SCHWEIZERISCHE BANKRECHTSTAGUNG 2019

Institut für Bankrecht, Universität Bern

Banken und ihre datenschutzrechtliche Verantwortlichkeit im Verkehr mit ihren Dienstleistern

David Rosenthal/Barbara Epprecht

In: Susan Emmenegger (Hrsg.), Banken und Datenschutz, Basel 2019

ISBN 978-3-7190-4269-1

Inhaltsübersicht

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*

---

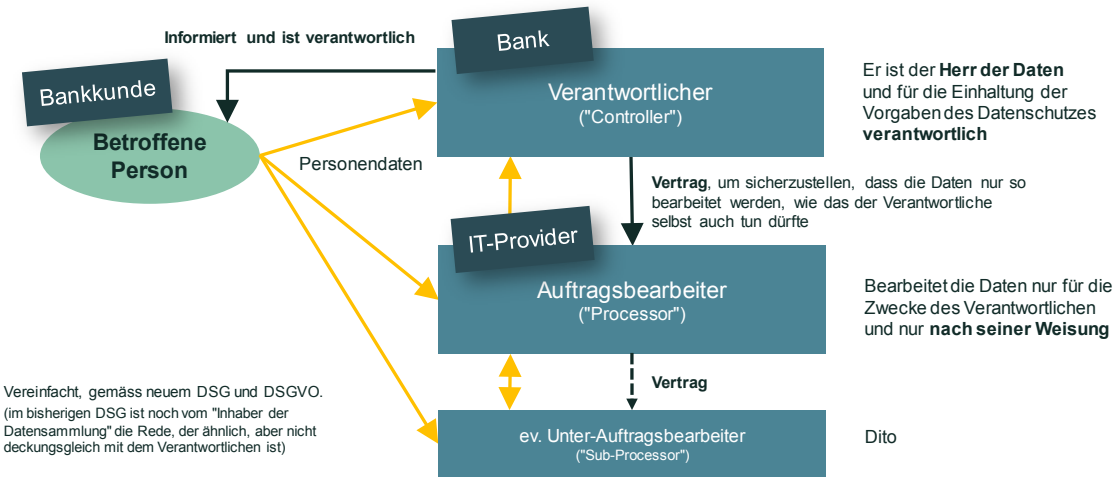
6 Während unter geltendem Datenschutzgesetz juristische Personen noch als Datensubjekte gelten (Art. 3 lit. b DSG), werden gemäss Art. 4 lit. b E-DSG nur noch natürliche Personen vom Anwendungsbereich des Gesetzes erfasst.

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.

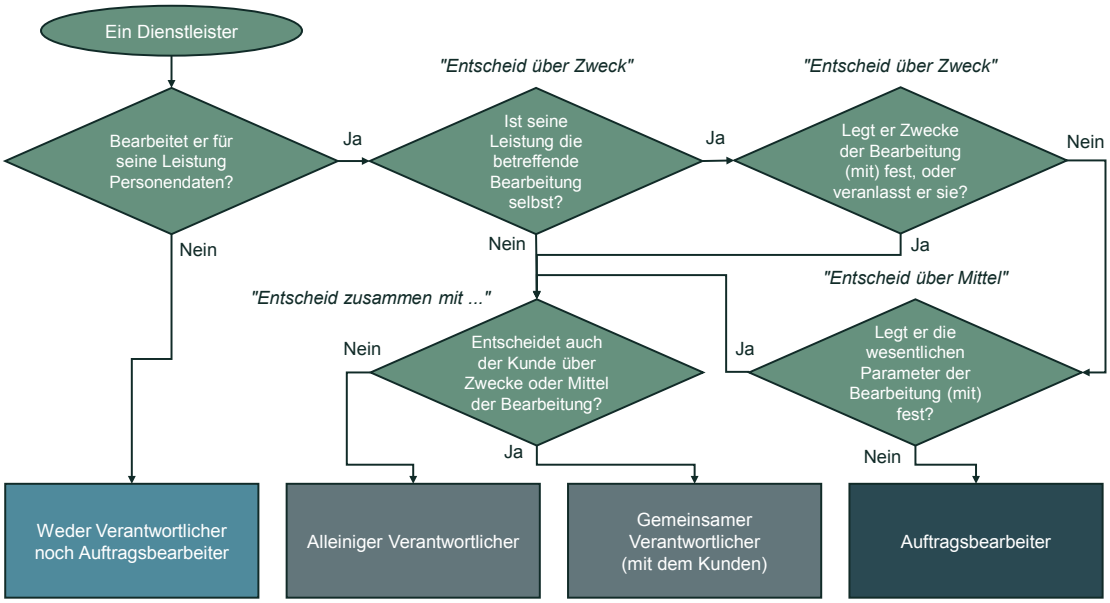
37 Ebd., Rz. 36 f.

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.