unserem Dafürhalten sollten Angebote im Rahmen einer solchen bestehenden Beziehung die Anwendbarkeit der DSGVO nicht auslösen können. Solche Angebote bewegen sich im Rahmen einer bestehenden Kundenbeziehung und entfalten damit nicht die Streuwirkung, um die es Art. 3 Abs. 2 lit. a DSGVO dem Erwägungsgrund 23 zufolge geht.

Ebenfalls nicht geklärt ist die Behandlung **allgemein-internationaler Angebote** zum Beispiel auf einer Website in englischer Sprache unter einer .com-Domain. Hier kann der Betreiber der Website vorbringen, sein Angebot habe zwar internationalen Charakter, richte sich aber nicht – jedenfalls nicht «offensichtlich» – an Personen im EWR. Dieses Argument ist besonders für amerikanische Anbieter wichtig, die andernfalls stets unter die DSGVO fielen; es sollte aber schon aus Gründen der Gleichbehandlung auch für schweizerische Betreiber zugelassen werden.

Im Ergebnis ist die Rechtslage in sehr vielen Punkten unklar. Es ist daher sinnvoll, besonders die eigene Website darauf zu prüfen, ob sich Indizien für eine Ausrichtung auf Privatkunden im EWR finden und diese entweder bewusst fortzuführen – mit den entsprechenden Folgen – oder die Website entsprechend anzupassen.

1.4 «Verhaltensbeobachtung»

Die DSGVO ist ferner anwendbar auf die Beobachtung des «Verhaltens» betroffener Personen, sofern das beobachtete Verhalten im EWR erfolgt (Art. 3 Abs. 2 lit. b DSGVO). Wie Erwägungsgrund 24 zeigt, geht es dem Gesetzgeber hier um **Online-Tracking** und vergleichbare Aktivitäten. Als «Beobachtung» gilt dabei die bewusste Bearbeitung von Personendaten, die Aufschluss über das Verhalten natürlicher Personen geben, die sich während des beobachteten Verhaltens im EWR aufhalten (wobei es

auf Wohnsitz und Nationalität wiederum nicht ankommt). Erfasst ist aber nur die personenbezogene Beobachtung, was die Frage aufwirft, welche Angaben im Online-Bereich überhaupt als Personendaten gelten. Obwohl diese Frage bei IP-Adressen und ähnlichen Angaben nicht geklärt ist,[18] ist davon auszugehen, dass Gerichte und Aufsichtsbehörden solche Angaben recht unterschiedslos als Personendaten behandeln werden.[19] Im Ergebnis schränkt die Anforderung des Personenbezugs die räumliche Anwendbarkeit der DSGVO im Bereich der Verhaltensbeobachtung daher kaum ein.[20]

Ob die Beobachtung bewusst Personen im EWR erfasst, spielt sodann keine Rolle.[21] Erforderlich ist aber, dass die Beobachtung mit einer gewissen **Intensität und Dauer** betrieben wird.[22] Das folgt nicht nur aus dem üblichen Verständnis des Begriffs der «Beobachtung», sondern ergibt sich dem Sinn nach auch aus Erwägungsgrund 24. Nach unserem Dafürhalten sollte ein Treuhandunternehmen daher nicht schon deshalb unter Art. 3 Abs. 2 lit. b DSGVO fallen, weil es eine Software wie beispielsweise Google Analytics für die Messung des Besucheraufkommens einsetzt. Weiter wäre zu fragen, ob eine allfällige Verhaltensbeobachtung in diesem Beispiel wirklich dem Unternehmen zuzurechnen wäre, das die Verhaltensbeobachtung durch Einbinden von Google Analytics in Auftrag gibt, oder vielmehr nur Google als dem Unternehmen, das die Verhaltensbeobachtung durchführt.[23]

Auch hier bestehen also zahlreiche Unklarheiten. Eine weitere kommt hinzu: Fällt nur die Beobachtung von Internetaktivitäten unter die Verhaltensbeobachtung oder auch die Beobachtung von **Verhalten, das sich offline abspielt**? Das kann beispielsweise dann relevant sein, wenn im Rahmen eines Vermögensverwaltungsmandats auf Konten einer natürlichen Person zugegriffen wird und dabei Einnahmen und Ausgaben nachvollzogen werden, die im EWR ausgelöst werden. Die Literatur steht einer Anwendung im Offline-Bereich aufgrund der Einschränkung in Erwägungsgrund 24 tendenziell ablehnend gegenüber, doch ist auch dieser Punkt noch nicht geklärt.[24]

Im Ergebnis kann die DSGVO insbesondere auf Internetauftritte anwendbar sein, sobald Technologien eingesetzt werden, die das Verhalten von Besuchern erfassen, zumindest wenn dabei im konkreten Fall eine gewisse Intensität erreicht wird. Hier besteht ein – bislang aber kaum hohes – Risiko einer Abmahnung besonders aus Deutschland, etwa wenn die Website nicht über eine DSGVO-konforme Datenschutzerklärung verfügt.[25]

1.5 Weitere Fälle

Ausserhalb der genannten Konstellationen – Niederlassung; Angebotsausrichtung; Verhaltensbeobachtung – verlangt die DSGVO keine Anwendung. Das gilt auch dann, wenn ein in der Schweiz ansässiges Unternehmen Personendaten durch einen Auftragsverarbeiter im Gebiet des EWR bearbeiten lässt, z.B. durch einen deutschen Hosting-Anbieter. In diesem Fall untersteht zwar der Auftragsbearbeiter der DSGVO, weshalb er einen der DSGVO entsprechenden Auftragsvertrag vorlegen wird; der schweizerische Auftraggeber wird der DSGVO dadurch aber nicht unterstellt.[26]

Die folgenden Situationen führen daher nach unserer Einschätzung und für sich genommen **nicht zur Anwendung der DSGVO**:[27]

- die Bearbeitung von Personendaten im Zusammenhang mit einem Angebot an oder der Tätigkeit für Unternehmenskunden, auch wenn sich das Angebot ausdrücklich an ausländische Unternehmen richtet (wie z.B. bei Mehrwertsteuervertretungen)
- die Bearbeitung von Personendaten im Zusammenhang mit einem Mandat einer natürlichen Person, das ohne Ausrichtung auf den ausländischen Markt gewonnen wurde, und zwar auch dann, wenn das Mandat im Lauf der Beziehung erneuert oder ausgebaut wurde
- die Pflege eines Verzeichnisses von Adressen von Unternehmenskunden, auch wenn dabei Personendaten (z.B. Angaben von Kontaktpersonen) bearbeitet werden
- die Auslagerung von Verarbeitungstätigkeiten an einen Auftragsverarbeiter (zum Beispiel IT-Dienstleister) im EWR
- die Beschäftigung von Mitarbeitern aus dem Ausland in der Schweiz

Dagegen kann die DSGVO auf zivilrechtliche Ansprüche anwendbar sein, wenn ein schweizerisches Gericht gestützt auf Art. 139 IPRG ausländisches Recht anzuwenden hat. Das wäre vor allem dann der Fall, wenn eine Person mit gewöhnlichem Aufenthalt in einem EWR-Staat **Ansprüche gegen einen schweizerischen Bearbeiter** richtet und sich dabei auf ihr Heimatrecht beruft. In diesem Fall wäre es zwar denkbar, dass ein schweizerisches Gericht immateriellen Schadenersatz zuspricht (Art. 82 Abs. 1 DSGVO); eine Busse käme aber nicht infrage.

2. Hauptpflichten betroffener Treuhänder nach der DSGVO

Ist die DSGVO auf eine bestimmte Bearbeitungstätigkeit anwendbar, so muss die DSGVO für diese Bearbeitungstätigkeit eingehalten werden.[28] Nachfolgend werden daher die wichtigsten Anforderungen der DSGVO skizziert.

2.1 Dokumentationspflichten

Wie eingangs erwähnt, verlässt sich die DSGVO nicht auf materielle Pflichten. Die vielleicht wichtigste flankierende Pflicht ist die Dokumentation der Einhaltung des Datenschutzes (Art. 5 Abs. 2 DSGVO; «Accountability») und – damit verwandt – die Führung eines sogenannten **Verfahrensverzeichnisses** (Art. 30 DSGVO). Für den ersten Punkt empfiehlt sich zumindest in KMU die Führung eines Log-Buchs, eines zentralen Verzeichnisses datenschutzrechtlich relevanter Vorgänge (z.B. von Betroffenenanfragen mit Eingangs- und Erledigungsdatum; von Datenschutz-Folgenabschätzungen bzw. dem Verzicht auf eine solche usw.).[29] Der zweite Punkt, das Verfahrensverzeichnis, ist in Art. 30 DSGVO geregelt. Danach müssen Verantwortliche wie auch Auftragsverarbeiter Verzeichnisse ihrer Datenbearbeitungen führen (soweit diese unter die DSGVO fallen). Das Verzeichnis erfasst dabei nicht jede einzelne Datenbearbeitung (d.h. nicht jeden Kunden einzeln), sondern einzelne Kategorien von Datenbearbeitungen (z.B. den Umgang mit Kundendaten). Art. 30 Abs. 1 und 2 DSGVO gibt den Mindestinhalt der Verzeichnisse vor, und im Internet sind Muster und Beispiele zu finden.[30] Auch der Entwurf des revidierten DSG sieht eine Pflicht vor, ein Verzeichnis der Bearbeitungstätigkeiten zu führen (Art. 11 E-DSG).

Mit Dokumentationspflichten verwandt ist die Pflicht, bei Bearbeitungen mit voraussichtlich «hohen Risiken» eine **Datenschutz-Folgenabschätzung** durchzuführen (einer Art «Datenschutzverträglichkeitsprüfung») und diese ggf. der zuständigen Aufsichtsbehörde zu melden (Art. 35 und 36 DSGVO; auch hier gibt es eine Entsprechung im Entwurf des DSG, Art. 20). Wann voraussichtlich hohe Risiken vorliegen, umschreibt die DSGVO selbst nur am Rande (Art. 35 Abs. 3 DSGVO). Aufsichtsbehörden haben dazu aber Listen nach Art. 35 Abs. 4 und 5 DSGVO veröffentlicht. Bei Treuhandunternehmen dürfte eine Pflicht zur Folgenabschätzung nicht häufig sein. Eine solche Pflicht ist aber etwa bei grossen Treuhandunternehmen denkbar, die vorwiegend Einzelpersonen betreuen, und bei «Big-Data-Analysen» von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden.[31]

2.2 Organisatorische Anforderungen

Unternehmen, deren Bearbeitungstätigkeiten unter die DSGVO fallen, ohne über eine Niederlassung im EWR zu verfügen (Art. 3 Abs. 2 lit. a und b DSGVO), sind verpflichtet, im EWR einen Vertreter zu bestellen (Art. 27 DSGVO). Der sogenannte **EU-Vertreter** dient als Anlaufstelle für Aufsichtsbehörden und betroffene Personen, also eine Art Briefkasten als Ersatz für die fehlende Niederlassung. Überdies muss er eine Kopie der Verfahrensverzeichnisse vorhalten (Art. 30 Abs. 1 und 2 DSGVO), damit sich Behörden ohne den Weg über die Amtshilfe ein Bild über entsprechende Bearbeitungstätigkeiten machen können. Die Bestellung erfolgt durch

einen entsprechenden Auftrag, und der EU-Vertreter muss in Datenschutzerklärungen genannt werden (Art. 13 und 14 DSGVO, je Abs. 1 lit. a). Eine Ausnahme von der Bestellungspflicht gilt indessen dann, wenn die betreffende – d.h. unter die DSGVO fallende – Bearbeitung nur gelegentlich erfolgt, keine besonderen Kategorien von Personendaten betrifft und nicht zu relevanten Risiken für die betroffenen Personen führt (Art. 27 Abs. 2 DSGVO). Zumindest kleinere und mittelgrosse Treuhandunternehmen werden sich regelmässig auf diesen Ausnahmetatbestand berufen können, jedenfalls dann, wenn die Betreuung ausländischer Privatkunden nur einen kleineren Teil der Geschäftstätigkeit ausmacht.

Sodann verlangt die DSGVO die Benennung eines (internen oder externen) **Datenschutzbeauftragten** (Art. 37 DSGVO). Eine solche Pflicht besteht allerdings nur, wenn die «Kerntätigkeit» des Unternehmens in einer umfangreichen, regelmässigen systematischen Überwachung besteht oder in der umfangreichen Bearbeitung besonderer Personendaten, was für Treuhandunternehmen i.d.R. nicht zutreffen wird. Die Bestimmung einer für den Datenschutz zuständigen Person ist trotzdem sinnvoll, die aber nicht als «Datenschutzbeauftragter», «Data Protection Officer» o.Ä. bezeichnet werden sollte, um Verwechslungen mit der Funktion des offiziellen Datenschutzbeauftragten i.S.v. Art. 37 DSGVO zu vermeiden.[32]

2.3 Datenschutzerklärungen und AGB

Nach dem geltenden DSG müssen betroffene Personen nur dann vorab über die Bearbeitung ihrer Personendaten informiert werden, wenn sie sich nicht von selbst versteht (Art. 4 Abs. 3 DSG: «aus den Umständen ersichtlich oder gesetzlich vorgesehen») oder besonders schützenswerte Personendaten oder Persönlichkeitsprofile beschafft werden (Art. 14 DSG). Ansonsten sind betroffene Personen auf das öffentliche Register bestimmter Datensammlungen (Art. 11a DSG) und vor allem das Auskunftsrecht angewiesen (Art. 8 DSG). Die DSGVO verfolgt – wie auch das revidierte DSG, Art. 17 ff. E-DSG – einen ganz anderen Ansatz: Über jede Datenbearbeitung ist im Voraus, **umfassend und aktiv zu informieren** (Art. 12 ff. DSGVO), auch über selbstverständliche Bearbeitungen. Davon sind nur wenige Ausnahmen vorgesehen.[33] Treuhänder haben daher Kunden, Mitarbeiter und Geschäftspartner aktiv über Bearbeitungen zu informieren, die unter die DSGVO fallen. Die Informationspflicht umfasst dabei u.a. die Kontaktdaten des Unternehmens, die Zwecke und Rechtsgrundlagen der Bearbeitung (also beispielsweise die Abwicklung des Mandats, die Verwaltung von Kundendaten, Marketing usw.), die Kategorien der bearbeiteten Personendaten, die Speicherdauer der Daten, mögliche Empfänger der Personendaten im In- und Ausland und die Rechte der betroffenen Personen. Um der Informationspflicht nachzukommen, wird das verantwortliche Unternehmen eine Datenschutzerklärung bzw. Datenschutzerklärungen veröffentlichen müssen, z.B. auf seiner Website, ggf. aber auch als Ergänzung zu allgemeinen Geschäftsbedingungen. Eine entsprechende Pflicht – aber mit geringerem Umfang – wird sich auch aus dem revidierten DSG ergeben.

Nach der DSGVO dürfen Personendaten ferner nur bearbeitet werden, wenn dafür ein **Erlaubnistatbestand** greift; andernfalls ist die Bearbeitung verboten (Art. 5 Abs. 1 lit. a, Art. 6 und Art. 9 DSGVO).[34] Die Bearbeitung von Personendaten für Mandanten stützt sich dabei in erster Linie auf die Rechtsgrundlage der Vertragsanbahnung bzw. -abwicklung (Art. 6 Abs. 1 lit. b DSGVO). Sofern dabei auch besondere Kategorien von Personendaten i.S.v. Art. 9 Abs. 1 DSGVO bearbeitet werden, z.B. Gesundheitsdaten, ist jedoch eine andere Rechtsgrundlage erforderlich. Hier wird eine ausdrückliche **Einwilligung** nötig sein, die i.d.R. aber über (ausdrücklich akzeptierte) AGB eingeholt werden kann.[35] Die Gestaltung einer rechtssicheren Einwilligungserklärung ist allerdings eine anspruchsvolle Aufgabe. Einwilligungen sind in den meisten Fällen auch für den Versand elektronischer Werbung erforderlich; allerdings weniger aufgrund der DSGVO als vielmehr nach Art. 3 Abs. 1 lit. o UWG bzw. (beim Versand an Personen im Ausland) nach dem anwendbaren lokalen Marktverhaltensrecht,[36] bis dieses in der EU bzw. im EWR durch die e-Privacy-Verordnung abgelöst wird. – Einwilligungen können jederzeit widerrufen werden (z.B. die Einwilligung zum Erhalt eines Newsletters). Es muss daher dokumentiert werden, für welche Bearbeitungstätigkeiten eine Einwilligung vorliegt und für welche sie widerrufen wurde.[37]

2.4 Einhaltung von Betroffenenrechten

Da das Datenschutzrecht die Bestimmung der betroffenen Personen über ihre Personendaten sicherstellen will, haben betroffene Personen bestimmte Rechte im Zusammenhang mit der Bearbeitung ihrer Daten (sogenannte Betroffenenrechte). Diese Rechte lassen sich kategorisieren in Rechte zur Sicherstellung der Transparenz (die Rechte auf Information, auf eine Kopie der Personendaten und ergänzende Angaben nach Art. 15 DSGVO und auf Gehör bei automatisierten Einzelentscheidungen, auf die hier nicht weiter eingegangen wird), zur Sicherstellung der Datenintegrität (das Recht auf Berichtigung und Vervollständigung nach Art. 16), zur Begrenzung der Datenverarbeitung (die Rechte auf Löschung nach Art. 17, auf Einschränkung der Verarbeitung nach Art. 18 und auf Widerspruch nach Art. 21) und das Recht auf Datenübertragbarkeit (Art. 20).

Das ist im Grundsatz nicht neu; auch das DSG gewährt eine Reihe von Betroffenenrechten (z.B. das Auskunftsrecht nach Art. 8 DSG; allerdings weniger umfassend als nun die DSGVO). Der Umgang mit Betroffenenrechten nach der DSGVO ist dennoch anspruchsvoll. Zum einen ist der Inhalt der Betroffenenrechte nicht immer klar und in vielen Details strittig. Zum anderen sind auch prozessbezogene Fragen offen, z.B. die **korrekte Identifikation** der Betroffenen. Dennoch sind Begehren grundsätzlich in einer Frist von **dreissig Tagen** zu behandeln (Art. 12 Abs. 3 DSGVO). Zumindest bei grösseren Unternehmen empfiehlt sich daher, entsprechende interne Abläufe vorzusehen oder anzupassen. Immerhin hat sich die Zahl der Anfragen in den meisten Unternehmen bisher nicht wesentlich erhöht.

2.5 Löschung von Daten

Wie bereits das geltende DSG verlangt auch die DSGVO, dass Personendaten gelöscht werden, wenn sie nicht mehr benötigt werden und keine Aufbewahrungspflicht besteht. Die Umsetzung dieser Pflicht ist allerdings keine einfache Aufgabe. Zunächst muss ein Unternehmen Übersicht über die von ihm bearbeiteten Personendaten und die entsprechenden Datenflüsse gewinnen, wobei Verfahrensverzeichnisse helfen können. Sodann ist jeder Kategorie von Personendaten eine Aufbewahrungsdauer zuzuweisen, die sich z.B. aus gesetzlichen Aufbewahrungspflichten ableitet. Anschliessend – und das ist der anspruchsvollste Teil – ist sicherzustellen, dass die Aufbewahrungsfristen, soweit möglich, eingehalten und Daten rechtzeitig aus produktiven Systemen archiviert werden, durch technische Massnahmen und Anweisungen an die Mitarbeiter.[38]

2.6 Auslagerungen von Datenbearbeitungen

Die Auslagerung von Datenbearbeitungen ist häufig und im Grundsatz unproblematisch. Die DSGVO privilegiert die Auslagerung im Verhältnis zu Bekanntgaben an andere Dritte, indem sie dafür keine besondere Rechtsgrundlage verlangt. Die Auslagerung ist daher grundsätzlich dann zulässig, wenn es auch die ausgelagerte Bearbeitung ist, unter Vorbehalt gesetzlicher oder vertraglicher Auslagerungsverbote. Bedingung dieser Privilegierung ist allerdings der **Abschluss einer Vereinbarung mit dem Auftragsverarbeiter**, der diesen der Kontrolle des Verantwortlichen unterstellt. Art. 28 Abs. 3 DSGVO gibt daher Mindestinhalte einer solchen Vereinbarung vor.[39] Soweit ein Treuhandunternehmen unter die DSGVO fällt und relevante (unter die DSGVO fallende) Bearbeitungen an einen Auftragsverarbeiter in der Schweiz oder im Ausland

auslagert, ist es deshalb verpflichtet, eine entsprechende Vereinbarung zu treffen.[40] Umgekehrt sind Auftragsverarbeiter mit einer Niederlassung im EWR ihrerseits verpflichtet, eine solche Vereinbarung zu schliessen, weshalb grössere Anbieter ihre AGB häufig bereits angepasst haben.

Befindet sich der Auftragsbearbeiter im Ausland, sind zudem die Anforderungen an die **Übermittlung von Personendaten ins Ausland** einzuhalten. Fehlt im Empfängerstaat ein angemessenes Datenschutzniveau, was etwa für die USA, Indien und China zutrifft, ist die Übermittlung häufig nur nach Abschluss eines ausreichenden Datenübermittlungsvertrags zulässig.[41] Bei Übermittlungen in die USA besteht sodann die Möglichkeit, dass sich der Empfänger dem sogenannten Privacy Shield unterstellt hat, einem Programm zur Sicherstellung eines angemessenen Datenschutzes; in diesem Fall besteht für den betreffenden Empfänger für die von der Zertifizierung gedeckten Übermittlungen ein angemessenes Schutzniveau.[42]

2.7 Datensicherheit

Wie nach schweizerischem DSG sind Personendaten auch nach der DSGVO angemessen vor Risiken – insbesondere vor unberechtigtem Zugriff, Verlust und Zerstörung – zu schützen (Art. 5 Abs. 1 lit. f, Art. 24 und Art. 32 DSGVO). Dafür sind angemessene Massnahmen technischer und organisatorischer Natur zu treffen (z.B. durch eine Beschränkung des Datenzugriffs bzw. des Zugangs zu Räumen etwa durch ein Badge-System, durch Verschlüsselung von Laptops, durch Weisungen usw.). Ebenfalls der Datensicherheit dient die Pflicht, Verletzungen des Datenschutzes in einer Frist von 72 Stunden der zuständigen Aufsichtsbehörde und u.U. auch den betroffenen Personen mitzuteilen (Art. 33 f. DSGVO; sog. «Breach Notification»). Das geltende schweizerische Datenschutzrecht kennt eine solche Pflicht bisher nicht, zumindest nicht ausdrücklich. Das revidierte DSG wird aber ebenfalls eine Breach Notification vorsehen (Art. 22 E-DSG).

3. Folgerungen

Treuhandunternehmen in der Schweiz müssen sich wie die meisten Unternehmen mit der Frage auseinandersetzen, ob sie die DSGVO umsetzen müssen oder wollen. Diese Frage steht aber im Kontext der Revision des DSG, denn viele Anforderungen der DSGVO werden sich auch im revidierten DSG finden. Vor diesem Hintergrund dient eine Umsetzung der DSGVO auch der Vorbereitung auf das revidierte DSG. Viele Unternehmen, deren Tätigkeit sich auf die Schweiz konzentriert, die eine Umsetzung der DSGVO aber dennoch nicht ausschliessen können, haben sich daher für eine moderate Umsetzung entschieden: Die DSGVO ist Leitschnur der Datenschutzcompliance, aber ohne dass das Unternehmen ausdrücklich auf die DSGVO verweist, und die Umsetzung folgt einem pragmatischen Ansatz (der bei jeder Umsetzung der DSGVO notwendig ist) und verzichtet auf unnötigen Druck. Diese Form der Umsetzung mit Augenmass bewährt sich nach der Erfahrung der Autoren.

Im Ergebnis dürfte ein **Vorgehen etwa wie folgt** für viele Treuhandunternehmen infrage kommen – nicht abschliessend, nicht unbedingt in dieser Reihenfolge und ggf. auch parallel:

- Bestimmung einer Person, die für den Datenschutz zuständig ist; bei Bedarf Sicherstellung externer Unterstützung
- Erfassung der im Unternehmen bearbeiteten Personendaten und Datenbearbeitungsprozesse (Verfahrensverzeichnisse)
- Prüfung des Online-Auftritts in inhaltlicher und technischer Hinsicht
- ggf. Bestellung eines EU-Vertreters
- Ausarbeitung von Datenschutzerklärungen und Prüfung und allenfalls Anpassung von AGB und Vertragsunterlagen
- Prüfung von Verträgen mit Dienstleistern
- Prüfung interner Abläufe beispielsweise in den Bereichen Personal, Marketing und Umfang mit Mandatsdaten
- Prüfung der Aufbewahrungsdauer von Personendaten und ggf. Anstoss für die Ausarbeitung eines Löschkonzepts ■

1 Das geltende schweizerische Datenschutzgesetz trat am 1. Juli 1993 in Kraft.

2 Je nach Darstellung liesse sich diese Liste ergänzen um das Verbot der Drittweitergabe besonderer Personendaten (Art. 12 Abs. 2 lit. c DSG) und die Freiheit der Bearbeitung veröffentlichter Personendaten (Art. 12 Abs. 3 DSG).

3 Vgl. dazu den Bericht des Bundesrates über die Evaluation des Bundesgesetzes über den Datenschutz vom 9. Dezember 2011, BBl 2012 335 («[…] kommt es selten vor, dass betroffene Personen den Rechtsweg beschreiten, […] Anwendungen neuer Technologien sind praktisch nie Gegenstand gerichtlicher Auseinandersetzungen»).

4 Verordnung (EU) 2016/679 vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG; sie löste die Datenschutz-Richtlinie ab (Richtlinie 95/46/EG vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr).

5 Die Revision dient nicht nur der Angleichung an die DSGVO, sondern auch der Umsetzung der revidierten Europaratskonvention Nr. 108; vgl. dazu die Botschaft vom 15. September 2017, BBl 2017, 6962 ff. Zur Revision vgl. z.B. David Rosenthal, Der Entwurf für ein neues Datenschutzgesetz, Jusletter vom 27. November 2017; Jacqueline Sievers / David Vasella, Der «Swiss Finish» im Vorentwurf des DSG, digma 2017, 44 ff.

6 Der Nationalrat wird in der Wintersession 2018 als Erstrat darüber beraten.

7 Derzeit ist beispielsweise nicht vorgesehen, in der Schweiz ein Recht auf Datenportabilität einzuführen, wie es in der DSGVO in Art. 20 verankert ist. Nach unserem Dafürhalten sollte auf ein solches Recht verzichtet werden.

[8] Der Europäische Wirtschaftsraum (EWR) umfasst die EU, ihre Mitgliedstaaten und das Fürstentum Liechtenstein, Island und Norwegen.

[9] Dieser Ausdruck wird hier verwendet, weil er sich eingebürgert hat; tatsächlich geht es aber weniger um die Extraterritorialität als vielmehr darum, unter welchen Umständen eine Datenverarbeitung als intraterritorial betrachtet werden kann.

[10] Es gibt dazu widersprechende deutsche Urteile.

[11] Die Umsetzungsgesetze enthalten i.d.R. eigene kollisionsrechtliche Bestimmungen, auch wenn sie diese Frage den vorbestehenden kollisionsrechtlichen Regeln überlassen könnten; vgl. beispielsweise § 1 Abs. 4 des deutschen Bundesdatenschutzgesetzes (BDSG) (wonach das BDSG bereits dann Anwendung finden kann, wenn eine Datenbearbeitung in Deutschland stattfindet; diesen Ansatz verfolgt auch das noch nicht verabschiedete revidierte DSG Liechtensteins) oder Art. 5-1 Abs. 1 des französischen Loi n° 78-17 relative à l'informatique, aux fichiers et aux libertés (wonach das französische Umsetzungsrecht zum Schutz der betroffenen Personen und der nationalen Souveränität stets Anwendung findet, wenn die betroffene Person in Frankreich Wohnsitz hat). Vgl. zum Ganzen auch die Überlegungen in der französischen Étude d'impact – Projet de Loi relatif à la protection des données personnelles, 12. Dezember 2017, 71 ff.

[12] Vgl. dazu das (letztinstanzlich in BGE 138 II 346 vom Bundesgericht beurteilte) Urteil des Bundesverwaltungsgerichts A-7040/2009 vom 30. März 2011 i.S. Google Streetview, E. 5. Im Bereich des öffentlichen Rechts gilt das Territorialitätsprinzip; dazu finden sich ebenfalls Hinweise im erwähnten Urteil des Bundesverwaltungsgerichts.

[13] Dazu Klar, in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung/BDSG, 2. Aufl. 2018, Art. 3 N 6 ff.

[14] Piltz, in: Gola (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 3 N 28.

[15] Ausnahmen sind denkbar, z.B. beim Angebot von Relocation-Leistungen.

[16] Etwa im Urteil des EuGH vom 7. Dezember 2010 – Alpenhof, Rs. C-585/08 und C-144/09, Rz. 81 und 83.

[17] A.A. Plath, in: Plath (Hrsg.), DSGVO – BDSG, 3. Aufl. 2018, Art. 3 DSGVO N 23 (Vertragsschluss genügt).

[18] Dazu Kühling/Buchner-Klar, Art. 4 Nr. 1 N 25 ff.

[19] Dabei werden sie sich auf den Wortlaut von Art. 4 Nr. 1 DSGVO berufen, auch wenn er diesen Schluss nicht eindeutig vorgibt: «[…] als identifizierbar wird eine natürliche Person angesehen, die […] insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder […] identifiziert werden kann.»

[20] Anbieter von Tracking-Software verlangen denn auch häufiger, dass ihr Kunde in seiner Datenschutzerklärung auf den Einsatz der Software hinweist.

[21] Kühling/Buchner-Klar, Art. 3 N 101.

[22] Kühling/Buchner-Klar, Art. 3 N 94 f.; Zerdick, in: Ehmann/Selmayr (Hrsg.), DS-GVO, 2. Aufl. 2018, Art. 3 N 20.

[23] Fiele in einer solchen Konstellation stets (auch) der Verantwortliche und nicht (nur) der Auftragsverarbeiter unter die DSGVO, hätte Art. 3 Abs. 2 DSGVO («durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter») anders formuliert werden müssen.

[24] So Kühling/Buchner-Klar, Art. 3 N 92; Plath-Plath, Art. 3 DSGVO N 27; wohl auch Ennöckl, in: Sydow (Hrsg.), Europäische Datenschutzgrundverordnung, 2. Aufl. 2018, Art. 3 N 15; Ernst, in: Paal/Pauly (Hrsg.), DS-GVO BDSG, 2. Aufl. 2018, Art. 3 N 19; tendenziell auch Meyerdierks, in: Moos/Schefzig/Arning (Hrsg.), Die neue Datenschutz-Grundverordnung, 2018, S. 50; a.A. von Lewinski, in: Auernhammer (Hrsg.),DSGVO BDSG, 5. Aufl. 2018, Art. 3 N 18; offengelassen: Gola-Piltz, Art. 3 N 31.

[25] Vgl. dazu oben.

[26] Näher Vasella, Zum Anwendungsbereich der DSGVO, digma 2017, 220 ff.

[27] Es ist allerdings nicht ausgeschlossen, dass in solchen Fällen das Recht eines Mitgliedstaats Anwendung findet; vgl. Fn. 11.

[28] Bei Unternehmen ausserhalb des EWR ist die Anwendbarkeit dabei stets eine punktuelle, d.h. auf die einzelne unter die DSGVO fallende Bearbeitungstätigkeit begrenzte.

[29] Dabei ist daran zu denken, dass ein solches Log-Buch den Behörden auf Anfrage herauszugeben ist, wobei sich bei Anfragen ausländischer Behörden weitere Fragen stellen (z.B. mit Bezug auf Art. 271 StGB).

[30] Vgl. z.B. http://datenrecht.ch/liechtenstein-muster-eines-verarbeitungsverzeichnisses.

[31] In Anlehnung an die entsprechende Liste der deutschen Datenschutzkonferenz, www.lda.bayern.de/media/dsfa_muss_liste_dsk_de.pdf.

[32] Bei zu grosser Ähnlichkeit der Bezeichnungen könnte von der freiwilligen Bestellung eines Datenschutzbeauftragten im Sinne von Art. 37 DSGVO ausgegangen werden; vgl. dazu die «Guidelines on Data Protection Officers» (rev.01) des Europäischen Datenschutzausschusses vom 5. April 2017.

[33] Die Mitgliedstaaten können gestützt auf Art. 23 DSGVO weitere Ausnahmetatbestände vorsehen, was z.B. Deutschland mit § 32 f. BDSG getan hat. Die Schweiz kann als Nicht-Mitgliedstaat dagegen keine Ausnahmetatbestände vorsehen.

[34] Demgegenüber verfolgen das geltende wie wohl auch das revidierte DSG einen anderen Ansatz: Im Einklang mit dem allgemeinen Persönlichkeitsrecht ist eine Datenbearbeitung grundsätzlich zulässig, sofern sie die Bearbeitungsgrundsätze einhält. Nur bei einer Verletzung der Grundsätze stellt sich die Frage einer Rechtfertigung.

[35] Zwar gilt die Einwilligung in eine Datenbearbeitung i.d.R. nicht als freiwillig, wenn sie zur Bedingung einer Leistung wird, weshalb sie nicht in AGB eingeholt werden kann («Kopplungsverbot»; s. Art. 7 Abs. 4 DSGVO und Erwägungsgrund 43). Wenn die Durchführung eines Vertrags ohne die Bearbeitung besonderer Personendaten aber nicht möglich ist, gleichzeitig aber kein anderer Rechtfertigungsgrund i.S.v. Art. 9 Abs. 2 DSGVO greift, ist die Einwilligung sachlich notwendig, sodass das Kopplungsverbot insoweit nicht zur Anwendung kommt.

[36] In Deutschland verlangt § 7 Abs. 2 Ziff. 3 und Abs. 3 des deutschen UWG grundsätzlich ebenfalls eine Einwilligung für den Versand elektronischer Werbung.

[37] Soweit es um die Einwilligung für Marketing geht, genügt es hier kaum, einen widersprechenden Empfänger lediglich aus der Versandliste zu löschen, zumindest dann, wenn die Gefahr besteht, dass seine Adresse einer Versandliste unbemerkt wieder hinzugefügt wird.

[38] Dies kann in einem sogenannten Löschkonzept festgelegt werden. Für die Entwicklung von Löschkonzepten gibt es eigene Standards, z.B. die ISO-Norm 66398.

[39] Das DSG verzichtet darauf, Mindestinhalte vorzugeben, auch das revidierte DSG.

[40] Allerdings ist nicht jede Dienstleisterin Auftragsverarbeiter. Häufig wird der Anwendungsbereich der Auftragsverarbeitung überschätzt. Hilfreich sind hier die FAQ des Bayerischen Landesamts für Datenschutzaufsicht (www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf): Eine Auftragsverarbeitung liegt nur vor, wenn ein Unternehmen «im Schwerpunkt mit der Verarbeitung personenbezogener Daten beauftragt wird»; eine begleitende oder beiläufige Datenbearbeitung durch den Dienstleister genügt daher nicht. In ihrem typischen Bereich keine Auftragsverarbeiter sind daher etwa Banken, Telecom-Anbieter, Post- und Versanddienste, Anwaltskanzleien, Personalvermittler, Reinigungsinstitute, Druckdienstleister usw.

[41] Vgl. Art. 46 und 49 DSGVO; meist werden in der Praxis die sogenannten EU-Standardvertragsklauseln verwendet. Ebenfalls zulässig ist die Übermittlung gestützt auf eine ausdrückliche Einwilligung, was in der Praxis nur in Ausnahmefällen praktikabel ist; wichtiger ist die Übermittlung für den Abschluss oder die Erfüllung eines Vertrags mit der betroffenen Person oder mit einem Dritten im Interesse der betroffenen Person (Art. 49 Abs. 1 lit. b und c DSGVO).

[42] Der Privacy Shield steht allerdings unter Druck seitens der EU-Kommission. Es empfiehlt sich daher sicherheitshalber der Abschluss eines Datenübermittlungsvertrags auch mit zertifizierten Unternehmen.