www.jusletter.ch

David Rosenthal

Controller oder Processor: Die datenschutzrechtliche Gretchenfrage

Kaum eine Rechtsfrage prägt den datenschutzrechtlichen Alltag seit letztem Jahr wie jene nach der Abgrenzung zwischen der Rolle des für eine Datenbearbeitung Verantwortlichen (Controller) und der des Auftragsbearbeiters (Processor). In der Praxis ist sie alles andere als trivial und auch nicht immer scharf möglich. Dieser Beitrag bietet eine Orientierungshilfe mit zahlreichen Beispielen aus der Praxis.

Beitragsarten: Wissenschaftliche Beiträge
Rechtsgebiete: Datenschutz; Informatik und Recht; Obligationenrecht

Zitiervorschlag: David Rosenthal, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, in: Jusletter 17. Juni 2019

ISSN 1424-7410, jusletter.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

EDITIONS WEBLAW

Inhaltsübersicht

1. Einleitung

[Rz 1] An sich ist die Frage nach der Verantwortlichkeit im Datenschutz einfach zu beantworten: Verantwortlich sind alle, die an einer Datenbearbeitung *mitwirken*. So verhält es sich jedenfalls in der Schweiz. Wer an einer widerrechtlichen Persönlichkeitsverletzung mitwirkt, kann diesbezüglich ins Recht gefasst werden (Art. 28 ZGB). Der Begriff der «Mitwirkung» ist dabei weit gefasst.[1] Dennoch hat sich im Datenschutz gemeinhin eine Ordnung entwickelt, nach welcher heute die Verantwortlichkeiten und dementsprechend auch die Aufgaben in der datenschutzrechtlichen Compliance aufgeteilt sind.

[Rz 2] Unterschieden wird üblicherweise zwischen dem «Verantwortlichen» (auch *Controller* genannt) und dem «Auftragsbearbeiter» (auch Auftrags*ver*arbeiter[2] oder *Processor* genannt). Ersterer ist als derjenige definiert, der gemeinsam mit anderen oder allein über «die Zwecke und Mittel» der Bearbeitung von Personen «entscheidet», während letzterer die Personendaten lediglich in dessen Auftrag bearbeitet. Das ist in der EU-Datenschutzgrundverordnung (DSGVO) so[3] und wird es auch im revidierten Datenschutzgesetz sein (jedenfalls basierend auf dem Entwurf des Bundesrates, E-DSG[4])[5]. Auch die meisten Pflichten im Zusammenhang mit der Datenbearbeitung knüpfen an eine dieser beiden Rollen an. Im Zentrum steht allerdings klar der Verantwortliche, wie bereits seine Bezeichnung sagt: Er ist derjenige, der dafür sorgen muss, dass eine Datenbearbeitung die gesetzlichen Vorgaben erfüllt und der primär die Verantwortung trägt, falls dies nicht der Fall sein sollte. Der Auftragsbearbeiter hingegen führt bloss aus, was ihm der Verantwortliche aufträgt. Dazu schliessen die beiden einen Auftragsdatenbearbeitungsvertrag –

1 Vgl. Entscheid des Bundesgerichts 5A_792/2011 vom 14. Januar 2013 i.S. «Tribune de Genève».

2 Dies ist die Bezeichnung im Rahmen der Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) DSGVO.

3 Art. 4 Ziff. 7 und 8 DSGVO, wobei dort von «Verarbeitung» statt «Bearbeitung» die Rede ist, was aber dasselbe meint.

4 Botschaft des Bundesrates über die Totalrevision des Bundesgesetzes über den Datenschutz und die Änderung weiterer Erlasse zum Datenschutz vom 15. September 2017; der Entwurf ist hier abrufbar: https://www.admin.ch/opc/de/federal-gazette/2017/7193.pdf (alle Webseiten zuletzt besucht am 29. Mai 2019).

5 Art. 8 Vorentwurf Bundesgesetz über den Datenschutz, E-DSG.

Datenschützer reden kurz von «ADV» – ab. Hält er sich daran, kommt er mit Ausnahme einiger weniger direkter gesetzlichen Pflichten[6] seiner Verantwortung nach.

2. Warum Dienstleister, die Daten bearbeiten, meist als Auftragsbearbeiter gelten

a. Ein beliebtes Konstrukt ...

[Rz 3] Im datenschutzrechtlichen Alltag scheint damit die Situation – auf den ersten Blick – mehr oder minder klar: Sobald ein Dienstleister im Auftrag eines Kunden von diesem Personendaten erhält oder für ihn beschafft und zur Erfüllung seines Auftrags bearbeitet, ist er nach weitverbreiteter Ansicht dessen Auftragsbearbeiter und es ist ein ADV abzuschliessen.

[Rz 4] Datenschutzrechtlich sind Auftragsbearbeitungen weitgehend problemlos umzusetzen und daher sehr beliebt: Technisch gibt der Kunde seinem Auftragsbearbeiter zwar Personendaten bekannt, doch ist der Auftragsbearbeiter rechtlich «privilegiert». Dies bedeutet, dass er datenschutzrechtlich nicht als Dritter gilt. Im DSG ist dies unbestritten und unter der DSGVO ebenfalls weitgehend anerkannt.[7] Wenn ein Auftragsbearbeiter für seinen Kunden Personendaten bearbeitet ist das daher so, als würde der Kunde diese Daten selbst bearbeiten. Er braucht dafür insbesondere keine Einwilligung des Kunden oder einen anderen Rechts- oder Rechtfertigungsgrund, jedenfalls im Normalfall.

[Rz 5] Das ist unter der DSGVO von besonderer Relevanz, da dort jede Bearbeitung, anders als unter dem DSG, zwingend einen Rechtsgrund erfordert, also zum Beispiel mit einer Einwilligung, einer gesetzlichen Pflicht, der Notwendigkeit zur Abwicklung eines Vertrags oder berechtigtem Interesse begründet werden muss.[8] Würde der Dienstleister nicht seinem Kunden zugerechnet und könnte die Bearbeitung durch den Dienstleister nicht durch den Rechtsgrund des Kunden legitimiert werden, weil sie als Bearbeitung zum Zweck des Dienstleisters und nicht mehr des Kunden gilt, wäre sie unzulässig. Doch dazu später mehr (Rz. 59 ff.).

b. Mit einfach umzusetzenden Anforderungen

[Rz 6] Liegt eine Auftragsbearbeitung vor, ist die betroffene Person vom Kunden unter der DSGVO und dem revidierten DSG zwar in allgemeiner Weise (ohne Namensnennung) darüber zu informieren,[9] aber eine Zustimmung ist im Normalfall nicht erforderlich und der Auftragsbearbeiter muss die betroffenen Personen gar nicht informieren, da er selbst nicht Verantwortlicher ist (vgl. jedoch Rz. 52 ff.).

---

6 Unter der DSGVO namentlich Art. 28 (weitere Pflichten nebst ADV), 29 (Mitarbeiter), 30 (Verzeichnis), 31 (Kooperation mit Aufsichtsbehörde), 32 (Datensicherheit), 33 (Data Breach Meldungen), 37 und 38 (betrieblicher Datenschutzbeauftragter) und Art. 44 ff. DSGVO (grenzüberschreitende Bekanntgabe von Personendaten).

7 Als «Dritter» gemäss Art. 4 Ziff. 10 DSGVO gilt er nach der Legaldefinition jedenfalls nicht. Wie weit seine Privilegierung reicht, ist aber nicht ganz unumstritten.

8 Art. 6, 9 und 10 DSGVO.

9 Weil der Auftragsbearbeiter als «Empfänger» gilt und über solche zu informieren ist (vgl. Art. 13 f. DSGVO, Art. 17 E-DSG).

[Rz 7] Auch die ADV stellen in der Praxis normalerweise kein Problem dar. Machte das geltende Datenschutzgesetz (DSG) und der Vorläufer der DSGVO noch kaum spezifische Vorgaben für einen solchen Vertrag, definiert die DSGVO acht Punkte, die jeder ADV abdecken muss (siehe Anhang «*Was in einen ADV gehört*»).[10] Der E-DSG übernimmt diese Vorgaben bis auf zwei Punkte nicht und lässt somit weiterhin einigen Spielraum; es hat einen leicht anderen Ansatz.[11] Das ist vernünftig, in der Praxis aber oft irrelevant,[12] da viele Unternehmen dazu übergegangen sind, ihre ADV standardmässig auch dann nach den Vorgaben der DSGVO auszugestalten, wenn die DSGVO gar nicht oder nicht immer zur Anwendung gelangt. Diskussionen zwischen Dienstleistern und ihren Kunden entstehen primär bezüglich der Frage der Kostentragung, der Art und Weise von Kundenaudits, wie das Weisungsrecht auszuüben ist und bezüglich der Schadloshaltung und Haftung bzw. ihrer Begrenzung.

c. Oft ein voreiliger Schluss

[Rz 8] Die Erfahrung zeigt freilich, dass Dienstleister in vielen Fällen voreilig als Auftragsbearbeiter qualifiziert werden. Der Umstand, dass ein Unternehmen seinen Kunden Leistungen erbringt und zu diesem Zweck von diesen Personendaten über deren Mitarbeiter, Kunden und anderen Dritten erhält, genügt nicht zur Annahme einer Auftragsbearbeitung. Auch das Vorliegen eines obligationenrechtlichen Auftrags oder Bestehen eines Weisungsrechts gegenüber dem Dienstleister führt nicht dazu, dass dieser Auftragsbearbeiter des Kunden ist, jedenfalls solange sich das Weisungsrecht nicht spezifisch auf die (Personen-)Datenbearbeitung bezieht.[13] Ebenso wenig genügt es, dass der Dienstleister die Daten nur für die Zwecke des Kunden bearbeitet und nicht auch für eigene Zwecke. Das Weisungsrecht und das Handeln für die Zwecke des Kunden sind zwar eine Voraussetzung für eine zulässige Auftragsbearbeitung. Entscheidend ist aber eine andere Frage: Ist der Dienstleister bezüglich der Datenbearbeitung, um die es geht, selbst ebenfalls Verantwortlicher? Ist er dies, fällt eine Auftragsbearbeitung ausser Betracht.[14]

3. Wann ist ein Dienstleister selbst Verantwortlicher?

[Rz 9] Fälle, in denen der Dienstleister *selbst* Verantwortlicher ist und daher als Auftragsbearbeiter nicht mehr in Betracht kommt, sind erfahrungsgemäss relativ häufig anzutreffen. Das gilt selbst dort, wo der Dienstleister schuldrechtlich durchaus nach der Weisung des Klienten handeln muss. Der Anwalt ist ein klassisches Beispiel: Er agiert unter einem Auftrag, ist an die Weisungen des Klienten gebunden und handelt nur für diesen. Soweit er zur Erfüllung seines Man-

10 Art. 28 DSGVO.

11 Statt in die Details zu gehen wie Art. 28 DSGVO, verlangt Art. 8 E-DSG, dass der Verantwortliche sicherstellt, dass der Auftragsbearbeiter nur das tut, was auch der Verantwortliche darf. Separat geregelt werden soll die Datensicherheit und die Unterauftragsbearbeitung.

12 Jedenfalls soweit ein ADV abgeschlossen wird. Die Schweizer Regelung hat den Vorteil, dass das Fehlen eines formellen Vertrags auch im Falle einer Auftragsbearbeitung nicht gleich zu einem Verstoss der Regelungen über die Auftragsbearbeitung führt, weil diese im Schweizer Recht auch ohne ADV eingehalten sein können, wenn sich der wesentliche Regelungsgehalt eines ADV anderweitig aus dem Verhältnis der Parteien ergibt.

13 Vgl. Artikel-29-Datenschutzgruppe, Stellungnahme 1/2010 zu den Begriffen «für die Verarbeitung Verantwortlicher» und «Auftragsverarbeiter» vom 16. Februar 2010 (WP169), S. 12.

14 Vgl. WP169 (Fn. 13), S. 30 f.

dats jedoch Personendaten bearbeitet, tut er dies als Verantwortlicher.[15] Darum muss mit ihm auch unter der DSGVO kein ADV abgeschlossen werden; es gibt nur wenige Ausnahmen, wo dies nicht gilt (Rz. 29).

[Rz 10] Warum das so ist und in welchen Fällen ein Dienstleister als Verantwortlicher gilt, ist nachfolgend erläutert und im Anhang mit zahlreichen Praxisbeispielen illustriert (vgl. Anhang: «*Beispiele aus der Praxis: Controller oder Processor?*»). Vorgängig ist allerdings noch ein kleiner, bald historischer Einschub erforderlich. Die nachfolgenden Ausführungen beziehen sich auf die Situation unter der DSGVO und dem E-DSG, welches die Terminologie von der DSGVO übernimmt. Unter dem heutigen DSG ist die Situation noch etwas anders. Es kennt den Begriff des Verantwortlichen und des Auftragsbearbeiters als solchen nicht. Stattdessen ist einerseits vom «Inhaber einer Datensammlung» die Rede[16] und andererseits vom Dritten, der im Auftrag eines anderen Daten bearbeitet.[17] Die beiden Rollen sind nicht deckungsgleich, wobei der Inhaber einer Datensammlung mit dem des Verantwortlichen eng verwandt ist. Letzterer bezieht sich jedoch auf einen Bearbeitungsvorgang, während ersterer sich auf eine Datensammlung bezieht. Theoretisch kann der Begriff der Auftragsbearbeitung unter dem heutigen DSG breiter verstanden werden als jener der DSGVO und dem E-DSG; so kann unter dem heutigen DSG auch der Mitarbeiter eines Unternehmens als Auftragsbearbeiter subsumiert werden[18], was unter der DSGVO klar nicht der Fall ist.[19] In der Praxis spielt dieser Unterschied aber zusehends keine Rolle mehr; in den letzten Jahren wurde auch im Schweizer Datenschutzrecht schleichend die Begriffsdefinition und das Begriffskonzept der EU-Datenschutzrichtlinie und DSGVO übernommen, weshalb auch hierzulande regelmässig nur noch vom Controller bzw. Verantwortlichen und vom Processor bzw. Auftragsbearbeiter die Rede ist. Die Revision des DSG soll dies formalisieren. Daher wird auch im vorliegenden Beitrag auf den allenfalls breiteren Geltungsbereich der Auftragsbearbeitung unter dem noch bestehenden DSG nicht mehr eingegangen.

4. Warum es den «Verantwortlichen» überhaupt gibt

a. Wer die datenschutzrechtlichen Parameter festlegt . . .

[Rz 11] Ausgangspunkt ist zunächst immer eine konkrete Bearbeitung von Personendaten, also z.B. das Führen der Personalakten, die Bearbeitung zur Abwicklung von Bestellungen eines Online-Shops, der Betrieb eines CRM-Systems, der Einsatz von Überwachungskameras, das Tracking der Nutzer einer Fitness-App oder der Betrieb eines Mail-Servers. Unter der DSGVO und dem E-DSG gilt nach der Legaldefinition diejenige Stelle als den dafür Verantwortlichen, der allein oder gemeinsam mit anderen «über die Zwecke und Mittel» dieser Datenbearbeitung «entscheidet».[20] Bei den Mitteln kommt es – wie weiter unten erläutert – primär auf die Eckwerte der Datenbearbeitung an, die für die Bestimmung der datenschutzrechtlichen Zulässigkeit oder

15 WP169 (Fn. 13), S. 35; Bayerisches Landesamt für Datenschutzaufsicht, FAQ zur DS-GVO, Auftragsverarbeitung, Abgrenzung, 20. Juli 2018 (https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf), S. 2.

16 Art. 3 Bst. i Bundesgesetz über den Datenschutz vom 19. Juni 1992 (DSG; SR 235.1).

17 Art. 10a DSG.

18 David Rosenthal, Handkommentar zum Datenschutzgesetz, Zürich 2008, Art. 10a DSG N 5 ff.

19 Dort sind Mitarbeiter unter Art. 29 DSGVO geregelt.

20 Art. 4 Ziff. 7 DSGVO, Art. 4 Bst. i E-DSG.

datenschutzrechtlichen Risiken der Bearbeitung von Relevanz sind.[21] Entscheidet ein Dienstleister also über diese «wesentlichen» Mittel oder sogar über den Zweck, der von ihm durchgeführten Datenbearbeitung, kann er diesbezüglich kein Auftragsbearbeiter sein, sondern ist selbst verantwortlich. Um als Verantwortlicher zu gelten genügt es bereits, wenn jemand nur über das eine *oder* das andere entscheidet, und er muss auch dies nicht einmal alleine tun. Entscheiden mehrere Unternehmen, Behörden oder andere Stellen über Zwecke oder Mittel ein und derselben Datenbearbeitung, werden sie als *gemeinsame* Verantwortliche betrachtet (dazu Rz. 67 ff.). Wer also aus Eigeninteresse auf eine Datenbearbeitung Einfluss nimmt und damit an der Entscheidung über die Zwecke und Mittel beteiligt ist, ist Verantwortlicher, wie es der EuGH zuletzt im Juli 2018 formulierte.[22]

b. . . . soll die Durchsetzung des Datenschutzes sicherstellen

[Rz 12] Die Figur des «Verantwortlichen» dient letztlich der Durchsetzung des Datenschutzes: Wann immer Personendaten bearbeitet werden, soll es immer jemanden geben, der dafür die Verantwortung trägt. Darum kann auch derjenige Verantwortliche sein, der ohne Plan Entscheide über die Zwecke oder Mittel einer Datenbearbeitung trifft, indem er Personendaten einfach zu bearbeiten beginnt. Da es nicht erforderlich ist, dass jeder Mitverantwortliche selbst Zugang zu den Personendaten hat (Rz. 72), ist es auch möglich denjenigen zu erfassen, der zwar selbst keine Daten bearbeitet, aber darauf aus eigenem Antrieb in anderer Weise einwirkt.

[Rz 13] Unter dem Schweizer Recht erscheint die Figur des Verantwortlichen auf den ersten Blick nicht zwingend erforderlich, da es wie erwähnt bereits den Grundsatz kennt, dass jeder, der an einer Persönlichkeitsverletzung «mitwirkt», für seinen Beitrag zur Verantwortung gezogen werden kann (Rz. 1). Da jedoch nicht alle sich aus dem Datenschutz ergebenden Pflichten auf diese Weise an eine Person anknüpfen lassen, ist die Figur des Verantwortlichen auch unter dem DSG nötig. Die Erfüllung der Betroffenenrechte (wie etwa das Auskunfts-, Korrektur- oder Löschrecht) oder von Meldepflichten sind Beispiele dafür. Sie werden normalerweise «nur» dem Verantwortlichen auferlegt (und bisher dem «Inhaber der Datensammlung»), nicht aber jedem Mitwirkenden; die Unterscheidung ist in der Praxis insbesondere für Risikoeinschätzungen von Relevanz.[23]

---

21 Gemeint sind Parameter wie die Kategorien von zu bearbeitenden Daten, woher sie stammen, wie sie ausgewertet und verknüpft werden, wie lange sie aufbewahrt werden, wem sie mitgeteilt werden, etc. Sie werden als die *wesentlichen Mittel* bezeichnet. Demgegenüber führt der Entscheid über die restlichen Mittel, d.h. die technischen und organisatorischen Massnahmen und sonstigen Schritte, die zur Durchführung der Datenbearbeitung und Datenschutz-Compliance vorgenommen werden (welche Software zum Einsatz kommt, wie sie konfiguriert ist, wie die Betroffenenrechte sichergestellt werden, die einzelnen Schritte zur Implementierung der datenschutzrechtlichen Parameter, Massnahmen zur Sicherstellung der Datensicherheit, etc.) grundsätzlich nicht zur Verantwortlichkeit für die Datenbearbeitung. Dazu ausführlich Rz. 44 ff.

22 Urteil des EuGH C-25/17 i.S. *Zeugen Jehovas* vom 10. Juli 2018, Rz. 68; im konkreten Fall ging es um Mitglieder der Zeugen Jehovas, die sich bei ihren Verkündigungen die Namen der von ihnen angesprochenen, nicht bekannten Personen notierten. Der EuGH erachtete nicht nur die Mitglieder als Verantwortliche, sondern auch deren Gemeinschaft, welche die Mitglieder organisiert, koordiniert und ermuntert hatte und damit an der Entscheidung über die Datenbearbeitung mitwirkte (Rz. 76 ff.).

23 Beispiel: Wenn Mitarbeiter eines Dienstleisters in der Schweiz an der ausländischen Datenbearbeitung eines ausländischen Kunden mitwirken, aber der Dienstleister nicht über Zwecke und Mittel entscheidet, so kann das DSG zwar auf etwaige Persönlichkeitsverletzungen Anwendung finden (Art. 139 IPRG) und sich Ansprüche auch gegen den Dienstleister aufgrund seines Tatbeitrags richten, die Betroffenenrechte müssen jedoch gegen den Kunden geltend gemacht werden (Art. 8 Abs. 4 DSG). Dieser Teil des DSG findet auf den Dienstleister keine Anwendung. Dem wäre selbst dann so, wenn der Mitarbeiter zwar über Zwecke oder Mittel der Bearbeitung entscheidet, er dies aber im Namen des Kunden tut.

c. Ob er verantwortlich sein will, spielt keine Rolle

[Rz 14] Aus dem Gesagten ergibt sich umgekehrt, dass unter der DSGVO und dem revidierten DSG nur aber immerhin derjenige ein Verantwortlicher mit Bezug auf eine Datenbearbeitung ist, der in der Lage ist, die zur Einhaltung des Datenschutzes nötigen Parameter dieser Datenbearbeitung festzulegen. Das kann sogar derjenige Dienstleister sein, der an sich Auftragsbearbeiter wäre (also z.B. ein Hosting-Provider), der von seinem Kunden aber keine Weisungen erhält und stattdessen die Ausgestaltung der datenschutzrechtlich relevanten Parameter der Datenbearbeitung selbst in die Hand nimmt. Durch dieses Verhalten ist er – möglicherweise ohne sich dessen bewusst zu sein – nebst dem Kunden Mitverantwortlicher und übernimmt damit auch die Verantwortung für die Einhaltung der DSGVO und des DSG, inklusive dem Risiko im Falle von Verstössen dafür sanktioniert zu werden. Daher wird es oft auch im Interesse eines Auftragsbearbeiters (und nicht nur des Kunden) sein, festzuhalten, dass der Dienstleister mit Bezug auf die Datenbearbeitung nur das tut, was ihm der Kunde vorgibt. Gibt es keinen ADV, sollte der Dienstleister sich mindestens «freiwillig» so verhalten, als agiere er unter einem ADV und nur das tun, was ihn der Kunde anweist zu tun und die Daten keinesfalls für eigene Zwecke verwenden (hingegen ist das Fehlen des ADV an sich für ihn nicht bussenträchtig[24]). Aus Sicht des Datenschutzes ist jedenfalls klar, dass es *immer* einen Verantwortlichen geben muss, wenn jemand Personendaten bearbeitet oder diesbezügliche Entscheide trifft, und jeder, der relevante Entscheide trifft, mit in der Verantwortung ist. Nur so können Schutzlücken vermieden werden.[25]

[Rz 15] Es gibt im Datenschutzrecht allerdings keine fixen Vorgaben, wie die Verantwortlichkeiten in einem Dienstleistungsverhältnis zu verteilen sind. Dies bietet entsprechenden Gestaltungsspielraum. Vernünftig erscheint immerhin, dass jeweils derjenige der (Haupt-)Verantwortliche sein sollte, der für die Sicherstellung der Datenschutz-Compliance aufgrund seiner Stellung dazu am besten geeignet ist. Dies fordert auch die Artikel-29-Datenschutzgruppe[26] in ihrem Papier zum Thema.[27] Das ist häufig derjenige, der von den betroffenen Personen als der natürliche Ansprechpartner bei etwaigen Datenschutzanliegen betrachtet wird. Das diesbezügliche Bauchgefühl erweist sich in der Praxis deshalb als relativ guter Ausgangspunkt für die Zuordnung der Verantwortlichkeit und Ausgestaltung der Vertragsbeziehung zwischen Kunde und Dienstleister.

---

24 Das gilt unter Art. 55 E-DSG, welcher lediglich die auf Seiten des Verantwortlichen handelnde Person strafrechtlich erfasst (bestraft werden die privaten Personen, die vorsätzlich «die Datenbearbeitung einem Auftragsbearbeiter übergeben, ohne dass die Voraussetzungen … erfüllt sind») und wohl auch unter der DSGVO, wo Art. 28 Abs. 3 den Vertrag selbst als Pflicht des Verantwortlichen ausgestaltet.

25 Dies wurde auch im «Facebook Fanpages»-Entscheid des EuGH (dazu Rz. 71 ff., m.w.H.) deutlich, der die Verantwortlichkeit für eine Statistikfunktion auf die Kunden von Facebook ausdehnte, weil Facebook diesen gewisse Mitbestimmungsmöglichkeiten überliess und sie die Schnittstelle zum Kunden kontrollierten. Es sollte sichergestellt werden, dass Facebook sich nicht auf den Standpunkt stellen kann, die Parameter der Statistik seien vom Kunden vorgegeben und nicht Sache von Facebook, während die Kunden wiederum argumentiert hätten, sie hätten gar keinen Zugriff auf die Personendaten und seien daher nicht verantwortlich. Die Kunden wurden in der Folge als Mitverantwortliche qualifiziert.

26 Die ehemalige Konferenz der EU-Datenschutzbehörden und Vorgängerinstitution des Europäischen Datenschutzausschusses (EDSA) unter der DSGVO.

27 WP169 (Fn. 13), S. 9, wonach im Zweifelsfall grundsätzlich die Lösung vorzuziehen sei, welche die grössten Chancen der wirksamen Durchsetzung des Datenschutzes verspricht.

5. Entscheid über die «Zwecke» der Bearbeitung

a. Wer hat die Datenbearbeitung veranlasst?

[Rz 16] Die Formel «der über Zwecke und Mittel entscheidet» mag zunächst etwas kryptisch anmuten, vor allem was die «Zwecke» der Bearbeitung betrifft. Der Begriff spielt nicht unmittelbar auf den Zweckbindungsgrundsatz an; ob ein Verantwortlicher ihn einhält oder er die Zwecke korrekt kommuniziert, spielt für seine Qualifikation als Verantwortlicher keine Rolle. Es geht auch nicht darum, wer die eigentlichen Inhalte für die Datenbearbeitung auswählt und liefert – das muss nicht notwendigerweise der Verantwortliche sein (die Personendaten selbst sind nicht die Mittel ihrer Bearbeitung).[28] Es geht vielmehr um die Frage, ob und warum die Datenbearbeitung überhaupt stattfindet und was sie erreichen soll – und wer diesbezüglich das Sagen hat, auch wenn sie datenschutzwidrig sein sollte. Es ist die Antwort auf die Frage: Wer hat die Datenbearbeitung veranlasst und das Ziel bestimmt?[29] In ihrer Empfehlung WP169, in welchem sich die Artikel-29-Datenschutzgruppe ausführlich mit dem Thema auseinandergesetzt hat, definiert sie den Zweck als «erwartetes Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet».[30] Ob der Entscheid zur Datenbearbeitung aus freien Stücken erfolgte oder durch eine gesetzliche oder vertragliche Pflicht provoziert ist, spielt dabei keine Rolle (zur gesetzlichen Pflicht vgl. Rz. 32).

[Rz 17] Es geht um die Frage beim Entscheid um den Zweck darum, *wessen* Datenbearbeitung es ist. Wer eine Datenbearbeitung als die Seine beansprucht und sich damit faktisch den Entscheid über die Zwecke einer Datenbearbeitung zu Eigen macht, muss daher auch damit rechnen, dass er als Verantwortlicher betrachtet wird. Im Gegensatz dazu führt der Auftragsbearbeiter eine *fremde* Datenbearbeitung aus, eine Datenbearbeitung über die bereits entschieden ist, nämlich von seinem Kunden: Es geht nur noch um die Frage, wer sich darum kümmert und ausführt, worüber der Verantwortliche im Wesentlichen bereits befunden hat. Die Datenbearbeitung ist *jene des Kunden*, nicht die des Auftragsbearbeiters. Er betreut sie lediglich für den Kunden.

[Rz 18] Auf den Fall eines Dienstleisters und dessen datenschutzrechtliche Qualifikation als Verantwortlicher angewandt, kann eine Unterscheidung zwischen den beiden folgenden Typen von Verantwortlichen helfen:

a. Die erste Fallgruppe umfasst Dienstleister, deren Leistung im Kern die Bearbeitung von Personendaten umfasst, die aber trotzdem über die Zwecke der Bearbeitung entscheiden. Die Leistung, die sie ihrem Kunden erbringen, *ist* das Bearbeiten von Personendaten. Trotzdem ist es *ihre* Datenbearbeitung, und nicht jene des Kunden.
b. Die zweite Fallgruppe umfasst Dienstleister, deren Datenbearbeitung lediglich der Erbringung ihrer – in der Sache anders gearteten. – Leistung dient oder aus anderen Gründen erfolgt. Die Leistung, die sie ihrem Kunden erbringen, ist jedenfalls *nicht* das Bearbeiten von Personendaten, auch wenn das Lieferobjekt solche enthalten mag.

[Rz 19] Die beiden Kategorien werden in den beiden nachfolgenden Kapiteln erörtert.

28 WP169 (Fn. 13), S. 35, Beispiel 22.

29 WP169 (Fn. 13), S. 11.

30 WP169 (Fn. 13), S. 16.

6. Wenn die Datenbearbeitung die Leistung selbst ist

a. Beispiel Social Media

[Rz 20] Ein Beispiel für die erste Kategorie ist eine Online-Kontaktbörse: Ihr Angebot besteht im Wesentlichen in der Bereitstellung von Kontaktanzeigen ihrer Benutzer, also in einer Bearbeitung von Personendaten. Auch entscheidet jeder Benutzer selbst, ob und mit welchem Inhalt er eine Kontaktanzeige aufgeben oder darauf antworten will. Über die Datenbearbeitung im Sinne des Betriebs der Plattform an sich entscheidet jedoch deren Betreiber; er entscheidet, ob es sie gibt, welche Inhalte und Nutzer er zulassen will und wozu die Daten genutzt werden können (z.B. auch für Werbung). Damit ist er derjenige, der darüber entscheidet, was mit der Datenbearbeitung namens «Online-Kontaktbörse» erreicht werden soll, und somit der datenschutzrechtliche Verantwortliche. Er hat sie veranlasst, er gibt den Rahmen vor, es ist *seine* Datenbearbeitung.

[Rz 21] Ob und von wem und mit welchem Inhalt seine Dienstleistung in diesem definierten Rahmen in Anspruch genommen wird, ist für die Frage der Qualifikation des Betreibers als Verantwortlicher nicht relevant – die Ausrichtung und Ausprägung der Datenbearbeitung als Ganzes ändert dies nicht. Es verhält sich wie mit einer Zeitung. Auch wenn sie fremden Autoren und Anzeigekunden einen Raum für deren Inhalte als Auftragsbearbeiterin bietet, bleibt es ihre Publikation. Die Inhalte werden Teil der Zeitung, d.h. die Zeitung ist nicht bloss Datenträger. Es käme aber niemand auf die Idee, sie als Auftragsbearbeiterin zu qualifizieren.[31]

[Rz 22] Dass der Betreiber der Kontaktbörse Verantwortlicher ist, bedeutet nicht, dass die Nutzer der Plattform nicht ihrerseits Verantwortliche sein können, so zum Beispiel mit Bezug auf einzelne Kontaktanzeigen – soweit sie darin Personendaten anderer verwenden oder mit Bezug auf private Nachrichten, die sie über das System an andere versenden (soweit die DSGVO darauf anwendbar ist[32]).[33] Je nachdem, auf welcher Ebene der Betreiber der Kontaktbörse und sein jeweiliger Kunde zusammenwirken, sind sie eigenständige oder gemeinsame Verantwortliche (dazu Rz. 81 ff. und insbesondere Rz. 86). Eine Auftragsbearbeitung liegt hingegen nicht vor, da der Betreiber der Kontaktbörse analog des Redaktors der Zeitung seine Hoheit über die Inhalte behalten will.[34] Er mag sich zwar nicht immer in die Inhalte einmischen, was aber auf der Plattform möglich ist, bestimmt er.

[Rz 23] Betreiber von Social-Media-Plattformen fallen aus demselben Grund ebenfalls grundsätzlich in die Kategorie der Verantwortlichen:[35] Sie beanspruchen für sich zu definieren, welche Datenbearbeitungen und sonstigen Vorgänge auf ihrer Plattform stattfinden sollen. Das grenzt sie zum reinen Hosting-Anbieter ab, der auf seinen Servern Speicherplatz für Internet-Auftritte, Web-Shops und andere Online-Aktivitäten zur Verfügung stellt. Zwar wird auch der Hosting-Anbieter in seinen Nutzungsbestimmungen festhalten, welche Inhalte auf seinen Servern untersagt sind. Dies hat jedoch keine redaktionellen Gründe wie im Falle der sozialen Medien, sondern dient in aller Regel alleine dem Schutz vor Verantwortlichkeitsansprüchen. Der Hosting-Anbieter

31 Unter der DSGVO ist zu beachten, dass gedruckte Zeitungen nicht unbedingt von der DSGVO erfasst sind, da sie nur für ganz oder teilweise automatisierte Bearbeitungen und für die Bearbeitung solcher Personendaten gilt, die in einer strukturierten Weise abgelegt sind.

32 Art. 2 Abs. 2 Bst. c DSGVO; das DSG hat demgegenüber einen etwas weiteren Anwendungsbereich.

33 WP169 (Fn. 13), S. 14, Fussnote 12.

34 Was nicht bedeutet, dass er damit tun und lassen kann, was er will, denn an den Datenschutz – insbesondere die Bearbeitungsgrundsätze – muss er sich natürlich trotzdem halten.

35 WP169 (Fn. 13), S. 26, Beispiel 12.

stellt nur Infrastruktur zur Verfügung. Für welche Datenbearbeitung der Kunde sie nutzen will, ist im Rahmen des technisch Möglichen und Zulässigen seine Sache. Es handelt sich um *seine* Datenbearbeitung.

b. Mischformen sind denkbar – es zählen die tatsächlichen Verhältnisse

[Rz 24] Die Übergänge sind freilich nicht immer so klar wie im Beispiel der Kontaktbörse. Zudem sind Mischformen denkbar: So ist es denkbar, dass auch der Betreiber einer Social-Media-Plattform gewissen (Geschäfts-)Kunden, analog einem Hosting-Anbieter, eine Plattform für deren Angebote anbietet – so ähnlich wie «Shop-im-Shop» im Detailhandel. Ist der Betreiber der Social-Media-Plattform in diesen Fällen bereit, seine Kontrolle über diesen Teil der Plattform dem Drittanbieter abzugeben,[36] wird er gegenüber diesem bezüglich dessen Drittangebots zum Auftragsbearbeiter oder gemeinsamen Verantwortlichen.

[Rz 25] Dienstleister haben es somit oftmals selbst in der Hand zu entscheiden, wie sie ihr Angebot gestalten: Wollen sie «bloss» Auftragsbearbeiter sein und sich aus der datenschutzrechtlichen Verantwortung weit herausnehmen oder aber wollen sie als Verantwortliche auftreten und eine entsprechende Kontrolle über die auf ihrer Infrastruktur stattfindenden Datenbearbeitungen ausüben? Bevor ein Dienstleister sich also fragt, ob er Auftragsbearbeiter oder Verantwortlicher ist, sollte er sich fragen, welche dieser beiden Rollen er denn übernehmen *will*. Beide haben ihre Vor- und Nachteile (dazu Rz. 114). Entsprechend dieser Wahl sind dann Angebot und Vertragsbedingungen auszugestalten. Dabei ist es ohne Weiteres möglich, dass ein Anbieter die im Wesentlichen selbe Dienstleistung für ein jeweils unterschiedliches Zielpublikum in beiden Ausprägungen anbietet (dazu Rz. 52). Es ist aber zu beachten, dass letztlich die gelebten Verhältnisse zählen. Es gibt immer wieder Dienstleister, die aus Bequemlichkeit oder Scheu vor Verantwortung sich in die Rolle des Auftragsbearbeiters flüchten und von den Kunden den Abschluss eines ADV verlangen, obwohl aufgrund der Umstände auf der Hand liegt und auch sinnvoller ist, dass sie selbst Verantwortliche sind, weil sie letztlich die Kontrolle darüber haben und behalten wollen, wie sie die Daten ihrer Kunden bearbeiten und sie oft auch für eigene Zwecke nutzen wollen. Darauf sollten sich Unternehmen nicht einlassen und auch für die Dienstleister ist diese Strategie sehr riskant.[37] Wer zwar auf dem Papier ein Auftragsbearbeiter ist, sich aber wie ein Verantwortlicher verhält, ist Verantwortlicher – ADV hin oder her (so geschehen im Fall SWIFT, Rz. 90 ff.).

c. Sonderfall: Der Auftraggeber ist die betroffene Person selbst

[Rz 26] Eine Ausnahme gibt es allerdings: Wenn ein Dienstleister ausschliesslich Personendaten seines Kunden bearbeitet, d.h. er zwar Personendaten hat, sie sich aber ausschliesslich auf den Kunden selbst als betroffene Person beziehen, ist der Dienstleister zwangsläufig Verantwortlicher. Dies liegt daran, dass ein Auftragsbearbeiter definitionsgemäss nur im Auftrag eines Ver-

36 Was zeitlich beschränkt und an Bedingungen geknüpft sein kann, deren Verletzung den Betreiber zur Rücknahme der Kontrolle berechtigen. Abgegeben hat er die Kontrolle für diesen Zeitraum jedoch trotzdem.

37 Insbesondere dann, wenn sich der Dienstleister tatsächlich aus der Verantwortung nimmt und dementsprechend nicht seinen diversen Pflichten als Verantwortlicher gemäss anwendbarem Datenschutzrecht nachkommt (wie z.B. die Information der betroffenen Personen) und sich so einem Bussenrisiko aussetzt.

antwortlichen tätig sein kann,[38] die betroffene Person bezüglich ihrer eigenen Personendaten aber definitionsgemäss nie zugleich Verantwortlicher sein kann. Soweit ein Cloud-Anbieter also einer Person ihren Speicher nur für dessen eigenen Personendaten anbietet, ist er deren Verantwortlicher. Sobald seine Cloud vom Kunden aber auch zur Speicherung von Personendaten anderer betroffener Personen benutzt wird, wird er zum Auftragsbearbeiter. Da der Cloud-Anbieter dies normalerweise nicht verhindern kann oder will, stellt er sich von vornherein auf eine Auftragsbearbeitung ein.

[Rz 27] In anderen Konstellationen kann die Unterscheidung von Relevanz sein: Ein Automobilhersteller, der in seinen Fahrzeugen einen Cloud-gestützten Fahrzeugortungsdienst anbietet, wird normalerweise nicht wissen können, wer das Fahrzeug fährt. Aus Sicht des Herstellers handelt es sich bei allen erhobenen Daten um Personendaten nur seines Kunden als betroffene Person. Der Hersteller ist damit Verantwortlicher. Dass der Kunde wiederum den Dienst für sich selbst nutzen kann um herauszufinden, wo sich jene anderen Personen befinden, denen er sein Auto ausleiht, ändert daran nichts (vgl. Rz. 96 ff.), macht jedoch den Kunden zu einem eigenständigen Verantwortlichen der betreffenden Datenbearbeitung. Eigenständig ist er deshalb, weil seine Datenbearbeitung nicht diejenige des Herstellers ist, d.h. sie auf einer anderen Ebene stattfindet (dazu Rz. 82 ff.).

7. Wenn die Datenbearbeitung nur das Mittel zum Zweck ist

a. Beispiel Anwalt

[Rz 28] In der zweiten Fallkonstellation geht es ebenfalls darum, wer das Ziel im Rahmen einer Dienstleistung erfolgenden Datenbearbeitung definiert. Allerdings erscheint hier die Situation augenfälliger, denn die Datenbearbeitung ist nicht der Zweck oder das Ziel der Dienstleistung, sondern lediglich Mittel zum Zweck des Dienstleisters. Geschuldet ist dem Kunden nicht eine Datenbearbeitung. Ob der Dienstleister die Datenbearbeitung vornimmt (und wie) entscheidet der Dienstleister, da sie unmittelbar nur ihm dient, auch wenn sie letztlich für die Zwecke des Kunden erfolgt und mittelbar diesem ebenfalls zu Gute kommt. Das unterscheidet den Anwalt vom Hosting- oder Cloud-Provider: Ersterer führt den Fall des Kunden; ob und wie weit er dazu Personendaten bearbeitet, ist seine Entscheidung – es sind seine Akten. Letzterer verspricht dem Kunden, seine Daten auf seinen Servern in einer bestimmten Art und Weise zu bearbeiten. Ob und wie weit dieser damit Personendaten bearbeitet, entscheidet der Kunde.

[Rz 29] Aus diesem Grund sind Dienstleister, deren Leistung im Wesentlichen nicht in der Erbringung einer Datenbearbeitung besteht, diesbezüglich meist auch dann keine Auftragsbearbeiter, wenn sie zwecks Vertragserfüllung Personendaten vom Kunden erhalten. Diese Daten sind dann aus der Optik der Verantwortlichkeit «ihre» Daten, und wenn sie diese bearbeiten, ist es «ihre» Datenbearbeitung.[39] Ob sie eine schuldrechtliche Herausgabepflicht haben (wie etwa der Auftragnehmer gegenüber dem Auftraggeber), spielt keine Rolle. Auch ein Weisungsrecht des Auftraggebers tangiert diese Qualifikation normalerweise nicht, es sei denn, das Weisungsrecht zielt darauf, wie die Daten zu bearbeiten sind. Um beim Beispiel des Anwalts zu bleiben: Norma-

38 Art. 4 Ziff. 8 DSGVO.

39 WP169 (Fn. 13), S. 35, Beispiel 21.

lerweise wird der Klient seinen Anwalt lediglich anweisen, in seinen Rechtsschriften, Vertragsverhandlungen oder seiner Beratung eine bestimmte Strategie zu folgen und bestimmte Dinge zu tun. Ob und wie der Anwalt hierzu seine Akten führt, welche Personendaten er erhebt oder welche Beweise er einreicht bestimmt primär er. Anders wäre es, wenn der Anwalt – wie bei grösseren Kanzleien teilweise der Fall – als Teil seiner Dienstleistung für den Kunden auch dessen Datenmanagement übernimmt, für ihn zum Beispiel den Datenraum unterhält, in welchem sein Klient einem potenziellen Investor Einblick in die Unterlagen der Gesellschaft gibt, oder im Rahmen eines US-amerikanischen Zivilprozesses eine Datenbank mit den im Rahmen einer e-Discovery vom Klienten der Gegenseite herauszugebenen Akten unterhält. Hier wird die Kanzlei zum Auftragsbearbeiter. Das ist im Übrigen auch dann der Fall, wenn der Klient sein Weisungsrecht nicht nur bezüglich der anwaltlichen Tätigkeit ausübt, sondern auch punkto Datenbearbeitung durch den Anwalt. Hat der Anwalt diesbezüglich keinen wirklichen Handlungsspielraum mehr, wird seine Datenbearbeitung zu jener des Klienten und er ebenfalls zum Auftragsbearbeiter.[40] Die Weisungen müssen sich jedoch letztlich darauf beziehen, wie er seine Daten zu bearbeiten hat[41] und nicht bloss, wie er den Fall führen soll (z.B. was er der Gegenpartei schreiben oder welches Beweismittel er einbringen soll).

b. Beispiel Banken und Versicherer

[Rz 30] Ein weiteres klassisches Beispiel eines Dienstleisters, für den die Datenbearbeitung nur Mittel zum Zweck ist, ist die Versicherung: Ihre Leistung besteht im Bereitstellen eines Versicherungsschutzes. Wenn nun ein Unternehmen im Rahmen der Versicherung seiner Mitarbeiter deren Angaben der Versicherungsgesellschaft zwecks Vertragsabwicklung mitteilt, liegt keine Auftragsbearbeitung vor. Auch hier ist es die Versicherung, die darüber entscheidet, dass es zu einer Datenbearbeitung kommt, weil sie entscheidet, ob und welche Mitarbeiterdaten sie für die Berechnung ihrer Prämien, die Eingrenzung des Versicherungsschutzes und auch sonst ihre Vertragserfüllung braucht; ihrem Kunden dient dies zwar mittelbar, aber es kann ihm im Grunde gleichgültig sein, ob die Versicherung diese Daten bearbeitet oder nicht – solange die Versicherung ihre Leistung erbringt. Die Versicherung ist daher bezüglich der Bearbeitung der Mitarbeiterdaten eine Verantwortliche.

[Rz 31] Genauso verhält es sich mit der Bank, die Zahlungsaufträge ausführt und dazu Personendaten des Bankkunden und Dritter (z.B. Zahlungsempfänger) bearbeiten muss, mit dem Mobilfunkanbieter, der allen leitenden Angestellten eines Unternehmenskunden eine persönliche Mobiltelefon-Nummer auf Kosten ihres Arbeitgebers bereitstellt sowie mit dem Zahlungsdienstleister, der im Auftrag eines Webshop-Betreibers auf dessen Website Kreditkartenzahlungen ab-

40 Die Artikel-29-Datenschutzgruppe erwähnt das Beispiel des Rechnungsprüfers, der für ein Unternehmen zwecks umfassender Buchprüfung tätig ist und dabei ausführlichen Weisungen des fest angestellten Buchprüfers des Unternehmens unterliegt (WP169 [Fn. 13], S. 35, Beispiel 23). Das Beispiel ist insofern unpassend, als es sich diesfalls weder um einen Auftragsbearbeiter noch um einen Verantwortlichen, sondern um eine unter ihrer Aufsicht arbeitende Person handeln würde (vgl. Art. 29 DSGVO, dazu Rz. 104 ff.).

41 Womit allerdings nicht die Vorsichtsmassnahmen gemeint sind, die sich z.B. in Controller-Controller-Verträgen finden, mit denen ein Klient seine Risiken in Grenzen halten will, indem er dem Anwalt etwa vorschreibt, dass er die Akten nach dem Mandat zurückzugeben hat. Zu denken ist an materielle Vorgaben wesentlicher Natur, wie der Anwalt seine Datenbearbeitungen in der Kanzlei mit Bezug auf das Mandat generell vorzunehmen hat, um seine Leistung zu erbringen (z.B. welche Daten er zu erheben hat und von wem), und nicht bloss Weisungen für einzelne Handlungen.

wickelt und dazu von dessen Kunden Personendaten erhebt und weitergibt. Sie alle sind Verantwortliche und keine Auftragsbearbeiter. Daher schliesst die Bank mit ihnen keinen ADV ab. Der Umstand, dass die Bank dem Empfänger einer Zahlung den Absender und Zahlungszweck mitteilt und ihre Leistung damit auch eine Datenbearbeitung beinhaltet, ändert nichts an ihrer Stellung als Verantwortliche: Der Inhalt stammt zwar vom Kunden, aber den Zweck dieser Datenbearbeitung hat die Bank bestimmt. Die Ausführung des Zahlungsauftrags ist *ihre* Datenbearbeitung. Mit dem Absenden des Zahlungsauftrags haben die Personendaten die Sphäre des Kunden, in welcher er der Verantwortliche ist, verlassen.

c. Bearbeitung aus eigenen gesetzlichen Pflichten

[Rz 32] Bearbeitet ein Dienstleister Personendaten seines Kunden nicht nur zur Vertragserfüllung, sondern noch aus anderen, eigenen, von den Zwecken des Kunden nicht gedeckten Gründen, ist die Wahrscheinlichkeit, dass er Verantwortlicher ist noch sehr viel höher. Ein klassisches Beispiel ist das Unternehmen, das Personendaten bearbeitet, um eine *eigene* gesetzliche Verpflichtung zu erfüllen, also etwa ein Finanzintermediär, der Daten aus dem Kreis seiner Kunden zur Erfüllung seiner Pflichten unter der Geldwäschereigesetzgebung bearbeitet, oder das Unternehmen, das mit Bezug auf seine Buchhaltungsbelege, die auch Kundendaten enthalten können, den gesetzlichen Aufbewahrungspflichten für solche Belege nachkommt.[42] Auch der Dienstleister, welcher einer Behörde auf deren Befehl hin Daten eines Kunden aushändigt, wird bezüglich dieser Datenbearbeitung meist zum Verantwortlichen (vgl. dazu Rz. 90).[43] Der Umstand, dass er auf den ersten Blick die Daten ausliefern *muss* ändert wie vorne bereits erwähnt (Rz. 16) nichts daran, dass es nach wie vor sein Entscheid ist, dem Befehl Folge zu leisten. Er könnte ihn auch anfechten, und er muss entscheiden, ob und wie er dem Befehl und zum Beispiel seinen Datenschutzpflichten nachkommt und die betroffenen Personen informiert. Das ist der Sinn der Sache. Führt die Einhaltung der gesetzlichen Verpflichtung durch einen Auftragsbearbeiter allerdings nicht zu einer separaten Datenbearbeitung, sondern beschlägt sie lediglich die Datenbearbeitung des Kunden (z.B. eine gesetzliche Geheimhaltungspflicht des Dienstleisters, die neben die vertragliche tritt) und liegt ihre Erfüllung im Rahmen dessen, was der Kunde ohnehin verlangt, so ändert dies am Status des Auftragsbearbeiters nichts.[44] In diesem Fall liegt der Datenbearbeitung kein selbstständiger Entscheid des Auftragsbearbeiters zugrunde.

---

42 Insofern erscheint der Vorbehalt in Art. 28 Abs. 3 Bst. g DSGVO, wonach ein Auftragsbearbeiter einem Löschbefehl seines Auftraggebers dann keine Folge leisten muss, wenn von ihm eine Gesetzespflicht verlangt, dass er die Daten aufbewahrt, lediglich theoretischer Natur. Wäre dies der Fall, würde er zum Verantwortlichen.

43 WP169 (Fn. 13), S. 14.

44 Dementsprechend sieht Art. 28 Abs. 3 Bst. a vor, dass der Auftragsbearbeiter dem Verantwortlichen mitteilen muss, wenn er wegen einer eigenen gesetzlichen Verpflichtung nicht in der Lage sein sollte, den Weisungen nachzukommen.

8. Entscheid über die «Mittel» der Bearbeitung

a. a. Die datenschutzrechtlichen Parameter, nicht ihre Umsetzung

[Rz 33] Etwas klarer erscheint auf den ersten Blick das Kriterium des Entscheids über die «Mittel» einer Bearbeitung von Personendaten. Hierbei wird danach gefragt, wer darüber entscheidet, wie die Personendaten bearbeitet werden, also die «Art und Weise, wie ein Ergebnis oder Ziel erreicht wird».[45] Der Begriff der Mittel umfasst nicht nur – wie es der Wortsinn suggeriert – die technischen und organisatorischen Mittel (z.B. Funktionalität von Software, Standort von Servern, Massnahmen der Datensicherheit, Prozesse zur Datenbearbeitung). Der Begriff der Mittel meint insbesondere, wie die Datenbearbeitung mit Bezug auf die datenschutzrechtlich relevanten Faktoren ausgestaltet ist, also zum Beispiel welche Art von Personendaten erhalten und wie lange die Daten bearbeitet werden, aus welchen Quellen, welche Bearbeitungsvorgänge wann und warum stattfinden, wer Zugang dazu erhält, ob Daten ins Ausland gehen und wohin. Bei der Bestimmung der Verantwortlichkeit stehen eben diese Parameter im Zentrum, nicht die technischen und organisatorischen Mittel (doch dazu später mehr, Rz. 48 ff.).

[Rz 34] Das Kriterium des Entscheids über die Mittel der Bearbeitung ist vor allem dort wichtig, wo auf den ersten Blick eine Auftragsbearbeitung vorliegen mag, weil der Kunde die Datenbearbeitung veranlasst, der Dienstleister aber nicht einfach die Weisungen seines Kunden ausführt, sondern über eine erhebliche Autonomie in der Ausgestaltung der Datenbearbeitung verfügt. Bestimmt der Dienstleister die datenschutzrechtlichen Parameter wesentlich mit, so ist er grundsätzlich ebenfalls Verantwortlicher (vgl. aber Rz. 41 ff.).[46] Damit ist wiederum sichergestellt, dass er für seine Mitwirkung zur Verantwortung gezogen werden kann, auch wenn es sich nicht um «seine» Datenbearbeitung handelt, weil er nicht die Zwecke der Datenbearbeitung bestimmt.

b. Beispiel Arzneimittelstudie

[Rz 35] Ein Pharmaunternehmen gibt beispielsweise in Auftrag, eine Arzneimittelstudie zu erstellen. Es ist jedoch ein Studienzentrum bzw. die teilnehmenden Ärzte, die die Studie – die Behandlung der Studienteilnehmer inklusive – durchführen. Auch wenn das Pharmaunternehmen als «Sponsor» die Studie veranlasst und hierfür Rahmenbedingungen vorgibt und am Ende über die Ergebnisse verfügen kann, hat ein solches Studienzentrum oft eine weitgehende Autonomie, wie es die Daten der Patienten bearbeitet, sofern es gewisse Vorgaben des Sponsors einhält, damit die Daten für den Sponsor brauchbar sind, und er sie schliesslich auch für seine Zwecke nutzen kann. Es klärt die Teilnehmer auf, holt ihre Einwilligungen ein, entscheidet, wann es welche Daten erhebt, gibt ihnen Auskunft und bestimmt auch sonst in wesentlicher Weise mit, wie die Daten zu bearbeiten sind. Das Studienzentrum bestimmt zwar letztlich nicht den Zweck der Datenbearbeitung (Studie) – oder höchstens, soweit es die medizinische Versorgung der Teilnehmer betrifft –, aber das Studienzentrum ist es, das wesentliche Entscheide über die Mittel der Bearbeitung trifft und sich damit zum Verantwortlichen macht,[47] wenn auch in aller Regel gemeinsam mit dem Sponsor (dazu Rz. 57 ff.). Das ist auch gefühlt richtig: Die Teilnehmer wissen zwar, dass

45 WP169 (Fn. 13), S. 16.

46 WP169 (Fn. 13), S. 17 unten.

47 So auch WP169 (Fn. 13), S. 36, Beispiel 25.

der Sponsor die Studie in Auftrag gegeben hat, aber ihr Ansprechpartner für alle Fragen ist das Studienzentrum. Gefühlt trägt es und nicht der Sponsor die Verantwortung für die Bearbeitung ihrer Daten; er hat womöglich nicht einmal Zugriff auf die Daten im Klartext. Setzt der Sponsor darüber hinaus noch zur Unterstützung oder Datenauswertung eine Clinical Research Organization (CRO) ein, wird diese hingegen oft eine Auftragsbearbeiterin sein, da sie lediglich die Datenbearbeitung des Sponsors (oder Studienzentrums) ausführt, wie auch involvierte IT-Provider.

c. Beispiel Übersetzer

[Rz 36] Ein weiteres Beispiel ist der externe Übersetzer von Texten im Auftrag seiner Kunden. Soweit in den Texten Personendaten enthalten sind und es daher auch seitens des Übersetzers zu einer Bearbeitung solcher kommt, bestimmt der Kunde die Zwecke der Datenbearbeitung. Er veranlasst sie und bestimmt damit den Zweck, überlässt es jedoch typischerweise dem Übersetzer, mit welchen Datenbearbeitungen er zum Ergebnis kommt. Damit bestimmt der Übersetzer die Art und Weise, wie sie erfolgt. Es ist dem Übersetzer in aller Regel auch freigestellt, die Texte zu behalten, damit er sie allenfalls bei anderen Übersetzungen zur Hilfe nehmen kann; wesentlich ist nur, dass er die Vertraulichkeit wahrt. Diesfalls bestimmt der Übersetzer sogar den Zweck der Bearbeitung mit. In solchen Fällen wird der Übersetzer zur (gemeinsamen) Verantwortlichen.[48] Das Beispiel zeigt jedoch auch, dass diese Qualifikation nicht naturgegeben ist: Sie ergibt sich aus den tatsächlichen Verhältnissen, nämlich, dass Kunden von professionellen Übersetzungsbüros deren Datenbearbeitungen – anders als etwa bei der Speicherung von Daten bei einem Hosting-Anbieter – nicht als ihre eigene Datenbearbeitung betrachten und sie diese Büros daher auch nicht kontrollieren wie ein Auftragsbearbeiter; die Kunden interessiert nur der abgelieferte Text, nicht, was innerhalb der Sphäre des Dienstleisters passiert und ob er den Text auch für eigene Zwecke benutzt, solange die Personendaten dort bleiben, wo sie sind. Ebenso betrachten sich die Übersetzungsbüros nicht als Auftragsbearbeiter.

[Rz 37] Es wäre freilich denkbar, dass ein Kunde einen Übersetzer auch wesentlich enger kontrolliert und ihm genaue materiell-rechtliche Vorgaben zur Datenbearbeitung macht, ihm die Nutzung zu eigenen Zwecken untersagt und ihn so zu seinem Auftragsbearbeiter werden lässt, weil der Übersetzer in den entscheidenden Punkten nicht die erforderliche Autonomie hat, um Verantwortlicher zu sein. Integriert der Kunde den freischaffenden Übersetzer gar in seine Organisation, so dürfte er von Art. 29 DSGVO erfasst sein (Rz. 104 ff.). Ganz anders sind die faktischen Verhältnisse und die Erwartungen bzw. das Kontrollbedürfnis der Kunden, wenn ein Unternehmen keine Übersetzungen anbietet, sondern lediglich den Betrieb einer Übersetzungssoftware. Instinktiv gehen hier alle Beteiligten von einer Auftragsbearbeitung aus, weil sie *wollen*, dass der Kunde in der Verantwortung und die Datenbearbeitung in der Sphäre des Kunden bleibt: Zwar definiert der Anbieter, was die Software kann und wie sie funktioniert, aber der Kunde entscheidet sich für dieses definierte Paket und benutzt es, um seine Texte bearbeiten zu lassen. Er bestimmt damit auch die Mittel der Bearbeitung. Immerhin kann auch dieser Service so ausgestaltet sein, dass der Dienstleister Verantwortlicher ist, etwa, wenn er die Texte des Kunden für das Training seiner Software (und damit für einen eigenen Zweck) einsetzen möchte. Der Vertrag

48 Wobei aufgrund der Verhältnisse klar ist, dass für die Einhaltung der Betroffenenrechte der Kunde verantwortlich sein wird. Davon gehen auch die betroffenen Personen aus.

muss dann differenzieren. Diese Beispiele zeigen erneut, dass die Frage, wer Auftragsbearbeiter ist und wer nicht, sich nicht zwingend aus der Natur der Datenbearbeitungen oder Dienstleistungen ergibt, sondern wesentlich aus dem Bedürfnis des Kunden ergibt, eine Datenbearbeitung kontrollieren zu können – oder lediglich ihr Ergebnis nutzen. Letztlich zählen die gelebten Verhältnisse. Ein weiteres solches Beispiel ist die Abgrenzung zwischen Fernmeldedienstanbieter und Hosting-Provider (dazu Rz. 82 ff. und Fn. 100).

d. Wer hat faktisch das Sagen?

[Rz 38] Auch der Anwalt, der in diesem Sinne für seinen Klienten den Datenraum nicht nur betreibt, sondern bei der Ausgestaltung der damit verbundenen Datenbearbeitungen aufgrund seines Know-hows freie Hand hat, ist nicht mehr nur Auftragsbearbeiter, sondern Verantwortlicher. Dasselbe gilt für das Meinungsforschungsinstitut, das zwar im Auftrag des Unternehmens eine Umfrage zur Kundenzufriedenheit oder Markenbekanntheit durchführt, aber als der Profi im Wesentlichen selbst festlegt, wie es dies tut. Wo somit ein Experte für einen Kunden aufgrund seines Fachwissens eine Datenbearbeitung bezüglich der datenschutzrechtlich relevanten Parameter ausgestaltet (dazu Rz. 49) und der Kunde ihm nicht «Dreinreden» will, liegt in vielen Fällen eine gemeinsame Verantwortlichkeit vor, auch wenn der Kunde bezüglich der Datenbearbeitung das letzte Wort haben mag.[49]

[Rz 39] Im Falle der beauftragten Marktforschung wird das Unternehmen unter Umständen sogar vertraglich festschreiben wollen, dass es nie Zugang zu den Aussagen der einzelnen befragten Personen haben will, weil dies den Teilnehmern zugesichert wurde. Dies ist in der Praxis ein weiteres wichtiges Indiz dafür, dass die Stelle, die die Datenbearbeitung faktisch kontrolliert, Verantwortlicher sein muss, weil sonst die Wahrung der Betroffenenrechte und des Datenschutzes nicht sichergestellt ist, was wiederum das ultimative Ziel der Verantwortlichkeitsordnung des Datenschutzes ist. Wie im Falle der klinischen Studie verorten auch bei der Marktforschung die Teilnehmer die Verantwortlichkeit für den Umgang mit ihren Daten primär beim Institut, das die Studie durchführt und nicht beim den Auftrag gebenden Unternehmen. Wer gefühlt der Verantwortliche ist, ist es in aller Regel auch rechtlich.

e. Relevanz des Zugangs zu den Personendaten

[Rz 40] Eine andere, damit verbundene Frage ist, ob ein Verantwortlicher überhaupt Zugang zu den Personendaten «seiner» Datenbearbeitung haben muss (zum Fall der gemeinsamen Verantwortlichkeit vgl. Rz. 72). Aus dem Begriff des Verantwortlichen ergibt sich das nicht: Weder E-DSG noch DSGVO verlangen, dass der Verantwortliche die Daten selbst bearbeitet. Zur Figur des Verantwortlichen gehört einzig, dass er über den Zweck und die wesentlichen Mittel einer Datenbearbeitung befindet. Die Durchführung der Datenbearbeitung selbst kann er an einen Auftragsbearbeiter delegieren, ebenso die Datenschutz-Compliance wie z.B. die Erfüllung der Betroffenenrechte. Er kann auch mehrere Auftragsbearbeiter oder weitere Personen einsetzen, die für ihn die nötigen Kontrollen und Aufsichtsfunktionen im operativen Betrieb vornehmen, und mit Hilfe von Dritten die Rücknahme der Daten lösen. Er kann sich von seinem Dienstleister

49 WP169 (Fn. 13), S. 35.

sogar versprechen lassen, ihm keinen Einblick in die Personendaten zu geben (Beispiel: Das Meinungsforschungsinstitut, das eine vertrauliche Mitarbeiterbefragung im eigenen Unternehmen durchführt, d.h. die Unternehmensleitung nicht sehen soll, was die Mitarbeiter gesagt haben). Da dem Verantwortlichen aber – wie dem Verwaltungsrat eines Unternehmens – die Oberaufsicht über die Datenbearbeitung obliegt, wird er sich gegenüber seinen Auftragsbearbeitern trotz allem vorbehalten müssen, ausnahmsweise selbst Zugang zur Datenbearbeitungen zu erhalten: Denn wenn ein Entscheid mit Bezug auf die Datenschutz-Compliance von solcher Tragweite zu fällen ist, dass ihn nur der Verantwortliche selbst gehörig treffen kann, wird er möglicherweise auch selbst sehen müssen, worum es geht (z.B. für eine Interessenabwägung). Ein solcher Datenzugang ist aber *keine* begriffliche Voraussetzung eines Verantwortlichen, sondern «nur» eine Sorgfaltspflicht bzw. Regelung für einen ADV.[50] Auch eine Stelle, die *keinen* Zugang zur Datenbearbeitung selbst hat, sie aber in relevanter Weise steuert, wird zur Verantwortlichen, denn sonst könnte der Datenschutz unterlaufen werden.

9. Wenn der Dienstleister «entscheidet» und trotzdem Auftragsbearbeiter ist

a. Standardisierung von Dienstleistungen

[Rz 41] Das Kriterium der Kontrolle über die Durchführung der Datenbearbeitung weicht in der Praxis insofern auf, als dass selbst im Rahmen einer Auftragsbearbeitung es oft der Dienstleister ist, der vorgibt, was der Kunde mit seinen Daten tun kann, d.h. welche Datenbearbeitungen durchgeführt werden können. Der Umstand, dass ein Dienstleister sein Serviceangebot selbst definiert und womöglich sogar allen Kunden standardisiert anbietet, bedeutet allerdings nicht, dass er damit Verantwortlicher ist. Solange es nach wie vor die Kunden sind, die entscheiden, ob sie seinen Service zur Umsetzung *ihrer* Datenbearbeitung einsetzen wollen, entscheiden sie über die Art und Weise, wie sie erfolgt. Es ist wie mit der Menükarte im Restaurant: Die Küche bietet eine vordefinierte Auswahl an Gerichten an, die Köche bereiten ein Gericht aber jeweils für den einzelnen Gast zu und er wählt es aus. Das Restaurant ist der Provider in der Cloud, der für seine Kunden zum Beispiel Mailserver in verschiedenen Farben und Formen anbietet, und der Kunde entscheidet, in welcher Ausprägung er einen solchen für ihn betreiben soll. Der Provider wird zu dessen Auftragsbearbeiter, obwohl der Provider nur tut, was er sich im Rahmen seines Serviceangebots selbst ausbedungen hat. Daran muss er sich allerdings halten; ein «Menu Surprise» gibt es nicht – es würde ihn sonst zum Mit-Verantwortlichen machen.

[Rz 42] Der Kunde kann in diesen Fällen zwar die Art und Weise, wie der Provider seinen Service erbringt, nicht ändern, aber er kann ihn künden und zu einem anderen Anbieter wechseln. Auf diese Weise kontrolliert er in den datenschutzrechtlich wesentlichen Punkten wie «sein» Mailserver betrieben wird (was die wesentlichen Punkte sind, die zwingend vom Verantwortlichen entschieden werden müssen, dazu sogleich in Rz. 48 ff.). Diese sehr beschränkte Entscheidungsmöglichkeit des Kunden genügt nach herrschender Ansicht, um als (alleiniger) Verantwortlicher

50 So verlangt Art. 28 Abs. 3 Bst. e, f und h DSGVO für einen ADV, dass der Auftragsbearbeiter dem Verantwortlichen auf Verlangen alle erforderlichen Informationen zum Nachweis der Einhaltung der Datenschutz-Compliance gegeben werden und er ihn bei der Einhaltung der eigenen Pflichten unterstützt.

zu gelten bzw. der Provider nicht auch Verantwortlicher ist;[51] weder DSGVO noch E-DSG verlangen, dass ein Verantwortlicher die Art und Weise seiner Datenbearbeitung beliebig gestalten können muss, solange das von ihm genutzte Standardangebot des Dienstleisters den datenschutzrechtlichen Vorgaben entspricht, was wiederum Sache des Kunden, und nicht des Providers ist.

[Rz 43] Basierend auf diesem Gedanken wird auch das dem Standardisierungswunsch des Providers entgegenstehende Weisungsrecht des Kunden und dessen Recht, Unterbeauftragte abzulehnen, in der Praxis gelöst: Das Weisungs- und Ablehnungsrecht besteht zwar formal, faktisch sind die Hürden aber sehr hoch. Im ADV wird festgehalten, dass die Servicebeschreibung des Providers, die vertraglichen Vorgaben und etwaige vom Kunden vorgenommenen Konfigurationen die abschliessenden und verbindlichen Weisungen des Kunden darstellen. Will er seine Weisungen ändern und ist der Provider dazu nicht bereit, muss der Kunde künden. Weiter wird festgehalten, dass der Kunde im Falle des Beizugs eines neuen Unterauftragsbearbeiters lediglich das Recht hat, aus dem Vertrag auszusteigen bzw. seine Daten zu löschen. Diese Kontrollmöglichkeiten seitens des Kunden genügen nach herrschender Auffassung, um den gesetzlichen Vorgaben an einen ADV gerecht zu werden: Die Kontrolle bleibt so zwar beim Kunden, aber seine einzige Kontrollmöglichkeit ist letztlich die Notbremse.[52] Die meisten Cloud-Provider wie Microsoft, Amazon oder Google operieren heute auf dieser Basis, wenn sie ihre Dienstleistungen als Auftragsbearbeiter den Unternehmen anbieten.

[Rz 44] Ob das Angebot eines Dienstleisters, der seinen Kunden eine standardisierte Auftragsbearbeitung anbietet, das einzige im Markt ist und Kunden somit gar keine Wahl haben, ein anderes zu benutzen und die Datenbearbeitung womöglich auch nicht selbst vornehmen könnten, weil ihnen das Know-how oder die Mittel fehlen, spielt keine Rolle. Entscheidend ist, dass es der Kunde ist, der die Durchführung seiner vertraglich in den wesentlichen Elementen vordefinierte Datenbearbeitung durch den Dienstleister veranlasst,[53] indem er den Vertrag abschliesst oder die Bearbeitung beendet, indem er ihn kündet. Auch das japanische Spitzenlokal, das als einziges auf der Welt den giftigen Kugelfisch in einer bestimmten Art und Weise zubereitet, tut dies im Auftrag des Gasts, der den Fugu bestellt. Was auf den Teller kommt, gehört dem Gast. So ist das Unternehmen, das für alle Spitäler in der Schweiz in einem bestimmten Fachbereich die Falldaten auf seinen Rechnern speichert, damit sie der Forschung in standardisierter Form zugänglich sind, typischerweise ein Auftragsbearbeiter: Ob ein Spital die Dienste des Unternehmens in Anspruch nimmt und in welcher Form (z.B. anonymisiert oder nicht anonymisiert) es die Daten zur Verfügung stellt, entscheidet ausschliesslich das Spital, indem es auf einem standardisierten Formular seine Weisungen durch Ankreuzen der entsprechenden Felder erteilt, die

51 WP169 (Fn. 13), S. 32 sowie Fussnote 18, wonach die Ausarbeitung der Vertragsbedingungen durch den Dienstleister nicht die Tatsache berührt, dass der Verantwortliche über wesentliche Aspekte der Bearbeitung entscheidet. Umgekehrt wird betont, dass ein Ungleichgewicht in der Vertragsposition es dem (kleinen) Kunden, der die Vertragsbedingungen nicht aushandeln kann, nicht berechtigt, eine datenschutzwidrige Vereinbarung abzuschliessen, weil er Verantwortlicher bleibt. Er muss diesfalls auf den Abschluss verzichten (vgl. Beispiel 18 zur E-Mail-Plattform in WP169).

52 Vgl. etwa die Online Service Terms (OST) von Microsoft (https://www.microsoft.com/en-us/licensing/product-licensing/products): «Microsoft wird personenbezogene Daten nur auf Basis dokumentierter Anweisungen des Kunden verarbeiten. Der Kunde erklärt sich damit einverstanden, dass seine Volumenlizenzvereinbarung (einschließlich der OST) zusammen mit der Nutzung der Professional Services durch den Kunden die vollständigen und endgültig dokumentierten Anweisungen des Kunden an Microsoft für die Verarbeitung personenbezogener Daten sind. Zusätzliche oder andere Weisungen müssen in Übereinstimmung mit dem Verfahren zur Änderung des Volumenlizenzvertrages des Kunden vereinbart werden.» (Stand vom April 2019).

53 Die im Vertrag bereits in ihren wesentlichen Elementen vordefinierte Datenbearbeitung unterscheidet diesen Fall etwa vom Mandat, das einem Anwalt erteilt wird. Es definiert die Datenbearbeitungen nicht.

sie jederzeit ändern können. Die Daten «gehören» weiterhin dem Krankenhaus; auch ist es der einzige Ansprechpartner der betroffenen Patienten. Dass der Dienstleister ein Monopol hat, ändert datenschutzrechtlich nichts. Anders wäre es, wenn der Dienstleister die Daten den Spitälern gewissermassen «abkaufen» würde, damit er sie unter eigenem Namen anbieten und in eigener Regie verwerten kann, auch wenn das Spital daran wirtschaftlich beteiligt sein mag und ein gewisses Mitsprache und Kontrollrecht hat; auch diese Modelle gibt es in der Praxis. Diese «unabhängigen» Intermediäre sind dann Verantwortliche.

b. Welche Freiheiten bedingt sich der Auftragsbearbeiter aus?

[Rz 45] In der Praxis kommt es denn auch immer wieder vor, dass Dienstleister zwar von der beschränkten Verantwortlichkeit eines Auftragsbearbeiters profitieren wollen, zugleich aber auch von den «Freiheiten» eines Verantwortlichen (etwa was die Möglichkeit zur Anpassung der Datenbearbeitungen nach ihren eigenen Vorstellungen oder zur Nutzung der Daten für eigene Zwecke betrifft). Dies ist ein Zielkonflikt, der sich nicht einfach mit dem Abschluss eines ADV lösen lässt. Handelt es sich bei der konkreten Dienstleistung ihrer Natur nach nicht um eine Auftragsbearbeitung (etwa weil der Dienstleister die Daten auch selbst nutzen will, sich andere Freiheiten bezüglich der wesentlichen Aspekte der Datenbearbeitung ausbedingt oder sich gegenüber den betroffenen Personen gegenüber wie ein Verantwortlicher verhält), so ändert daran auch das Vorliegen eines ADV mit Weisungsrecht und die oben erwähnte Möglichkeit der Standardisierung nichts.

[Rz 46] Zudem ist zu prüfen, worauf sich das Weisungsrecht bezieht bzw. was die Weisungen des Kunden umfassen: Geht es um die wesentlichen Mittel der Datenbearbeitung und deren Zwecke oder bloss um andere Aspekte der Datenbearbeitung? Ein Dienstleister wird nicht schon deshalb zum Auftragsbearbeiter, weil er es dem Kunden erlaubt zu bestimmen, von welchen Personen er ihm Personendaten zur Bearbeitung übergibt; das wäre beispielsweise kein Entscheid über die wesentlichen Mittel der Ausgestaltung der Daten*bearbeitung* des Dienstleisters, sondern ein Entscheid über die übergebenen Daten.

[Rz 47] Zu prüfen ist weiter, ob etwaige «standardisierte» Weisungen bzw. der Vertrag tatsächlich alle für die Datenschutz-Compliance wesentlichen Aspekte der Datenbearbeitung abdecken oder nur einige wenige Dinge (z.B. Kategorien von Daten), der Dienstleister in anderen wesentlichen Belangen (z.B. Aufbewahrungsfristen, Quellen von Personendaten) hingegen stillschweigend freie Wahl hat. Nutzt der Dienstleister diese Autonomie und legt er in der Folge in Eigenregie wesentliche Mittel der Datenbearbeitung fest, wird er trotz ADV zum Mit-Verantwortlichen. Dasselbe gilt übrigens regelmässig dann, wenn Personendaten des Kunden auch für seine eigenen Zwecke bearbeitet, selbst wenn diese nicht personenbezogen sind (dazu Rz. 51).

c. Welche Entscheide an den Auftragsbearbeiter delegiert werden dürfen

[Rz 48] Anerkannt ist immerhin, dass ein Verantwortlicher gewisse Entscheide über die Art und Weise, wie seine Datenbearbeitung durchzuführen ist, an den Auftragsbearbeiter delegieren darf

ohne diesen zum Verantwortlichen zu machen.[54] Wesentlich ist, dass der Verantwortliche den Rahmen vorgibt, den der Auftragsbearbeiter dann mit seinem Fachwissen und der Nähe zur Sache ausfüllt. Auch hier hilft die Analogie zum Restaurant: Welches Gericht die Küche für ihn zubereitet, bestimmt der Gast, aber dem Koch bleibt trotz allem ein erheblicher Spielraum es auszugestalten. Ein typisches Beispiel sind die Massnahmen zur Datensicherheit. Das Schweizer Recht verlangt nicht, dass die einzelnen Massnahmen vereinbart werden. Ein ADV nach den Standards der DSGVO muss zwar üblicherweise eine grobe Umschreibung der Massnahmen enthalten, aber dem Auftragsbearbeiter darf es erlaubt werden, sie einseitig an geänderte Umstände anzupassen, soweit das Schutzniveau erhalten bleibt. Ein weiteres Beispiel sind Fälle, in denen der Kunde zwar im Wesentlichen vorgibt, wie die Daten zu bearbeiten sind, die Wahl der dazu benutzten Software und deren Konfiguration im Detail ist aber dem Dienstleister überlassen.

[Rz 49] Wo genau die Grenze verläuft, ist freilich nicht immer klar. Orientierungs- und Argumentationshilfe kann hier wieder der Grundgedanke sein, dass die Figur des Verantwortlichen dazu dient, eine Ansprechperson für die Sicherstellung des Datenschutzes zu haben. Entscheidungen über inhaltliche Fragen, die den Kern der Rechtmässigkeit der Bearbeitung wesentlich betreffen, sind dem Verantwortlichen vorbehalten.[55] Gemeint ist damit, wie bereits weiter vorne erwähnt, die Festlegung der datenschutzrechtlich relevanten Parameter einer Datenbearbeitung, also z.B. welche Datenkategorien bearbeitet, von wem sie wie und wo beschafft, wem sie weitergegeben und wie lange sie aufbewahrt werden oder ob sie ins Ausland gehen.[56] Steckt der Kunde diesbezüglich den Rahmen ab, und sei es auch nur abstrakt[57] oder durch die Vorgabe eines gewissen Zwecks, aus dem sich die Parameter ergeben (z.B. Einhaltung einer bestimmten Gesetzesnorm, die definiert, was an Daten wie zu bearbeiten ist), so bleibt allein der Kunde in der Verantwortlichkeit.[58] Dementsprechend machen Entscheide zu den technischen und organisatorischen Mitteln der Datenbearbeitung, d.h. wie die Einhaltung der datenschutzrechtlich relevanten Parameter sicherzustellen oder wie sie umzusetzen zu sind, den Auftragsbearbeiter noch nicht zum Mitverantwortlichen.[59] Auch dies kommt den Cloud-Providern entgegen und erlaubt ihnen, im Unternehmensgeschäft Auftragsbearbeiter zu bleiben, auch wenn sie bestimmen, welche Software zum Einsatz kommt und wie sich diese weiterentwickelt. Verlangt wird immerhin, dass der Kunde darüber mindestens in groben Zügen informiert ist,[60] denn ein Auftragsbearbeiter kann letztlich nur derjenige sein, der unter der Kontrolle eines Verantwortlichen tätig wird. Handelt er faktisch mit weitgehender Autonomie, wird er zum Mitverantwortlichen (Rz. 38). Cloud-Anbieter müssen darum dafür sorgen, dass datenschutzrechtlich relevante Anpassungen ihrer Lösungen (z.B. neue Funktionalitäten), die sie den Unternehmenskunden als Auftragsbearbeiter zur Verfügung stellen, von diesen kontrolliert werden können (z.B. als Option oder über

54 WP169 (Fn. 13), S. 16 ff.

55 WP169 (Fn. 13), S. 18.

56 WP169 (Fn. 13), S. 39, welche von den «materiellrechtlichen» Fragen spricht.

57 Hinreichend wäre z.B., wenn der Kunde den Auftragsbearbeiter anweist, die Daten nach Ablauf der gesetzlichen Aufbewahrungs- und Verjährungsfrist zu löschen, während der Auftragsbearbeiter bestimmen muss, nach wie vielen Jahren das der Fall ist.

58 WP169 (Fn. 13), S. 16 unten und S. 18 oben.

59 WP169 (Fn. 13), S. 17 unten.

60 WP169 (Fn. 13), S. 34, welche von der Information über «die beteiligten Akteure, Sicherheitsmassnahmen, Gewähr hinsichtlich der Verarbeitung in Drittländern, usw.» spricht.

deren Konfiguration) oder sie sonst vertraglich vereinbart sind (wenn auch nur auf Basis einer Änderungskündigung).

d. Wenn der Auftragsbearbeiter sich nicht an den ADV hält

[Rz 50] Hält sich der Auftragsbearbeiter hingegen nicht an die Weisungen des Kunden oder den Vertrag, selbst wenn die resultierte Datenbearbeitung datenschutzkonform sein sollte, wird er automatisch zum Verantwortlichen; es muss wie bereits mehrfach erwähnt immer sichergestellt sein, dass jemand für die getroffenen Entscheide verantwortlich ist.[61] Wenn der Auftragsbearbeiter die Daten seines Kunden somit länger als vereinbart aufbewahrt oder mehr (oder auch weniger) Daten erhebt, als der Kunde angewiesen hat oder vertraglich vereinbart ist, wird der Auftragsbearbeiter diesbezüglich zum Mit-Verantwortlichen.

[Rz 51] In diese Kategorie fällt auch der Dienstleister, der Personendaten aus der Auftragsbearbeitung für seinen Kunden auch für eigene Zwecke verwendet oder im Rahmen der Auftragsbearbeitung eigene Personendaten erhebt. Während der Einfluss eines Auftragsbearbeiters auf die Mittel der Bearbeitung wie gezeigt von einer gewissen Erheblichkeit sein muss, um ihn zum Verantwortlichen zu machen, genügt hinsichtlich der Zweckbestimmung bereits wenig (wie das selbstbestimmte Zufügen eines weiteren Zwecks), damit jemand zum (Mit-)Verantwortlichen wird. Die Artikel-29-Datenschutzgruppe erwähnt hier das Beispiel eines Werbedienstleisters, der die Adressdaten seines Kunden auch für Werbung seiner anderen Kunden nutzt.[62] Es ist hier allerdings eine Differenzierung nötig: Tut der Werbedienstleister dies aus eigenem Antrieb ohne sich mit dem Kunden abzusprechen, so wird er bezüglich der Sondernutzung zum Verantwortlichen. Vereinbart der Werbedienstleister dies jedoch mit dem Kunden, so sind beide Konstellationen denkbar. Hier ist es entscheidend, wer faktisch bestimmt: Wird der Werbedienstleister beauftragt, die Daten seinen anderen Kunden zugänglich zu machen, weil der Kunde selbst etwas davon hat, so bleibt der Kunde für die Weitergabe weiterhin der alleinige Verantwortliche (und der Dienstleister nimmt die Daten im Auftrag der anderen Kunden für diese entgegen). Erteilt der Kunde dem Dienstleister jedoch bloss die Erlaubnis, die Daten auch anderweitig zu nutzen, und sei es, um einen Preisnachlass zu erhalten, so wird der Dienstleister zum Verantwortlichen. Es ist in diesem Fall «sein» Zweck.

10. Auftragsbearbeiter und Verantwortlicher in einem

a. Dieselbe Datenbearbeitung in zwei Ausprägungen

[Rz 52] Genügt einem Dienstleister die Gestaltungsfreiheit seiner «Menükarte» nicht, steht es ihm frei, seine Dienstleistung als Verantwortlicher auszugestalten. Google bietet den Betrieb eines Mailservers beispielsweise sowohl als Auftragsbearbeitung an («G-Suite» für Unternehmen) als auch als öffentlicher Gratis-Mail-Dienst, für welchen der Konzern als Verantwortlicher zeichnet («Gmail»). In beiden Fällen entscheidet der Kunde, ob er die Dienstleistung nutzt und wie lange, und in beiden Fällen ist die technische Infrastruktur und die Funktionalität jedenfalls aus

61 WP169 (Fn. 13), S. 31.

62 WP169 (Fn. 13), S. 18, Beispiel 3.

datenschutzrechtlicher Sicht vergleichbar; E-Mails lassen sich versenden und empfangen, der Benutzer kann einen Kalender führen und seine Kontakte speichern. Im Falle der Gratis-Mail-Version betreibt Google den Mailserver im eigenen Namen und legt in eigener Regie fest, wie er betrieben wird und kann dies auch jederzeit ändern. Im Falle von G-Suite sind es die einzelnen Unternehmenskunden, die entscheiden, ob Google einen solchen Dienst für sie betreiben soll und in welcher Konfiguration. Wer ihn wie nutzen darf, entscheidet daher im ersteren Fall Google, im letzteren Fall das Unternehmen. Die unterschiedlichen Rollen, die der Dienstleister einnimmt, spiegeln sich auch in seinen Datenschutzerklärungen bzw. -verträgen wieder.[63] Der wirtschaftliche Grund für diese Zweiteilung liegt darin, dass viele Unternehmen aus datenschutzrechtlichen Gründen nie den Betrieb ihres Mailservers einem anderen Verantwortlichen überlassen würden, weil er Dritter ist und sie ihn zu wenig kontrollieren könnten.[64] Hinzu kommt, dass Google, soweit ihre Kunden natürliche Personen sind, mit Bezug auf deren Daten Verantwortlicher sein muss (Rz. 26).

b. Nebenleistungen, für welche der Dienstleister Verantwortlicher ist

[Rz 53] In der Praxis ist allerdings zu beachten, dass auch in den Fällen einer Auftragsbearbeitung der Dienstleister in gewissen Bereichen trotz allem auch Verantwortlicher ist. Dies liegt daran, dass die Stellung des Dienstleisters als Verantwortlicher für jede seiner Datenbearbeitungen separat ermittelt werden muss. Die Hauptleistung des Dienstleisters mag im Betrieb eines Mailservers bestehen, doch um sie erbringen zu können, sind jedoch weitere Datenbearbeitungen nötig, die der Dienstleister selbst kontrolliert und für die er als Verantwortlicher gilt.

[Rz 54] Im genannten Beispiel führt der Dienstleister etwa eine Datenbank derjenigen Mitarbeiter des Kunden, die berechtigt sind, Anpassungen an der Konfiguration der Dienstleistung vorzunehmen. Bietet er seine Leistung in der Cloud bzw. als Software-as-a-Service an, so liegen die Datenbearbeitungen im Zusammenhang mit den Administratorenkonten des Kunden in der Verantwortlichkeit des Dienstleisters – er bestimmt, wie seine Kunden seine Dienstleistung online verwalten können, welche Daten er von diesen benötigt (Benutzernamen, Passwörter, Zugriffsberechtigungen). Er ist auch Verantwortlicher bezüglich der Datenbearbeitungen zum Zwecke der Störungsbehebung (z.B. in Form des Trouble-Ticket-Systems) oder zum Zwecke der Rechnungsstellung. Darum ist bei der Formulierung eines ADV auch darauf zu achten, dass diese Datenbearbeitungen von dessen Regelungen nicht erfasst werden, obwohl auch sie die Bearbeitung von Personendaten des Kunden beinhalten (z.B. welche seiner Mitarbeiter in welcher Weise wie seine Dienstleistungen nutzen oder anpassen dürfen oder dies tatsächlich tun). Diese Datenbearbeitungen sind von jenen abzugrenzen, die der Dienstleister im Namen des Kunden erbringt (z.B. welche seiner Mitarbeiter ein Postfach auf dem vom Dienstleister für den Kunden betriebenen Mailserver haben).

[Rz 55] Bezüglich der vom Dienstleister als Verantwortlicher betrieben Datensammlungen treffen ihn selbstverständlich alle gesetzlichen Pflichten direkt, wie beispielsweise die Informations-

63 Seinen Unternehmenskunden bietet Google daher einen ADV an (https://gsuite.google.com/terms/dpa_terms.html?), während die Nutzer des Gratis-Dienstes keinen solchen erhalten und sich Google in der Datenschutzerklärung als für die Datenbearbeitung Verantwortlicher ausweist (https://policies.google.com/privacy?hl=en&gl=CH).

64 Vgl. WP169 (Fn. 13), S. 32, Beispiel 18.

pflicht und Erfüllung der weiteren Betroffenenrechte, die Notwendigkeit einer Rechtsgrundlage im Falle der DSGVO und die Einhaltung der Bearbeitungsgrundsätze. Die meisten Verträge mit Dienstleistern, die als Auftragsbearbeiter tätig sind, adressieren diesen Aspekt heute nicht. In der Praxis führt dies allerdings aus Opportunitätsgründen kaum zu Problemen. Immerhin wäre es sinnvoll, in solchen Fällen die Bestimmungen eines ADV um eine Klausel zu ergänzen, die für den Fall, dass der Dienstleister als Verantwortlicher auftritt, der Kunde die Verantwortung übernimmt, dass er seine Mitarbeiter und anderen Personen, dessen Daten der Dienstleister in eigener Verantwortung bearbeitet, über diesen Umstand informiert (z.B. durch Vorlage der Datenschutzerklärung des Dienstleisters) und dafür verantwortlich ist, dass der Kunde die für die Bearbeitung durch den Dienstleister allenfalls erforderlichen Einwilligungen oder sonstigen Rechtsgrundlagen[65] sicherstellt. Bietet der Dienstleister seine Dienstleistung online an bzw. wird die Serviceleistung über eine Online-Schnittstelle administriert, kann er diese nutzen, um die betroffenen Mitarbeiter und Dritten direkt über seine Datenbearbeitungen zu informieren und allenfalls erforderliche Einwilligungen einzuholen. Diese, von ihm in eigener Verantwortung bearbeiteten Daten sind – mangels anderweitiger Absprache – auch nicht von der bei einem ADV erforderlichen Datenrückgabepflicht am Ende des Auftrags abgedeckt.

c. Relevanz der Aufschaltung einer Datenschutzerklärung

[Rz 56] In der Praxis kann die Frage auftauchen, wie sich die Publikation einer Datenschutzerklärung durch einen Dienstleister mit seiner Rolle als Auftragsbearbeiter verträgt. Sie steht einer Qualifikation als Auftragsbearbeiter nicht entgegen, solange der Dienstleister nicht selbst die Verantwortung für die im Auftrag des Kunden durchgeführte Datenbearbeitung beansprucht, indem er sich etwa als deren (Mit-)Verantwortlicher im Sinne der DSGVO oder des E-DSG ausgibt. Tut ein Auftragsbearbeiter dies, dürfte regelmässig eine Verletzung des anwendbaren Datenschutzrechts vorliegen, indem er die betroffene Person über die Verhältnisse der Datenbearbeitung täuscht, an welcher er mitwirkt. Im Ergebnis lässt er sich die beanspruchte Verantwortung in aller Regel mit anrechnen. Hingegen ist es unproblematisch, ja sogar sinnvoll, wenn auch der Auftragsbearbeiter gegenüber den betroffenen Personen für Transparenz und klare Verhältnisse mit Bezug auf die sie betreffenden Datenbearbeitungen sorgt. Er darf dies aus eigenem Antrieb tun (es ist dies keine Datenbearbeitung), er kann dies aber auch im Namen und Auftrag eines Kunden oder sogar aller seiner Kunden tun. Ist der Dienstleister sowohl Verantwortlicher als auch Auftragsbearbeiter, ist auch eine gemeinsame Datenschutzerklärung möglich[66] – solange für die betroffenen Personen klar ist, wer wofür verantwortlich ist.

---

65 Soweit der Dienstleister von seinem Kunden zwecks Erfüllung der Auftragsbearbeitung oder sonstigen Erbringung seiner Dienstleistung Personendaten seiner Mitarbeiter benötigt (in deren Eigenschaft als Hilfspersonen des Kunden), wird dies durch den Rechtsgrund der Abwicklung des Arbeitsvertrags der betreffenden Personen gedeckt sein (Art. 6 Abs. 1 Bst. b DSGVO), indem der Dienstleister mit seiner Leistungserbringung an den Arbeitgeber dem Arbeitgeber als Vertragspartner des Mitarbeiters zugerechnet wird (damit der Arbeitgeber die Arbeitsleistung seines Mitarbeiters nutzen kann, muss er in der Lage sein, seinen eigenen Kunden und Lieferanten die Namen seiner Mitarbeiter mitteilen zu können). Soweit besondere Kategorien von Personendaten bearbeitet werden, erfordert dies jedoch regelmässig eine ausdrückliche Einwilligung der Mitarbeiter (Art. 9 Abs. 2 Bst. a DSGVO).

66 Ein Beispiel ist Datasport, die Zeitmessungen bei Wettkämpfen durchführt und dabei einerseits Daten als Verantwortlicher bearbeitet, andererseits aber auch als Auftragsbearbeiter für die Wettkampfveranstalter, die in aller Regel über keine eigene Datenschutzerklärung verfügen und diese Aufgabe daher an Datasport delegieren: https://www.datasport.com/de/datenschutzerklaerung/.

11. Eigenständige und gemeinsame Verantwortliche

[Rz 57] Die grösste Herausforderung in der Praxis sind jene Fälle, in welchen nicht nur der Kunde, sondern auch sein Dienstleister als Verantwortlicher gilt. Dabei können sich die jeweiligen Datenbearbeitungen des Kunden und des Dienstleisters bloss an ihren Schnittstellen «berühren» oder der Kunde und der Dienstleister sind – von aussen betrachtet – an ein und derselben Datenbearbeitung beteiligt.[67] Der letzte Fall – die Rede ist von *gemeinsam* Verantwortlichen oder «Joint Controllern» – stellt besondere Herausforderungen. Art. 26 DSGVO verlangt in solchen Fällen ausdrücklich den Abschluss eines Vertrags, der die Aufteilung der Verantwortlichkeit unter den gemeinsamen Verantwortlichen regelt (Rz. 67 ff.).

[Rz 58] Der erste Fall – der der *eigenständigen* Verantwortlichen – ist die in den Rechtsfolgen einfachere der beiden Konstellationen: Eine eigenständige Verantwortlichkeit liegt vor, wenn der Dienstleister alleine für die Datenbearbeitungen im Rahmen seiner Dienstleistungen verantwortlich ist, d.h. dass er selbst sowohl das Ziel seiner Datenbearbeitungen definiert wie auch über deren Art und Weise der Durchführung bestimmt. Die Versicherung, die von ihrem Unternehmenskunden Personendaten zu den zu versichernden Angestellten erhält, ist ein Beispiel, ebenso die Bank, die für ihren Kunden einen Zahlungsauftrag ausführt und dazu von ihm den Namen des Empfängers erhält (Rz. 31). In diesen Fällen gibt ein Verantwortlicher Personendaten Dritter an einen anderen Verantwortlichen weiter. Dies wird auch als «Controller-Controller-Transfer» bezeichnet, in Anlehnung an die englischsprachige Bezeichnung für den Verantwortlichen. Der Kunde betreibt eine Datenbearbeitung, während der Dienstleister seine eigene Datenbearbeitung betreibt. Die Daten wandern von der einen Datenbearbeitung zur anderen.

12. Herausforderungen von Controller-Controller-Transfers

a. Von Gesetzes wegen ist kein Vertrag erforderlich

[Rz 59] Weder E-DSG noch DSGVO schreiben für einen Controller-Controller-Transfer den Abschluss eines Vertrags vor. Das gilt jedenfalls solange sich beide Controller innerhalb eines Staats mit einem angemessenen gesetzlichen Datenschutzniveau befinden, also etwa bei Übermittlungen innerhalb des EWR und der Schweiz. Ist das nicht der Fall und liegt keiner der gesetzlichen Ausnahmen vor,[68]so muss ein angemessener Datenschutz der Daten auf vertraglichem Wege sichergestellt sein, wozu in der Praxis (auch in der Schweiz) meist auf die Standardvertragsklauseln der Europäischen Kommission zurückgegriffen wird.[69]

[Rz 60] Trotzdem sind bei Controller-Controller-Transfers zwei Aspekte zu berücksichtigen: Erstens die Anforderung der Zweckkompatibilität und Rechtsgrundlage, und zweitens andere Gründe dafür, trotz allem einen Vertrag auch bei Controller-Controller-Transfers abzuschliessen.

---

67 Die Artikel-29-Datenschutzgruppe spricht von einer «Vorgangsreihe» und unterscheidet zwischen einer Betrachtung der Mikro- und Makroebene, wobei letztere die relevante sein soll (WP169 [Fn. 13], S. 25).

68 Art. 6 Abs. 2 DSG, Art. 49 DSGVO.

69 EDÖB, Übermittlung ins Ausland, https://www.edoeb.admin.ch/edoeb/de/home/datenschutz/handel-und-wirtschaft/uebermittlung-ins-ausland.html.

b. Die Anforderung der Zweckkompatibilität und Rechtsgrundlage

[Rz 61] Die Bekanntgabe von Personendaten eines Verantwortlichen an einen anderen, selbstständigen[70] Verantwortlichen stellt anders als im Falle der Bekanntgabe an einen Auftragsbearbeiter datenschutzrechtlich eine Bekanntgabe an einen Dritten dar.[71] Eine solche ist unter dem DSG und der DSGVO grundsätzlich nur erlaubt, wenn der Zweck der Bekanntgabe im Rahmen der Beschaffung der Personendaten für die betroffenen Personen erkennbar war bzw. sie jemand darüber informiert hat (z.B. mit einer Datenschutzerklärung). Wenn ein Unternehmen den betroffenen Personen verspricht oder erklärt, dass es die von ihnen erhaltenen Daten nur für «eigene Zwecke» benutzt oder «nicht Dritten mitteilt», so ist ein Controller-Controller-Transfer auf den ersten Blick ausgeschlossen und würde den Zweckbindungsgrundsatz[72] verletzen – es sei denn, der Begriff des Dritten wird etwas weniger streng ausgelegt. Sind die betroffenen Personen hingegen informiert, dass ihre Daten auch mit weiteren Stellen wie z.B. Dienstleister oder Berater geteilt werden können, ist der Zweckbindungsgrundsatz nicht verletzt.

[Rz 62] Unter der DSGVO kommt hinzu, dass unabhängig davon für jeden Zweck, zu welchem Personendaten bearbeitet werden (was deren Bekanntgabe mitumfasst), eine Rechtsgrundlage bestehen muss. Sollen also einem anderen Verantwortlichen für *dessen* Zwecke Daten mitgeteilt werden, so benötigen beide Verantwortliche hierzu eine Rechtsgrundlage. Bei nicht sensitiven Daten kann das beispielsweise eine Einwilligung der betroffenen Person sein, die Abwicklung eines Vertrags mit oder im Interesse der betroffenen Person, die Erfüllung einer gesetzlichen Pflicht im EWR oder ein überwiegendes berechtigtes Interesse.[73] Unter dem DSG ist die Regel eine andere und sie ist liberaler: Hier ist ein Rechtfertigungsgrund (im Sinne von Art. 13 DSG) nur aber immerhin dann erforderlich, wenn die Bekanntgabe an den anderen Verantwortlichen den Zweckbindungsgrundsatz verletzt, was davon abhängt, was für die betroffenen Personen im Rahmen der Datenbeschaffung erkennbar war bzw. ihnen mitgeteilt worden ist. Wer frühzeitig korrekt informiert, benötigt diesbezüglich unter Schweizer Recht somit keinen Rechtfertigungsgrund.

[Rz 63] Diese Anforderungen sind denn auch der Grund, warum gerade Unternehmenskunden ihre Dienstleister, denen sie Daten bekanntgeben müssen, gerne als Auftragsbearbeiter qualifizieren: Es erleichtert ihnen das Leben, weil ihnen weder die Einhaltung des Zweckbindungsgrundsatzes noch die Gewährleistung eines Rechtsgrunds Sorgen bereiten muss, solange sich der Dienstleister an den ADV hält. Controller-Controller-Transfers haben allerdings zu Unrecht einen schlechten Ruf: Selbst die DSGVO steht solchen Transfers in vielen der hier relevanten Konstellationen im Zusammenhang mit der Inanspruchnahme von Dienstleistern durch ihre Kunden nicht entgegen. Ist nämlich sichergestellt, dass der Dienstleister die Personendaten trotz seiner Eigenschaft als Verantwortlicher weiterhin ausschliesslich für die Zwecke seines Kunden bearbeitet, kommt es zum Einen nicht zur verpönten Zweckänderung der Datenbearbeitung. Unter der DSGVO kann sich der Dienstleister in diesen Fällen zum Anderen oftmals auch auf denselben Rechtsgrund stützen wie sein Kunde, womit auch die zweite Hürde genommen ist.

---

70 Also nicht gemeinsamen Verantwortlichen; siehe dazu Rz. 80.

71 Vgl. dazu die Definition des Dritten gem. Art. 4 Ziff. 10 DSGVO.

72 Art. 4 Abs. 3 DSG, Art. 5 Abs. 1 Bst. b DSGVO.

73 Art. 6, 9 und 10 DSGVO.

[Rz 64] Nehmen wir den Anwalt als Beispiel: In aller Regel wird er eigenständiger Verantwortlicher sein, weil er alleine über seine Datenbearbeitungen – das Führen seiner Mandatsakten und die Erstellung seiner Arbeitsprodukte – bestimmt, und zwar sowohl bezüglich ihrem Ziel als auch der Art und Weise, wie er sie ausgestaltet. Dennoch dienen die Datenbearbeitungen voll und ganz dem Zweck seines Klienten und nicht seinem eigenen. Datenschutzrechtlich tritt der Anwalt in die Schuhe des Klienten, auch wenn er dies datenschutzrechtlich in eigener Verantwortung tut. Es liegt somit bezüglich der Bearbeitung der vom Klienten erhaltenen oder in seinem Auftrag beschafften Personendaten weder eine Zweckänderung vor, noch wird ein zusätzlicher Rechtsgrund erforderlich. Soll beispielsweise ein Vertrag vor Gericht durchgesetzt werden, so kann sich der Anwalt auf den Rechtsgrund der Vertragsabwicklung berufen, denn er bearbeitet in diesem Fall Personendaten des Vertragspartner seines Klienten, die für die Erfüllung des Vertrags erforderlich sind.[74] Es ist nicht nötig, dass der Anwalt selbst ebenfalls Vertragspartner ist. Er ist zwar datenschutzrechtlich genau genommen «Dritter» (Rz. 61), wird jedoch nach allgemeinem Sprachverständnis nicht als solcher erachtet, wenn die Datenschutzerklärung des Klienten verspricht, dass keine Daten an «Dritte» gehen.

c. Weitere Gründe für eine vertragliche Regelung bei Controller-Controller-Transfers

[Rz 65] Aus den eben dargelegten und weiteren Gründen kann es sinnvoll sein, mit dem Dienstleister einen datenschutzrechtlichen Vertrag abzuschliessen. An sich wäre es nicht erforderlich, die Zweckbindung im Rahmen eines Controller-Controller-Transfers vertraglich festzuschreiben, denn soweit der empfangende Verantwortliche selbst einem angemessenen Datenschutzrecht unterliegt, darf er die erhaltenen Personendaten ohnehin nur für einen zulässigen Zweck bearbeiten, da er selbst genauso an den Zweckbindungsgrundsatz und im Bereich der DSGVO die Notwendigkeit eines Rechtsgrunds gebunden ist, wie der andere Verantwortliche.

[Rz 66] In der Praxis empfiehlt es sich jedoch für Kunden regelmässig, bei Controller-Controller-Transfers zu Dienstleistern deren Befolgung der Zweckbindung und Wahrung der Vertraulichkeit vertraglich absichern zu lassen. Der Dienstleister ist dann zwar verantwortlich gegenüber den betroffenen Personen, darf aber deren Daten trotzdem nur für die Zwecke des Kunden bearbeiten und sie nicht Dritten zugänglich machen. Im Grunde können in einem Controller-Controller-Vertrag sämtliche Regelungspunkte eines ADV aufgenommen werden (vgl. Anhang «*Was in eine ADV gehört*.»). Sogar die Weisungsbefugnis kann insoweit vorgesehen werden, als der Dienstleister nach wie vor selbst für die Einhaltung des Datenschutzes verantwortlich und diesbezüglich nicht weisungsgebunden ist. In der Praxis ähneln solche Controller-Controller-Verträge mit Dienstleistern daher durchaus einem ADV, indem sie die Datensicherheit regeln, Meldepflichten bei Datensicherheitsverletzungen vorsehen (obwohl der Dienstleister selbst einer Meldepflicht gegenüber den Behörden unterliegt), eine Beschränkung des Datenexports und Prüfrechte. Die Motivation hinter solchen Klauseln ist nicht unbedingt das Datenschutzrecht, sondern das wirtschaftliche Interesse, die Kontrolle über die Personendaten nicht an den Dienstleister zu verlieren, und das Interesse an der Wahrung der eigenen Reputation: Wenn ein Kunde seine Personendaten einem Dienstleister anvertraut und dieser daraufhin damit Schindluder treibt, fällt dies

74 Art. 6 Abs. 1 Bst. b DSGVO.

ungeachtet der eigenständigen rechtlichen Verantwortlichkeit des Dienstleisters immer auch auf den Kunden zurück.

13. Wenn mehrere Stellen für eine Datenbearbeitung gemeinsam verantwortlich sind

a. Anforderung einer vertraglichen Regelung der Verantwortlichkeiten

[Rz 67] Komplizierter wird es, wenn Kunde und Dienstleister als «gemeinsame» Verantwortliche gelten (dazu Rz. 71 ff.). In diesen Fällen schreibt Art. 26 DSGVO vor, dass die Parteien in einem Vertrag regeln müssen, wer sich um welche Aspekte der Datenschutz-Compliance und insbesondere die Erfüllung der Betroffenenrechte kümmert.[75] Das DSG und der E-DSG kennt jedenfalls für den privaten Bereich keine solche Regelung, jedenfalls keine ausdrückliche (ihre Notwendigkeit kann sich jedoch aus den Umständen ergeben; im öffentlichen Bereich gibt es sie teilweise[76]). In beiden Fällen sind alle gemeinsame Verantwortliche – es müssen nicht nur zwei sein – im Aussenverhältnis für die gesamte (gemeinsame) Datenbearbeitung solidarisch verantwortlich. Das gilt so unter der DSGVO (Rz. 78) und gilt im Ergebnis auch im Schweizer Recht.[77] Dies führt dazu, dass alle Verantwortliche über die konkrete Anforderung von Art. 26 DSGVO hinaus ein Interesse haben können, die Datenbearbeitung durch die anderen mitkontrollieren zu können, um nicht ihrerseits zur Verantwortung gezogen zu werden, weil ein anderer «Mit»-Verantwortlicher gegen das anwendbare Datenschutzrecht verstösst.

b. Anwendbares Recht bei Verantwortlichen in mehreren Staaten

[Rz 68] Gerade die Frage des anwendbaren Datenschutzrechts bietet in solchen Konstellationen allerdings besondere Herausforderungen, denn es ist ohne Weiteres denkbar, dass das auf die einzelnen Verantwortlichen anwendbare Datenschutzrecht nicht identisch ist. Qualifizieren ein Schweizer Kunde und sein deutscher Dienstleister als gemeinsame Verantwortliche, so unterliegt letzterer aufgrund des Sitzlandprinzips ohne Weiteres der DSGVO,[78] während es ersterer möglicherweise nicht tut, weil er sich ausserhalb des territorialen Anwendungsbereichs von Art. 3 DSGVO bewegt. Der Umstand, dass an derselben Datenbearbeitung eine andere, der DSGVO unterstellte Person mitwirkt, kann für sich vernünftigerweise nicht zur Unterstellung aller Verantwortlicher oder gar aller Beteiligter führen. Der Fall ist vergleichbar mit der Konstellation, in welchem sich ein Schweizer Verantwortlicher für seine Datenbearbeitung eines Auftragsbearbeiters in der EU bedient; hier ist mittlerweile anerkannt, dass dies nicht zur Unterstellung auch

75 Vgl. etwa das Muster des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg, abrufbar unter https://bit.ly/2K0UYBZ.

76 So sieht Art. 16 Abs. 2 DSG vor, dass der Bundesrat spezielle Regelungen trifft, wenn Bundesorgane Personendaten gemeinsam bearbeiten (allenfalls gemeinsam mit Privaten); kantonale Datenschutzgesetze kennen ähnliche Regelungen, wie z.B. § 5 Abs. 1 IDG ZH («Das öffentliche Organ verwaltet seine Informationen so, dass das Verwaltungshandeln nachvollziehbar und die Rechenschaftsfähigkeit gewährleistet ist. Bearbeiten mehrere öffentliche Organe einen gemeinsamen Informationsbestand, regeln sie die Verantwortlichkeiten.»).

77 Zivilrechtlich kann jeder, der an einer Persönlichkeitsverletzung «mitwirkt», ins Recht gefasst werden (Art. 28 ZGB). Haftungsrechtlich ergibt sich die Solidarität aus Art. 50 Obligationenrecht vom 30. März 1911 (OR; SR 220).

78 Art. 3 Abs. 1 DSGVO.

des Schweizer Verantwortlichen führt,[79] soweit die Anforderungen von Art. 3 DSGVO durch ihn nicht selbst erfüllt sind, er also zum Beispiel Kunden im EWR anspricht. Immerhin kann Art. 3 DSGVO dort greifen, wo ein Schweizer Verantwortlicher den Mit-Verantwortlichen im EWR selbst gesellschaftsrechtlich oder anderweitig kontrolliert, so dass dieser als seine Niederlassung gilt.[80] Solche Verhältnisse können in Konzernsituationen auftreten, etwa wenn das Mutterhaus in der Schweiz und die Tochter, Zweigniederlassung oder Repräsentanz im EWR, gemeinsame Verantwortliche sind.

[Rz 69] Findet also die DSGVO oder das E-DSG auf einen der gemeinsamen Verantwortlichen keine Anwendung, auf andere aber schon, haben letztere ein evidentes Eigeninteresse daran, die Einhaltung der DSGVO bzw. des E-DSG durch die anderen gemeinsamen Verantwortlichen vertraglich sicherzustellen. Der übliche Satz, wonach jeder Verantwortliche «das anwendbare Datenschutzrecht» einzuhalten hat, wird diesfalls nicht genügen. Es muss sich jeder verpflichten, alle auf *jeden* der gemeinsamen Verantwortlichen anwendbaren Datenschutzrechte einzuhalten, also zum Beispiel DSGVO *und* E-DSG, jedenfalls soweit die Einhaltung der DSGVO oder des E-DSG nicht bereits durch einen der Mit-Verantwortlichen hinreichend abgedeckt ist.

[Rz 70] Schon vor diesem Hintergrund liegt es auf der Hand, dass eine gemeinsame Verantwortlichkeit in der Praxis nicht gerne gesehen wird. Sie kommt allerdings häufiger vor, als manchen lieb sein mag. Aus der Definition des Verantwortlichen ergibt sich, dass gemeinsame Verantwortlichkeit dann vorliegt, wenn *gemeinsam* über Zweck und Mittel der Datenbearbeitung entschieden wird.[81] Es ist anerkannt, dass das «gemeinsam» nicht bedeutet, dass alle Entscheide zusammen zu treffen sind. Es genügt, dass es sich um *eine* Datenbearbeitung handelt, deren Zweck und Mittel teilweise der eine und teilweise der andere entscheidet. Das drückt sich auch bei der Frage der Haftung aus (Rz. 78).

14. Mitbestimmung führt zur gemeinsamen Verantwortlichkeit

a. Der Fall Facebook Fanpages: Es braucht nicht viel zur gemeinsamen Verantwortlichkeit

[Rz 71] Praxis zur gemeinsamen Verantwortlichkeit gibt es nur spärlich. Für Aufsehen sorgte immerhin ein Urteil des EuGH vom 5. Juni 2018 i.S. Facebook Fanpages.[82] In der Sache ging es um ein Unternehmen aus Deutschland, das auf Facebook eine sog. Fanpage betrieb, eine unternehmenseigene Seite auf Facebook. Betreibern solcher Fanpages wird zwingend eine Funktion bereitgestellt, über welche sie anonymisierte statistische Daten über die Nutzer ihrer Seite erhalten. Eine deutsche Datenschutzbehörde ging dagegen unter dem Titel der mangelnden Transparenz vor. So stellte sich die Frage, ob neben Facebook auch das Unternehmen, das sich entscheidet, eine solche Fanpage zu betreiben, als Verantwortlicher bezüglich der von Facebook auf dieser Fanpage von den Besuchern erhobenen Personendaten gilt.

79 Europäischer Datenschutzausschuss (EDSA), Guidelines 3/2018 on the territorial scope of the GDPR (Article 3), version for public consultation, 22. November 2018, S. 10 f.

80 In diesem Falle wäre eine Anwendbarkeit gemäss Art. 3 Abs. 1 DSGVO gegeben.

81 Art. 4 Ziff. 7 DSGVO, Art. 4 Bst. i E-DSG.

82 Urteil des EuGH C-210/16 i.S. *Wirtschaftsakademie Schleswig-Holstein* vom 5. Juni 2018.

[Rz 72] Der EuGH bejahte dies. Der Entscheid erging noch unter der alten Datenschutzrichtlinie der EU, dürfte aber auch unter der DSGVO herangezogen werden. Der Gerichtshof befand, dass der Begriff der Verantwortlichkeit im Hinblick auf einen möglichst wirksamen und umfassenden Schutz der betroffenen Personen weit auszulegen ist. Entscheidend sei, ob und inwieweit ein Unternehmen als Betreiber einer Fanpage einen *Beitrag* zur Entscheidung über die Zwecke und Mittel der Bearbeitung der Personendaten der Besucher seiner Fanpage leistet.[83] Die blosse Nutzung von Facebook durch ein Unternehmen soll es zwar noch nicht verantwortlich dafür machen, was Facebook mit den Daten der Besucher seiner Fanpage tut.[84] Im konkreten Fall konnte das Unternehmen jedoch angeben, welches Zielpublikum es mit seiner Seite ansprechen will und Kriterien festlegen, nach denen Facebook die dem Unternehmen zur Verfügung gestellten Nutzungsstatistiken erstellt.[85] Bezeichnet werden konnten u.a. die Kategorien von Personen, deren Personendaten ausgewertet werden sollen, und Facebook wiederum lieferte dem Unternehmen demografische Angaben über die Nutzer seiner Seite. Das Gericht befand, dass das Unternehmen «durch die von ihm vorgenommene Parametrierung u.a. entsprechend seinem Zielpublikum sowie den Zielen der Steuerung oder Förderung seiner Tätigkeiten an der Entscheidung über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Besucher seiner Fanpage beteiligt» war und damit gemeinsam mit Facebook Verantwortlicher sei.[86] Der Umstand, dass das Unternehmen diese Daten nur in Form anonymisierter Statistiken erhält, war aus Sicht des EuGH irrelevant; bei einer gemeinsamen Verantwortlichkeit muss nicht jeder Verantwortlicher Zugang zu den Personendaten haben (ob mindestens einer ihn haben muss: Rz. 40).[87]

[Rz 73] Ist somit ein Kunde daran beteiligt, die datenschutzrechtlichen Parameter der Datenbearbeitung eines von ihm beanspruchten Dienstleisters festzulegen, so muss er damit rechnen, zusammen mit diesem für diese Datenbearbeitung verantwortlich zu sein, soweit sie für oder wegen ihm erfolgt. Der Fall Facebook Fanpages stellt allerdings auch klar, dass die Mitwirkung nicht eine beliebige sein kann: Der Umstand, dass der Kunde es dem Dienstleister ermöglicht, Personendaten von Dritten zu bearbeiten, fördert zwar die Datenbearbeitung, beinhaltet aber noch keine Entscheidung diesbezüglich. Es genügte daher nicht, dass das Unternehmen eine Fanpage bei Facebook betrieb und es so Facebook überhaupt erst ermöglichte, als Verantwortlicher für die Plattform Daten über die Nutzer der Fanpage zu sammeln. Nötig ist – wie auch unter dem Schweizer Recht – ein Mitwirken an der Datenbearbeitung selbst, und es muss kontrollierender Natur sein, d.h. entweder den verfolgten Zweck (welchem Ziel dient die Statistikfunktion?) oder die dazu verwendeten Mittel (welche Daten werden wie ausgewertet?) mitbestimmen; im Falle der Fanpage-Statistik lag beides vor.

[Rz 74] Diese Einschränkung auf ein Mit*bestimmen* liegt auf der Hand: Verantwortlich kann nur sein, wer überhaupt die Möglichkeit hat, die Datenbearbeitung irgendwie zu steuern, d.h. festzulegen, in welche Richtung sie sich bewegt und wie sie erfolgt (wobei hierbei die Datenbearbeitung als solche bzw. bezüglich ihrer Ausgestaltung gemeint ist, nicht die einzelnen Inhalte). Die Mitbestimmung muss freilich wie bereits mehrfach bekannt nicht beides oder alles betreffen. Es ist nur aber immerhin genügend, dass *datenschutzrechtlich relevante Aspekte* der Datenbearbeitung

83 Ebd., Rz. 31.

84 Ebd., Rz. 35.

85 Ebd., Rz. 36.

86 Ebd., Rz. 39.

87 Ebd., Rz. 38.

je nach Entscheid des Mitverantwortlichen anders ausfallen. Angenommen Facebook erstelle für alle Fanpages dieselben Statistiken und das Unternehmen könnte lediglich bestimmen, welche Statistiken Facebook ihm anzeigen soll, wäre es dementsprechend nicht mehr gemeinsam mit Facebook verantwortlich dafür: Es wäre lediglich Konsument der Ergebnisse der Datenbearbeitung, hätte auf sie aber keinen Einfluss mehr.

[Rz 75] Den umgekehrten Fall gibt es übrigens auch: Der Kunde bestimmt primär über die Datenbearbeitung, der Dienstleister trifft aber wesentliche Entscheide über datenschutzrechtliche Parameter der Datenbearbeitung, d.h. setzt sie nicht bloss um (vgl. dazu Rz. 48 ff.). Ein solches Beispiel ist SWIFT und wird nachfolgend diskutiert (Rz. 90 ff.).

b. Der Fall Zeugen Jehovas: Die Mitbestimmung kann auch eine mittelbare sein

[Rz 76] Nicht erforderlich zur Annahme einer gemeinsamen Verantwortlichkeit ist, dass eine Stelle die Datenbearbeitung *unmittelbar* mitbestimmt. Einen Monat nach dem Facebook-Fanpages-Entscheid befand der EuGH, dass es genügen kann, das eine Stelle das Umfeld einer Datenbearbeitung schafft, die dann andere für sie bzw. in ihrem Interesse vornehmen:[88] Es ging um Mitglieder der Zeugen Jehovas, die sich bei ihren Verkündigungen von Tür zu Tür nach eigenen Angaben zur Gedächtnisstütze für spätere Besuche informell unter anderem die Namen von Personen notierten, die ihnen nicht bekannt waren. Die Gemeinschaft hat von den einzelnen Mitgliedern diese Datenerhebung zwar angeblich nicht verlangt, aber sie hat ihnen Anleitungen zur Erstellung solcher persönlicher Notizen gegeben und hätte sie auch verbieten können. Es stellte sich für den Gerichtshof die Frage, ob neben den einzelnen Mitgliedern auch die Gemeinschaft als solche als Verantwortliche anzusehen sei.

[Rz 77] Das bejahte der EuGH: Es sei zwar Sache der Mitglieder gewesen zu entscheiden, unter welchen konkreten Umständen sie Personendaten über aufgesuchte Personen erheben, welche Daten sie genau erheben und auf welche Weise sie sie anschliessend verarbeiten.[89] Allerdings taten sie dies im Rahmen der von der Gemeinschaft organisierten und koordinierten Verkündigungstätigkeit. Die Erhebung der Personendaten über aufgesuchte Personen und die anschliessende Verarbeitung dieser Daten diente nach Ansicht des Gerichts der Umsetzung des Ziels der Gemeinschaft der Zeugen Jehovas – nämlich der Verbreitung ihres Glaubens – und sei folglich von ihren verkündigenden Mitgliedern im Interesse der Gemeinschaft vorgenommen worden.[90] Das Gericht befand, dass die Gemeinschaft der Zeugen Jehovas ihre verkündigenden Mitglieder dazu ermuntere, im Rahmen der von ihr organisierten und koordinierten Verkündigungstätigkeit Personendaten zu verarbeiten, und somit gemeinsam mit den Mitglieder an der Entscheidung über den Zweck und die Mittel der Verarbeitung mitwirkt.[91]

88 Urteil des EuGH C-25/17 i.S. *Zeugen Jehovas* vom 10. Juli 2018.

89 Ebd., Rz. 70.

90 Ebd., Rz. 71.

91 Ebd., Rz. 72 f.

c. Nicht jeder gemeinsame Verantwortliche hat dieselbe Verantwortung

[Rz 78] Während eine Mitbestimmung punkto den Zweck oder den datenschutzrechtlichen Parametern einer Datenbearbeitung grundsätzlich zur (Mit-)Verantwortlichkeit führt, ist der Grad der Verantwortung mehrerer gemeinsamer Verantwortlicher nicht zwingend derselbe,[92] auch wenn dies nur teilweise von praktischer Relevanz ist: Der eine Verantwortliche hat aufgrund seiner Position möglicherweise wesentlich mehr Einfluss auf die Ausgestaltung der Datenbearbeitung als der andere, der vielleicht nur aufgrund seiner Mitbestimmung betreffend ein Nebenaspekt Mitverantwortlicher ist. Im Aussenverhältnis spielt dies für die Frage der Haftung keine Rolle, denn nach Art. 26 Abs. 3 DSGVO und Art. 82 Abs. 4 DSGVO kann die betroffene Person grundsätzlich jeden (Mit-)Verantwortlichen auf den vollen Schadenersatz belangen. Auf Schadenersatz nicht belangt werden kann nach Art. 82 Abs. 3 DSGVO nur derjenige Verantwortliche, der zeigen kann, dass er auf die Umstände, die zur Haftung führen, keinerlei tatsächlichen oder rechtlichen Einfluss hatte.[93] Eine Abrede unter den Verantwortlichen, dass nur der eine von ihnen für eine Verletzung haften soll, schützt diese, also höchstens im Innenverhältnis. Sie kann immerhin bewirken, dass derjenige von ihnen, der intern verantwortlich ist, in jedem Fall auch gegen aussen verantwortlich ist, auch wenn er keinen tatsächlichen Einfluss auf die Verletzung hatte. Dasselbe kann auch der Aussenauftritt der gemeinsam Verantwortlichen bewirken: Wer sich so präsentiert, dass ihn die betroffenen Personen als ihren Ansprechpartner bzw. Hauptverantwortlicher wahrnehmen, muss sich diese mindestens suggerierte Einflussnahme als tatsächliches Element zurechnen lassen und damit mithaften.

[Rz 79] Differenzierter verhält es sich mit Bezug auf das Bussgeldrisiko unter der DSGVO: Hier wird mit Hinweis auf die Bussgeld-Bemessungskriterien nach Art. 83 DSGVO vertreten, dass es durchaus darauf ankommt, in welchem Umfang ein Verantwortlicher für eine Verletzung tatsächlich mitverantwortlich ist.[94] Hierbei kommt es allerdings nicht nur darauf an, welche tatsächliche und rechtliche Einflussmöglichkeit der jeweilige Verantwortliche hatte, sondern auch, inwieweit die Aufgabenteilung unter den Verantwortlichen auf den konkreten Sachverhalt bezogen sachgerecht und klar erfolgt ist.[95] Ist also die Pflicht zur Erfüllung von Betroffenenrechten einem Verantwortlichen zugewiesen, der sie aufgrund seiner Stellung gar nicht richtig erfüllen kann, so mag daran auch die anderen Verantwortlichen ein Verschulden treffen.[96] Dasselbe gilt, wenn der eine Verantwortliche seiner Pflicht nicht nachkommt und es damit einem anderen Verantwortlichen ermöglicht, das Datenschutzrecht zu verletzen.[97]

---

92 Ebd., Rz. 66.

93 Kristina Schreiber, Gemeinsame Verantwortlichkeit gegenüber Betroffenen und Aufsichtsbehörden, in: Zeitschrift für Datenschutz (ZD) 2019, 55, Ziff. II.2, m.w.H.

94 Schreiber (Fn. 93), Ziff. II.4, m.w.H.

95 WP169 (Fn. 13), S. 30, wobei vertreten wird, dass sich auch die Haftung danach richtet, wie klar die Zuständigkeitsregel der gemeinsam Verantwortlichen ausgestaltet ist, was aber unter der DSGVO grundsätzlich keine Rolle spielen kann.

96 Die Artikel-29-Datenschutzgruppe erwähnt das Beispiel einer Plattform zur Verwaltung von Gesundheitsdaten, die zwar eine zentrale Stelle betreibt, aber so viele Mit-Verantwortliche hat, die sie füttern, dass eine vernünftige Behandlung von Betroffenenrechten nur möglich ist, wenn dafür die zentrale Stelle zuständig ist (WP169 [Fn. 13], S. 29, Beispiel 15).

97 Die Artikel-29-Datenschutzgruppe erwähnt hier das Beispiel eines Unternehmens, dessen Vorstandsmitglied beschliesst, gewisse Mitarbeiter heimlich zu überwachen. Sie wertet dies als Ergebnis unzureichender Sicherheitsmassnahmen, die es dem Vorstandsmitglied überhaupt erlaubt haben, die Überwachung auf eigene Faust einzuführen. Dieses wird sich allenfalls ebenfalls als (Mit-)Verantwortlicher qualifizieren lassen und ist damit (mit-)haftbar (WP169 [Fn. 13], S. 21, Beispiel 4).

d. Privilegierung unter den gemeinsamen Verantwortlichen?

[Rz 80] Noch ungeklärt ist unter der DSGVO hingegen die Frage, ob ein Datenaustausch unter gemeinsamen Verantwortlichen ähnlich privilegiert ist wie der Austausch zwischen einem Verantwortlichen und seinem Auftragsbearbeiter. Während dies unter dem Schweizer Recht so angenommen werden kann, d.h. der gemeinsame Verantwortliche nicht als Dritter gilt,[98] ist dies unter der DSGVO noch umstritten. Der Begriff des Dritten ist dort in Art. 4 Ziff. 10 definiert und meint jede Stelle «ausser der betroffenen Person, dem Verantwortlichen, dem Auftragsbearbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten». Nach der hier vertretenen Ansicht umfasst der Begriff des Verantwortlichen in dieser Definition auch die gemeinsam Verantwortlichen, womit sie keine Dritten sind.[99] Die Frage ist freilich von beschränkter Relevanz: Ob der Zweckbindungsgrundsatz und das Erfordernis eines Rechtsgrunds erfüllt ist, beurteilt sich nicht primär danach, ob es sich bei gemeinsam Verantwortlichen um Dritte handelt oder nicht, sondern was sie insgesamt mit den Daten tun. In der Praxis wird selbst der Austausch von Personendaten zwischen zwei eigenständigen Verantwortlichen diesbezüglich nicht unbedingt ein Hindernis sein, wenn beide die Daten für denselben Zweck verwenden und er von einegemeinsamen Rechtsgrund abgedeckt ist (Rz. 61 ff.).

15. Abgrenzung zwischen gemeinsamer und eigenständiger Verantwortlichkeit

a. Problematik überlagernder Datenbearbeitungen am Beispiel von Fernmeldenetzen

[Rz 81] Im Falle von Facebook beteiligte sich der Kunde an der Datenbearbeitung des Dienstleisters; es war aufgrund der Umstände klar, dass beide an *derselben* Datenbearbeitung mitbestimmten und sie daher gemeinsame Verantwortliche sein mussten. Doch in der Praxis sind die Verhältnisse nicht immer so klar und die Unterscheidung zwischen gemeinsamer und eigenständiger Verantwortlichkeit kann erhebliche Mühe bereiten.

[Rz 82] So ist es denkbar, dass zwei Datenbearbeitungen zwar miteinander verknüpft sind oder sich sogar überlagern, aber dennoch als getrennte Vorgänge mit getrennten und damit eigenständigen Verantwortlichen betrachtet werden müssen.

[Rz 83] Die Übermittlung von Daten über ein Fernmeldenetz ist ein solches Beispiel: Ein Kunde betreibt eine Personaldatenverwaltung, die auf Servern an zwei Standorten läuft; er alleine bestimmt über den Zweck und die Mittel der diesbezüglichen Datenbearbeitung. Zur Vernetzung der beiden Standorte und Server bedient sich der Kunde jedoch eines Fernmeldenetzes. Gehen wir für die Zwecke des Beispiels davon aus, dass der Fernmeldeverkehr unverschlüsselt erfolgt,

98 Rosenthal (Fn. 18), Art. 3 DSG N 113, noch zum heutigen Begriff des «Inhabers der Datensammlung».

99 Dagegen lässt sich anführen, dass ein gemeinsamer Verantwortlicher anders als ein Auftragsbearbeiter viel weniger nah an den anderen Verantwortlichen angebunden ist und daher eine vergleichbare Freiheit hat wie ein Dritter. Dem kann entgegengehalten werden, dass gemeinsame Verantwortliche durchaus miteinander verbunden sind, sei es über ihre gemeinschaftliche Haftung (Rz. 78) oder über ihren Vertrag, den sie nach Art. 26 DSGVO abzuschliessen haben. Inwieweit sie letzteren nutzen, ist eine andere Frage, die primär das Innenverhältnis betrifft, so namentlich den Regress im Haftungsfall.

d.h. dass die Übermittlungsinhalte für den Fernmeldedienstanbieter (FDA) Personendaten darstellen (für den Fall der Verschlüsselung vgl. Rz. 98 f.). Der FDA bewegt unbestreitbar Personendaten vom einen Standort zum anderen und bearbeitet diese damit in datenschutzrechtlichem Sinne. Obwohl er dies zweifellos einzig für den Kunden tut, ist er diesbezüglich kein Auftragsbearbeiter: Es ist allen Beteiligten klar und die Kunden akzeptieren, dass ab Übergabe der Daten an das Netzwerk alleine der FDA die Art und Weise kontrolliert, wie sich die Daten in seinem Fernmeldenetz bewegen (solange der FDA gewisse Mindeststandards mit Bezug auf Bandbreite, Reaktionszeit, etc. erfüllt). Das unterscheidet ihn vom Hosting-Anbieter.[100] Es ist der FDA, der alleine entscheiden soll, ob und welche Subunternehmer er beizieht, wo sie durchgeleitet und wie lange sie im System zwischengespeichert[101] werden, welche Sicherheitsmassnahmen nötig sind. Er leitetet den Behörden Netzwerkverkehr weiter, wenn ihn das Gesetz[102] dazu verpflichtet. Der Kunde hat keine Auditrechte, und die Inanspruchnahme von Fernmeldedienstleistungen gilt nicht als Outsourcing.[103] Es kann sogar vertreten werden, dass der FDA und nicht der Kunde es ist, der durch den Aufbau seines Netzwerks entschieden hat eine Datenbearbeitung namens «Datenübermittlung für Dritte» durchzuführen, sie also veranlasst hat.[104] Damit bestimmt der FDA den Zweck und die Mittel und ist damit Verantwortlicher nicht nur für die Bearbeitung der Randdaten, die beim Betrieb seines Fernmeldenetzes anfallen,[105] sondern auch für die von ihm übermittelten Inhalte.

[Rz 84] Dies führt zur Frage, wie diese datenschutzrechtliche Verantwortlichkeit des FDA für die Datenübertragungen zur Verantwortlichkeit des Kunden steht, die dieser ebenso für jede Übermittlung innehat, die er über das Fernmeldenetz vornimmt. Es ist allen klar, dass der FDA sich (von Spezialfällen wie etwa Mehrwertdiensten abgesehen) inhaltlich aus der Verantwortung nimmt und zu nehmen hat: Ob und für welche Personendaten ein Kunde seinen Internet-Anschluss nutzt, ist – im Rahmen des gesetzlich erlaubten und technisch störungsfrei möglichen – Sache nur des Kunden. Unter herkömmlichen Gesichtspunkten müssten die beiden als gemeinsame Verantwortliche gelten, was eine vertragliche Abgrenzung ihrer Verantwortlichkeiten nach Art. 26 DSGVO erforderlich machen würde, was jedoch nicht sinnvoll erscheint; der FDA hat keinen Einfluss auf die Inhalte seiner Kunden und soll sich auch nicht damit auseinandersetzen, welche Personendaten sich in den Datenströmen befinden, die über seine Leitungen fliessen.

[Rz 85] Eine mögliche Lösung wäre im Sinne einer ergebnisorientierten Auslegung zu sagen, dass die Übermittlung von Daten von A nach B gar keine Datenbearbeitung ist, weil sie sich datenschutzrechtlich nicht sinnvoll befriedigend regeln lässt. Es kann aus Gründen der Opportunität

100 Diese Unterscheidung ist *nicht* technisch und aus der Natur der eingesetzten Mittel und vorgenommenen Handlungen begründet: FDA und Hosting-Anbieter stellen eine Infrastruktur zur Verfügung zur Bearbeitung von digitalen Daten. Entscheidend ist das unterschiedliche Verständnis über das *Kontrollbedürfnis* und die damit einhergehende Verantwortung. Beim FDA endet die Sphäre des Kunden ab der Übergabe an den FDA, während der vom Hosting-Provider bereitgestellte Speicherplatz die Sphäre des Kunden bleiben soll. Dementsprechend wäre es ebenso denkbar, dass sich die Erbringung von Fernmeldedienstleistungen als Auftragsbearbeitung ausgestaltet und der Hosting-Provider Verantwortlicher ist. Vgl. dazu Rz. 36 ff.

101 Z.B. bei SMS.

102 Bundesgesetz betreffend die Überwachung des Post- und Fernmeldeverkehrs vom 18. März 2016 (BÜPF, SR 780.1).

103 So findet z.B. das Outsourcing-Rundschreiben 2018/3 der FINMA keine Anwendung und der von einer Bank für Fernmeldedienstleistungen beanspruchte FDA gilt auch nicht als «Beauftragter» im Sinne von Art. 47 Bundesgesetz über die Banken und Sparkassen vom 8. November 1934 (BankG; SR 952.0) (Bankgeheimnis).

104 Allerdings ist nicht jeder Anbieter von Infrastruktur automatisch Verantwortlicher; vgl. dazu Rz. 88.

105 Hier ist der Fall sowieso klar: Diese Datenbearbeitungen sind lediglich Mittel zum Zweck der Leistungen des FDA und fallen daher sowieso in seine eigene Verantwortlichkeit (WP169 [Fn. 13], S. 13 f.).

und Einfachheit durchaus sinnvoll sein, eine nicht planmässige Datenbearbeitung, also Vorgänge, die zwar technisch gesehen zu einer Bearbeitung von Personendaten führen, es aber nicht um Daten in ihrer Eigenschaft als Personendaten geht, generell auszublenden und das Datenschutzrecht höchstens dann zur Anwendung zu bringen, wenn etwas schief läuft oder die Daten zweckentfremdet (und dann eben doch planmässig als Personendaten) verwendet werden. So verlockend diese «Vogel-Strauss»-Argument allerdings auch ist, so ist es trotz allem unbefriedigend und mit dem heutigen Datenschutzrecht nicht vereinbar; weder kennt es eine de-minimis-Regel für Datenbearbeitungen, noch gibt es Datenbearbeitung ohne Verantwortlichen (vgl. dazu auch Rz. 103 f.).

b. Das Ebenenmodell als Abgrenzungshilfe bei überlagernden Datenbearbeitungen

[Rz 86] Lösen lässt sich dieser Zielkonflikt im Beispiel des FDA durch das sog. *Ebenenmodell*, indem Verantwortlichkeiten nicht nur horizontal definiert werden (wie das auch die Artikel-29-Datenschutzgruppe tut[106]), sondern eine Abgrenzung ebenso vertikal stattfindet. Am vorgenannten Beispiel des Kunden und seines FDA erklärt: Die Datenbearbeitung des FDA überlagert zwar einen Teil der Datenbearbeitung seines Kunden, aber trotzdem sind es zwei logisch getrennte Vorgänge, da sie auf zwei unterschiedlichen Ebenen stattfinden: Der Personaldatenlösung (Applikationsebene) und dem Fernmeldenetz (Netzebene). Auf der Applikationsebene werden Personaldaten bearbeitet, auf der Netzebene Netzwerkverkehr, der überdies noch sehr viel mehr als nur Personaldaten enthält. Aus diesem Grund ist der FDA datenschutzrechtlich ebenso wenig verantwortlich für die Netzwerknutzung seines Kunden, wie die Telefongesellschaft für den Inhalt der Gespräche ihrer Kunden.[107] Der FDA bleibt hingegen allein verantwortlich für die Datenbearbeitung auf der Netzwerkebene: Leitet der FDA den Netzwerkstrom seines Kunden trotz korrekter Adressierung an die falsche Adresse, haftet dafür einzig der FDA.

[Rz 87] Genauso verhält es sich im Übrigen bei der Post mit Bezug auf deren Bearbeitung von Personendaten: Für die Datenbearbeitung auf der Transportebene – wozu auch die Adressen auf den Postsendungen gehören – ist die Post verantwortlich; die Datenbearbeitung auf der Inhaltsebene – was die Kunden in ihren Briefen oder auf ihren Postkarten schreiben – ist Sache der Kunden. Es liegt aufgrund des Ebenenmodells keine gemeinsame Verantwortlichkeit vor. Deshalb tangiert ein von der Post fehl*zugestellter* Brief nicht die datenschutzrechtliche Verantwortlichkeit des Kunden, während ein falsch*adressierter* Brief einzig die Verantwortlichkeit des Kunden ist – mit entsprechenden Folgen etwa für die Meldepflichten bei Datenschutzverstössen.

[Rz 88] Die Beispiele machen deutlich, wie wichtig es für die Ermittlung der Verantwortlichkeit ist, genau zu bestimmen, worin die relevante Datenbearbeitung besteht, d.h. welche Vorgänge zusammengefasst werden müssen, weil sie eine logische Einheit bilden, und welche davon separat zu beurteilen sind. Auch hierfür gibt es keine allgemeingültige Formel; eine logische Einheit

106 Vgl. WP169 (Fn. 13), S. 25, wo von «Vorgangsreihen» die Rede ist, was begrifflich allerdings nur sequentiell verknüpfte Datenbearbeitungen erfasst.

107 Dies ist in der Praxis zwar anerkannt, wird aber nicht schlüssig begründet. Es wird lediglich festgehalten, dass der FDA bezüglich der Inhalte seiner Übertragungen nicht Verantwortlicher sei. Wer er mit Bezug auf seine unbestreitbar stattfindenden Bearbeitungen des Netzwerkverkehrs des Kunden jedoch wirklich *ist*, wird nicht erklärt. Vgl. WP169 (Fn. 13), S. 14 und insb. Fussnote 14.

kann z.B. bilden, was demselben Zweck dient und allenfalls sogar weitere datenschutzrechtliche Parameter teilt, was von derselben Person oder einheitlich kontrolliert wird, was in der Aussenwirkung hin als Einheit erscheint, was datenschutzrechtlich einheitlich zu behandeln ist, was in der praktischen Ausführung untrennbar miteinander verkettet ist. So erscheint es sinnvoll, beim FDA die diversen Übermittlungsvorgänge, die in seinem Netzwerk stattfinden, als *eine* Datenbearbeitung zu betrachten, während bei einem Hosting-Provider, der seine Rechnerkapazitäten seinen einzelnen Kunden zur Verfügung stellt, deren Aktivitäten jeweils als *separate* Datenbearbeitungen gelten. Beide Dienstleister bieten ihre Infrastruktur ihren Kunden zur Nutzung an, und bei beiden bleiben die Daten der einzelnen Kunden voneinander getrennt, d.h. kein Kunde hat Zugang zu den Daten des anderen. Im Falle des FDA ist es aber der FDA, der die Datenbearbeitung veranlasst (der Kunde übergibt die Daten ans «Netz» des FDA, was als *ihre* Sphäre gilt), während es beim Hosting-Provider der jeweilige Kunde ist, der dies tut (der Kunde erhält «seinen» Speicher oder virtuellen Server zugewiesen, der als *seine* Sphäre gilt). Dementsprechend ist der FDA Verantwortlicher, der Hosting-Provider nur Auftragsbearbeiter (vgl. Rz. 83).

[Rz 89] Notabene ist diese Aufteilung nicht naturgegeben, sondern lediglich der Ausfluss der heute üblichen Rollen- bzw. Sphärenordnung, die wiederum den allgemeinen Sitten und Gebräuche entspringt. Das Datenschutzrecht ordnet sich diesen letztlich unter, weil es lediglich sicherstellen will, dass «der Richtige» die Verantwortung für dessen Einhaltung trägt. Es sind daher auch andere als die klassischen Geschäftsmodelle denkbar. Benötigt es z.B. in einem konkreten Fall aus Datenschutzgründen einen Datentreuhänder, bewahrt dieser zwar womöglich wie ein Hosting-Anbieter die Daten eines Kunden bei sich für diesen auf, aber die Parteien werden zugleich wollen, dass nur der Dienstleister die Kontrolle darüber hat; damit ist dieser Dienstleister Verantwortlicher.

c. Der Fall SWIFT: Die Autonomie führte zur gemeinsamen Verantwortlichkeit

[Rz 90] Die Grenzen können freilich verschwimmen. Dies zeigt das Beispiel des Finanzmitteilungsdiensts SWIFT, der sich kurz gesagt nicht auf die Transportebene beschränkte, sondern sich in die Inhaltsebene «eingemischt» hat. Banken können den Dienst nutzen, um anderen Banken Geldüberweisungen (und andere von SWIFT vordefinierte Nachrichten) sicher zu übermitteln. SWIFT speicherte die Überweisungsdaten ab 2001 für einige Monate in ihren Rechenzentren in der EU und den USA. In den USA verlangten die US-Behörden Zugang zu diesen Daten, den SWIFT gewährte. Dies erfuhr die breite Öffentlichkeit erst einige Jahre später und sorgte für entsprechende Schlagzeilen.[108] SWIFT stellte sich auf den Standpunkt, sie sei blosse Auftragsbearbeiterin. Die Artikel-29-Datenschutzgruppe kam jedoch 2006 zum Schluss, dass sie mit den Banken mit Bezug auf den betreffenden Geldüberweisungsdienst «SWIFTNet-FIN» als gemeinsame Verantwortliche zu betrachten sei, enthalten die Zahlungsaufträge doch Personendaten von Dritten.[109]

---

108 Heute setzt SWIFT drei Rechenzentren ein, wobei eines sich in der Schweiz befindet. War früher das US-RZ der Spiegel des europäischen RZ, ist heute das Schweizer RZ der Spiegel für die beiden anderen, so dass europäische Daten nicht mehr in den USA gespeichert werden.

109 Artikel 29-Datenschutzgruppe, Stellungnahme 10/2006 zur Verarbeitung von personenbezogenen Daten durch die Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128).

[Rz 91] Für die Verantwortlichkeit von SWIFT gab es zwei Gründe:[110]

a. *Erstens* habe SWIFT im Laufe der Jahre eine Reihe von Verantwortlichkeiten übernommen, die über das blosse Ausführen von Anweisungen hinausgehen und sowohl Entscheide über den Zweck wie auch die Mittel der Datenbearbeitung beinhalten. So definiert SWIFT und nicht die Banken, welche Arten von Daten die Banken im Rahmen von über SWIFT abzuwickelnden Zahlungsaufträgen bereitstellen müssen und in welcher Form. SWIFT bestimmte, wie sie Zahlungsaufträge auf Richtigkeit überprüft und wie lange sie bei sich archiviert werden. Sie entschied auch darüber welche Sicherheitsstandards zum Einsatz kommen, wo die Rechenzentren stehen und wie die Verträge ausgestaltet sind.

b. *Zweitens* war es SWIFT, die den Entscheid traf, die ihr im US-Rechenzentrum vorliegenden (Personen-)Daten den US-Behörden zur Verfügung zu stellen und jedenfalls gewissen Banken nichts darüber zu sagen. Dies verdeutlicht zwei Prinzipien bei der Zuordnung der Verantwortlichkeiten: Zum Einen ist derjenige, der eine *eigene* gesetzliche Pflicht erfüllt und hierzu Daten bearbeitet, mit Bezug auf diese Datenbearbeitung automatisch Verantwortlicher, auch wenn es um Daten seines Kunden geht (Rz. 32). Zum Anderen wäre SWIFT mit Bezug auf diese Datenbearbeitung selbst dann Verantwortliche, wenn sie ansonsten lediglich Auftragsbearbeiter gewesen wäre: Sobald ein solcher mit den ihm anvertrauten Daten etwas tut, das – wie hier – nicht mehr von seinem Auftrag gedeckt ist, ist er ebenfalls automatisch Verantwortlicher und kann daher für diese Handlungen direkt ins Recht gefasst werden (vgl. Rz. 50).

[Rz 92] Dass SWIFT die Verantwortung mit den Banken *gemeinsam* trägt, war für die Artikel-29-Datenschutzgruppe darin begründet, dass SWIFT anders als andere Dienstleister so organisiert war, dass die Banken auf ihre Entscheidfindung über verschiedene Gremien aktiv Einfluss nehmen können; rechtlich war und ist SWIFT als Genossenschaft strukturiert, deren Mitglieder die Banken sind.[111] Auch bestimmen die Banken, ob sie sich an SWIFT und ihrem Regelwerk anschliessen und wie und welche Zahlungsaufträge sie über SWIFT abwickeln. Ebenso stehen die Banken und nicht SWIFT mit den betroffenen Personen in Kontakt und handeln im eigenen Namen. Die letztgenannten Punkte könnten freilich zu einer eigenständigen Verantwortlichkeit der Banken führen. Da jedoch anders als beim Fernmeldeanbieter SWIFT sich nicht darauf beschränkte, die fernmeldetechnische Übertragung auf der Netzwerkebene sicherzustellen, sondern massgeblich auch auf der Applikationsebene mitbestimmte (indem sie z.B. definierte, wie die Zahlungsaufträge ausgestaltet sein müssen), wirkten die Banken und SWIFT bei dieser Datenbearbeitung zusammen. Dies führte für die Artikel-29-Datenschutzgruppe richtigerweise zu einer gemeinsamen statt einer sich teilweise überschneidenden, eigenständigen Verantwortlichkeit wie beim FDA (Rz. 86). SWIFT hat durch ihr Verhalten die Transport- und die Inhaltsebene miteinander verknüpft. Dieser Fall wurde zwar noch unter dem alten EU-Recht beurteilt, dürfte aber unter der DSGVO – wie der Facebook-Fanpage-Entscheid – gleich ausfallen, da sie die Verantwortlichkeitsordnung des bisherigen Rechts mehr oder weniger übernimmt.

110 Article 29 Data Protection Working Party, Opinion 10/2006 on the processing of personal data by the Society for Worldwide Interbank Financial Telecommunication (SWIFT) (WP128), S. 14.

111 WP128 (Fn. 110), S. 15 ff.

d. Beispiel: Reisebüro v. Reiseportal

[Rz 93] Ein weiteres Beispiel zur Abgrenzung zwischen eigenständiger und gemeinsamer Verantwortlichkeit ist dasjenige eines Reisebüros, welches für seine Kunden Flugreisen und Hotelübernachtungen arrangiert.[112] Nimmt das Reisebüro im Auftrag seiner Kunden entsprechende Buchungen vor und sendet es den Fluggesellschaften und Hotels dazu die Personendaten seiner Kunden, damit diese die Buchungen bestätigen, handeln alle als eigenständige Verantwortliche. Beschliessen das Reisebüro, eine Hotelkette und eine Fluggesellschaft jedoch eine gemeinsame, Internet-basierte Plattform zur einfacheren Vornahme von Buchungen zu schaffen und vereinbarten sie die wesentlichen Elemente der einzusetzenden Mittel (z.B. welche Daten wie lange aufbewahrt und wie Reservierungen zugewiesen werden, wer Zugang erhält) und nutzen sie die Daten für gemeinsame Werbeaktionen, so sind sie diesbezüglich gemeinsame Verantwortliche. Betreibt hingegen nur das Reisebüro alleine das Portal, erlaubt es den Fluggesellschaften und Hotels jedoch, über diesen Kanal Buchungen entgegenzunehmen, mit den Kunden zu kommunizieren und Werbung für sich zu betreiben, so liegt keine gemeinsame Verantwortlichkeit vor. Das Reisebüro bleibt die Verantwortliche für die Datenbearbeitung des Portals, während die Entgegennahme von Buchungen und die Kommunikation mit Kunden, auch wenn sie über das Portal abgewickelt werden, in der (alleinigen) Verantwortlichkeit der Fluggesellschaften und Hotels sind; auch hier löst das Ebenenmodell den Zielkonflikt der sich überlagernden Datenbearbeitungen: Die Datenbearbeitung «Portalbetrieb» findet auf einer anderen Ebene statt als die Datenbearbeitung «Buchung entgegennehmen» und «Kundenkommunikation» (vgl. Rz. 22).[113]

[Rz 94] Die Beispiele zeigen, dass selbst im Bereich der gemeinsamen Verantwortlichkeit ein gewisser Gestaltungsspielraum besteht. Die Ausführungen des EuGH und der Artikel-29-Datenschutzgruppe machen jedoch deutlich, dass derjenige, der einen datenschutzrechtlich relevanten Entscheid trifft, auch Verantwortlicher sein muss, damit er dafür zur Rechenschaft gezogen werden kann. Im Falle der Facebook Fanpages war es dem Gericht jedenfalls wichtig, keine Schutzlücke zu schaffen: Facebook sollte sich nicht aus der Verantwortung ziehen können, da es ja die Unternehmen seien, welche die Statistiken steuern, während die Unternehmen nicht argumentieren können sollten, dass sie gar keine Personendaten bearbeiten, weil sie ja nicht feststellen können, wer ihre Seiten auf Facebook besucht und sie somit gar keine Personendaten bearbeiten. Die Annahme einer gemeinsamen Verantwortlichkeit löste das Problem elegant und sorgt somit dafür, dass für alle Aspekte der Datenbearbeitung – wie zum Beispiel die Information der betroffenen Personen – ein Verantwortlicher zur Rechenschaft gezogen werden kann.

e. Schranken für die Regelung der Verantwortlichkeit im Innenverhältnis?

[Rz 95] Wie die Parteien die Verantwortlichkeiten im Innenverhältnis regeln, erscheint nach Art. 26 DSGVO ihnen überlassen. Frei sind sie nach Ansicht jedenfalls der deutschen Datenschutzbehörden trotzdem nicht. Im Falle von Facebook schaltete die Social Media Plattform flugs neue Vertragsbedingungen auf, in welchen Facebook die Verantwortlichkeit im Innenverhältnis

112 WP169 (Fn. 13), S. 24, Beispiel 7 und 8.

113 Vgl. dazu auch WP169 (Fn. 13), S. 26, Beispiel 11.

weitgehend selbst übernahm.[114] Die Deutsche Datenschutzkonferenz bemängelte daraufhin, dass die Unternehmen von Facebook «nicht hinreichend transparent und konkret» über die Datenbearbeitung informiert seien und so ihre Mit-Verantwortung gar nicht wahrnehmen könnten, was aber eine Voraussetzung für die Rechtmässigkeit der Datenbearbeitung sei.[115] Dies geht zu weit. Zu Ende gedacht, wäre es bei gemeinsamen Verantwortlichen nicht ausreichend, dass die einzelnen datenschutzrechtlichen Verantwortlichkeiten jeweils einem von ihnen zugewiesen werden. Stattdessen müsste jeder Mit-Verantwortliche auch im Innenverhältnis bezüglich aller wesentlicher Aspekte der Datenbearbeitung Mitspracherechte haben. Das steht im Widerspruch zur Rechtsprechung des EuGH, wonach sich die Verantwortlichkeiten auf verschiedene Phasen einer Datenbearbeitung verteilen können und der Grad der Verantwortlichkeit mehrerer Verantwortlicher nicht zwingend derselbe ist.[116]

16. Führt bereits der Zugang zu Daten zur Auftragsbearbeitung?

a. Ausgangslage

[Rz 96] Nebst der klassischen Rollenverteilung zwischen Verantwortlichem und Auftragsbearbeiter kommen in der Praxis regelmässig auch Fälle vor, in denen ein Dienstleister zwar Zugang zu Personendaten hat oder solche auf seinen Systemen gespeichert sind, er aber weder Auftragsbearbeiter noch Verantwortlicher ist. Diese Fälle führen in der Praxis besonders häufig zu Fehleinschätzungen. Hierbei sind grundsätzlich zwei Fallkonstellationen zu unterscheiden:

a. Der Dienstleister erhält zwar Personendaten zur Bearbeitung, aber diese sind so verschlüsselt, dass er nicht feststellen kann, um welche Personen es sich handelt. Aus seiner Sicht liegen keine Personendaten vor,[117] für den Kunden sind es jedoch Personendaten, da dieser den Schlüssel dazu hat. In der Fachsprache ist von *pseudonymisierten* Daten die Rede, also eine Art «subjektive» Anonymisierung; die Totalverschlüsselung von Daten ist dabei die extremste Form der Pseudonymisierung.

b. Der Dienstleister erhält zwar Zugang zu Personendaten im Klartext, aber er hat damit nichts zu tun. Sie sind nicht Gegenstand seiner Leistung, er kann sie nur aber immerhin im Rahmen seiner Vertragserfüllung zur Kenntnis nehmen. Er tut damit auch nichts.

[Rz 97] In beiden Fällen ist der Dienstleister weder Verantwortlicher noch Auftragsbearbeiter, jedenfalls solange er im ersten Fall nicht an den Schlüssel gelangt (ergo keine Personendaten vorliegen) und im zweiten Fall mit den Daten tatsächlich nichts tut (ergo keine Bearbeitung vorliegt).

---

114 Vgl. Facebook, Seiten-Insights-Ergänzung bezüglich des Verantwortlichen https://www.facebook.com/legal/terms/page_controller_addendum.

115 Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook Fanpages sowie der aufsichtsbehördlichen Zuständigkeit, 1. April 2019 (https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/Positionierung_Facebook_Fanpages.pdf).

116 Urteil des EuGH C-25/17 i.S. *Zeugen Jehovas* vom 10. Juli 2018, Rz. 66.

117 David Rosenthal, Personendaten ohne Identifizierbarkeit?, in: digma 2017/4, S. 198 ff. (https://media.homburger.ch/karmarun/image/upload/homburger/Hka534QSz-DIGMAROD.pdf)

b. Fall 1: Kein Zugang zu Personendaten im Klartext

[Rz 98] Ein Beispiel für die *erste Fallgruppe* ist ein Cloud-Anbieter, in welchem die Kunden ihre Daten in verschlüsselter Form speichern. Wichtig ist, dass es nicht der Cloud-Anbieter ist, der die Daten verschlüsselt, sondern der Kunde; sie erreichen die Cloud bereits in verschlüsselter Form und der Anbieter hat keine Möglichkeit, sie zu entschlüsseln. Weil damit aus rechtlicher Sicht für den Dienstleister keine Personendaten mehr vorliegen, fällt auch eine Auftragsbearbeitung ausser Betracht: Der Auftragsbearbeitung ist es begriffsimmanent, dass der Auftragsbearbeiter Personendaten bearbeitet, was voraussetzt, dass er solche erhebt, erfasst oder eine der anderen Handlungen vornimmt, die unter die Legaldefinition des Bearbeitens fällt.[118] Ein Bearbeiten im Sinne des DSG oder der DSGVO *ohne* Personendaten gibt es begrifflich nicht; gibt ein Verantwortlicher einem Dritten einen Satz verschlüsselter Daten weiter, ohne dass der Empfänger die betroffenen Personen bestimmen kann, so stellt dies auch keine Bekanntgabe von Personendaten dar, sondern lediglich eine Bekanntgabe von nicht personenbezogenen Daten, was datenschutzrechtlich nicht erfasst ist.[119] Dies ist das Ergebnis der relativen Natur des Begriffs der Personendaten.[120]

[Rz 99] Hierbei sind jedoch drei Vorbehalte zu beachten:

a. *Erstens* muss sichergestellt sein, dass keine Re-Identifikation der betroffenen Personen erfolgen kann, sei es, indem der Dienstleister trotz allem Zugang zu den Daten im Klartext erhält, oder sei es, dass er sie einer Person zugänglich macht oder machen muss, die ihrerseits eine Re-Identifikation durchführen kann.[121] Geschieht dies, liegen Personendaten und von diesem Moment möglicherweise auch eine Auftragsbearbeitung vor, die dann aber nicht mehr den gesetzlichen Anforderungen entspricht. Der Kunde des Dienstleisters schliesst somit unter Umständen vorsichtshalber trotzdem einen ADV ab, obwohl er nicht unbedingt erforderlich wäre.

b. *Zweitens* muss der Kunde des Dienstleisters selbstverständlich weiterhin den Datenschutz beachten, auch dahingehend, was der Dienstleister des Kunden mit seinen Daten tut. Aus seiner Sicht sind es weiterhin Personendaten, und die Bearbeitungsvorgänge des Dienstleisters werden ihm als Verantwortlichen zugerechnet, auch wenn es für den Dienstleister keine Personendaten sind.[122] Der Kunde muss also weiterhin die Bearbeitungsgrundsätze einhalten, die Betroffenenrechte (z.B. das Recht auf Auskunft, Berichtigung oder Löschung) wahren und unter dem revidierten DSG zum Beispiel in den vorgeschriebenen Fällen eine Datenschutz-Folgenabschätzung vornehmen. Das kann er aber oft nur, wenn ihm der Dienstleister entsprechend zur Hand geht bzw. er den Dienstleister bezüglich dessen Leistung kontrollieren kann, er also z.B. Daten nicht einfach löscht ohne dazu ermächtigt zu

118 Art. 3 Bst. e DSG, Art. 4 Bst. d E-DSG, Art. 4 Ziff. 2 DSGVO (wo von «Verarbeiten» die Rede ist).

119 Selbstverständlich muss sichergestellt sein, dass der Empfänger diese Daten nicht einer Person weitergibt, die ihrerseits die betroffenen Personen bestimmen kann.

120 Rosenthal (Fn. 117), S. 202.

121 Etwa eine Behörde, die durch eine Zwangsmassnahme auf die Daten des Dienstleisters zugreift und über andere Mittel der Re-Identifikation verfügt und auch ein entsprechendes Interesse hat.

122 Im Schweizer Recht sind ungeachtet dessen Situationen denkbar, in denen auch der Dienstleister für Datenschutzverstösse haftet, da er ungeachtet seiner Möglichkeit zur Identifikation der betroffenen Personen an der Bearbeitung deren Daten im Sinne von Art. 28 ZGB «mitwirkt».

sein oder dem Kunden ermöglicht, Daten für ein Auskunftsbegehren abzurufen. Der Kunde hat also auch aus diesem Grund regelmässig ein Interesse daran, einen ADV bzw. einen analogen Vertrag abzuschliessen, weil ihm ein solcher die Kooperation des Dienstleisters vertraglich sichert, auch wenn dies nicht nötig wäre, wenn anderweitig sichergestellt ist, dass der Datenschutz betreffend die Personendaten aus Sicht des Kunden eingehalten ist.

c. *Drittens* kann die Situation eintreten, in welcher der Dienstleister für den Kunden Daten beschafft, ohne dass sie für den Dienstleister Personendaten darstellen. Zu denken ist etwa an den Dienstleister, der pseudonymisierte Daten erhält, diese bei Dritten um zusätzliche Angaben erweitert und die so veredelten Daten dem Kunden zurückspielt. Da die veredelten Daten für den Kunden Personendaten darstellen, liegt seitens des Dienstleisters eine Bekanntgabe von Personendaten vor. Für diese ist der Dienstleister datenschutzrechtlich mitverantwortlich. Unter dem DSG ist er als Mitwirkender erfasst (nicht jedoch als Auftragsbearbeiter),[123] unter der DSGVO – je nach seinem Grad der Autonomie – als gemeinsamer Verantwortlicher (quasi der umgekehrte Fall aus dem Facebook-Fanpage-Urteil, Rz. 72).

c. Fall 2: Zugang zu Personendaten, aber sie sind nicht zu bearbeiten

[Rz 100] Ein Beispiel für die *zweite Fallgruppe* ist ein Dienstleister, der Soft- oder Hardware installiert, konfiguriert, programmiert oder sonst wartet und bei Gelegenheit dieser Handlung auch Personendaten zur Kenntnis nehmen kann, die die Hard- oder Software bearbeitet (z.B. Kopiertechniker nimmt bei der Reparatur eines Kopierers gedruckte Dokumente mit Personendaten wahr, der Softwarespezialist kann beim Fernzugriff auf das Kundensystem oder vor Ort Auszüge der Datenbank sehen, welche von der von ihm gewarteten Software genutzt wird). Solange die Bearbeitung dieser Daten im Namen des Kunden nicht zur Leistung des Dienstleisters gehört, scheidet eine Auftragsbearbeitung aus. Die blosse Kenntnisnahme oder gar nur die Möglichkeit zur Kenntnisnahme stellt noch keine Bearbeitung und erst recht keine Delegation einer solchen dar; auch sind jene Fälle auszuscheiden, in welcher der Dienstleister als eigenständiger Verantwortlicher auftritt (vgl. dazu Rz. 53 f.).

[Rz 101] In einer solchen Situation wird es typischerweise angezeigt sein, dem Dienstleister zu untersagen, etwaige zur Kenntnis genommene Informationen zu verwenden und ihn zur Geheimhaltung verpflichten. Ein ADV ist in diesen Fällen jedoch nicht erforderlich. Der Fall ist vergleichbar mit dem des Reinigungsinstituts in einem Unternehmen, welches bei der Reinigung der Büros ebenfalls personenbezogene Inhalte von Akten auf Schreibtisch oder auf Tafeln in Sitzungszimmern wahrnehmen kann, und sogar angehalten ist, letztere wegzuwischen oder den Müll (mit

123 Vgl. BGE 136 II 508 (Logistep), Erw. 3.4, in welchem die Beschwerdegegnerin ins Recht gefasst wird, obwohl für sie selbst die von ihr beschafften Daten keine Personendaten bereitstellen. Das wird teilweise so interpretiert, als sei es nicht erforderlich, dass die Personen für den Auftragsbearbeiter selbst bestimmbar sein müssen. Nach der hier vertretenen Ansicht wird damit in das Urteil etwas hineininterpretiert, was es nicht sagt: Es besagt lediglich, dass der Umstand, dass es sich für die Beschwerdegegnerin nicht um Personendaten handelt, nicht bedeuten kann, dass das Datenschutzgesetz nicht trotzdem auf sie angewandt werden kann. Über die Figur der Mitwirkung an einer Persönlichkeitsverletzung ist dies sichergestellt. Die Figur des Auftragsbearbeiters ist hier nicht relevant; sie spielt im Schweizer Recht lediglich eine Rolle, wenn es um die flankierenden Massnahmen wie z.B. die Betroffenenrechte oder Meldepflichten geht. Zur Frage, ob ein Verantwortlicher seinerseits Zugang zu Personendaten haben muss, vgl. Rz. 40.

den darin enthaltenen Personendaten) zu entleeren. Auch hier käme niemand auf die Idee, eine Auftragsbearbeitung anzunehmen oder gar einen ADV abzuschliessen. Hingegen kann es nötig sein, die Musterklauseln der Europäischen Kommission für Controller-Controller-Transfers abzuschliessen, falls der Dienstleister sich in einem Land ohne angemessenen Datenschutz befindet und die Personendaten dort zur Kenntnis nehmen kann (z.B. via Fernzugriff): Auch wenn der Dienstleister mit den Daten nichts tut, so sind sie ihm trotz allem bekanntgegeben im Sinne des DSG bzw. der DSGVO, weil er sie wahrnehmen kann. Sobald er sie entgegen seinem Auftrag doch bearbeiten sollte, würde er als Verantwortlicher gelten. Darum passen die Musterklauseln für Auftragsbearbeiter nicht in dieser Konstellation.

[Rz 102] Insbesondere die Deutsche Lehre und Praxis vertritt selbst seitens der Datenschutzbehörden[124] trotzdem immer wieder, dass die Prüfung und Wartung von Datenverarbeitungsanlagen (z.B. Fernwartung, Support) ebenfalls eine Auftragsbearbeitung darstelle, wenn bei diesen Tätigkeiten ein Zugriff auf Personendaten nicht auszuschliessen ist. Dieses Verständnis ist überholt. Es hat seinen Grund im früheren, nationalen deutschen Recht, wo dieser Tatbestand *ex lege* der Auftragsbearbeitung zugeordnet wurde, da er aus systematischer Überlegung keine solche ist, der Gesetzgeber ihn aber erfassen wollte.[125] Mit der DSGVO ist diese Sonderregelung hinfällig geworden, da sie keine solche vorsieht und für eine solche Interpretation auch keinen Raum lässt. Im aktuellen Bundesdatenschutzgesetz ist sie daher nicht mehr enthalten. Es bleibt zu hoffen, dass die Datenschutzbehörden ihre diesbezüglichen Ausführungen an die neue Rechtslage anpassen, da dies in der Praxis immer wieder zu Irritationen führt. Die Ansichten bezüglich dieser Frage gehen allerdings auch in der deutschen Literatur auseinander. Es wird dabei nach Argumenten gesucht, wie die ehemalige deutsche Sonderposition auch unter der DSGVO begründet werden kann. Das ist wenig sachgerecht, da die Subsumption schon unter die Auftragsbearbeitung unter dem früheren deutschen Recht nie aus der Sache begründet war und dies auch heute nicht ist.[126]

---

124 Z.B. Bayerisches Landesamt für Datenschutzaufsicht, FAQ zur DS-GVO, Auftragsverarbeitung, Abgrenzung, 20. Juli 2018 (https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf), S. 1; Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder (DSK), Kurzpapier Nr. 13, Auftragsverarbeitung, Artikel 28 DS-GVO, S. 4; CNIL, General Data Protection Regulation: a guide to assist processors, https://www.cnil.fr/en/general-data-protection-regulation-guide-assist-processors («digital service companies (formerly known as IT engineering service companies/SSII in French) who have access to data»).

125 Vgl. den früheren § 11 Nr. 5 BDSG (vor der DSGVO). Dazu etwa Jürgen Hartung: in: Kühling/Buchner (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz. Kommentar, 2. Aufl., München 2018, Art. 28 N 53.

126 Die Argumentation ist, dass sich die alte Position unter der DSGVO damit wieder erschaffen lässt, indem der Begriff der Offenlegung i.S. von DSGVO 4(2) weiter verstanden würde als der Begriff der Übermittlung nach (alt)BDSG 11 Nr. 5, bereits die Möglichkeit der Kenntnisnahme bei einer Wartungsarbeit eine Datenbearbeitung sei, die als Auftragsdatenbearbeitung gelten müsse (also die Kenntnisnahme bereits eine Verarbeitungshandlung sei) (Hartung, ebd.). Wäre dem so, wären unzählige Vorgänge im Alltag ebenfalls datenschutzrelevant, weil jeder Mensch überall die Gelegenheit zur Wahrnehmung von Personendaten hat, ob er im Zug andere Gespräche mitbekommt, der Handwerker beim Einbau einer Waschmaschine auf dem Küchentisch einen Bussenzettel sieht oder eine Zeitung das Bild einer Strasse abdruckt, auf welchem im Hintergrund Menschen erkennbar zu sehen sind und dieses Bild von jedem Zeitungsleser zur Kenntnis genommen werden kann. Andere halten der Subsumption unter die Auftragsbearbeitung dementsprechend entgegen, dass die zufällige Kenntnisnahme von Daten im Rahmen einer Wartungsleistung sei keine planmässige Datenbearbeitung und damit auch keine Auftragsdatenbearbeitung (Rudi Kramer, in: Gierschmann/Schlender/Stentzel/Veil (Hrsg.), Kommentar. Datenschutz-Grundverordnung, Köln 2018, Art. 28 N 21), der auch auf die Meinungsvielfalt hinweist. Andere Stimmen wollen statt Art. 28 DSGVO in solchen Fällen Art. 26 DSGVO analog angewandt wissen. Diese Lehrmeinungen verkennen, dass in Fällen, wo Personendaten bloss zur Kenntnis genommen werden können, jede datenschutzrechtliche Verantwortlichkeit fehl am Platz ist, sofern keine Bearbeitung stattfindet, weil sie gar nicht wahrgenommen werden könnte. Handlungsbedarf gibt es in solchen Fällen einzig bezüglich der Wahrung der Vertraulichkeit, was mit einer simplen Geheimhaltungsklausel mit Verwendungsverbot geregelt werden kann – mehr ist nicht nötig und macht auch datenschutzrechtlich überhaupt keinen Sinn. Nur aber immerhin dann, wenn der Dienstleister die von ihm wahrgenommenen

[Rz 103] Zu einer Auftragsbearbeitung kann es im Rahmen von Wartung und Support natürlich trotzdem kommen. Das gilt dort, wo die Leistung auch die Bearbeitung von Daten des Kunden für diesen umfasst. Wenn beispielsweise ein Datenbankspezialist sich nicht nur um die richtige Konfiguration des Datenbankmanagementsystems kümmert, sondern auch die Datenbestände (die Personendaten enthalten) mit Hilfe seiner Werkzeuge neu organisiert, durchsucht oder konvertiert, um beispielsweise mehr Leistung oder Stabilität für den Kunden zu erreichen, besteht ein Teil seiner Leistungen darin, Personendaten des Kunden für diesen zu bearbeiten. Er wird Auftragsbearbeiter. Nicht hinreichend ist allerdings, wenn er durch seine Manipulationen an einer Software oder Hardware eine Datenbearbeitung auslöst (z.B. in einem darunterliegenden Datenbanksystem) oder wenn er im Rahmen seiner Leistung zufällig mit Personendaten in Kontakt kommt und sie benutzt (z.B. der Kopiertechniker, der testet, ob der Kopierer nun funktioniert und ein Dokument mit Personendaten, das zuvor Probleme bereitete, zu kopieren probiert). Solche zufälligen Bearbeitungen, auch wenn sie für die Zwecke der Leistungserbringung erfolgen, lösen in der Regel keine Auftragsbearbeitung aus, da es regelmässig am Willen der Delegation einer Datenbearbeitung und damit am begriffsnotwendigen Auftrag fehlt (zum Ansatz, sie komplett zu ignorieren: Rz. 85). Wahrscheinlicher ist ein Fall von Art. 29 DSGVO (dazu sogleich Rz. 104 ff.). Liegt auch dieser nicht vor, weil die Person nicht unter der Aufsicht des Kunden tätig ist oder sich nicht an die Weisungen hält, bleibt jedenfalls im heutigen System nur die Möglichkeit, dass der Datenbearbeiter ebenfalls Verantwortlicher ist – zum Beispiel, wenn der Kopiertechniker das beim Kunden vorgefundene Dokument mit Personendaten mitnimmt und für sich selbst verwendet.

17. Datenbearbeiter, aber weder Verantwortlicher noch Auftragsbearbeiter?

a. Personen, die «unter der Aufsicht» arbeiten

[Rz 104] Im Geltungsbereich der DSGVO ist zu beachten, dass nebst der Qualifikation des Dienstleisters als Verantwortlicher oder Auftragsbearbeiter noch eine dritte Rolle möglich ist, die in der Praxis oft übersehen wird. Es ist die Bearbeitung von Personendaten *unter der Aufsicht* eines Verantwortlichen oder Auftragsbearbeiters und ist in Art. 29 DSGVO geregelt. Für diese Fälle sieht die DSGVO vor, dass die betreffenden Personen Personendaten nur auf Weisung des betreffenden Verantwortlichen oder Auftragsbearbeiters bearbeiten dürfen.

[Rz 105] Der klassische Anwendungsfall ist der eigene Mitarbeiter, wobei der Festangestellte ebenso erfasst ist wie der lediglich auf Stundenbasis tätige Arbeitnehmer. Erfasst sind allerdings auch alle anderen Personen, die wie ein Arbeitnehmer in die interne Arbeitsorganisation integriert bzw. in dieser tätig sind, wie z.B. das von Personalverleihunternehmen einem Einsatzbetrieb zur Verfügung gestellte Personal oder freie «externe» auf Mandatsbasis agierende Mitarbeiter, deren Leistung im Zurverfügungstellen ihrer Arbeitskraft steht.[127] Ein weiteres Beispiel sind entsandte Mitarbeiter oder sog. *Secondments*, also beispielweise Mitarbeiter, die eine Anwalts-

Personendaten selbst zu verwenden beginnt, liegt ein datenschutzrechtlich relevanter Vorgang vor; in diesen Fällen ist der Dienstleister typischerweise selbst Verantwortlicher und kann erfasst werden.

127 Hartung (Fn. 125), Art. 29 N 13; Mario Martini, in: Paal/Pauli (Hrsg.), Datenschutzgrundverordnung Bundesdatenschutzgesetz. Beck'sche Kompakt Kommentare, 2. Aufl., München 2018, Art. 29 N 14.

kanzlei oder ein Beratungsunternehmen ihrem Klienten für eine bestimmte Zeitdauer überlässt, damit sie nach Weisung des Klienten tätig sind.

[Rz 106] Immer sind es die natürlichen Personen selbst, d.h. nicht die Unternehmen, bei welchen sie möglicherweise arbeitsrechtlich angestellt sind. Auf die rechtliche Qualifikation des Vertragsverhältnisses zum Verantwortlichen bzw. Auftragsbearbeiters bzw. ob ein solches überhaupt direkt besteht, kann es nicht ankommen. Entscheidend muss sein, wie auch in Art. 29 DSGVO festgehalten, dass die natürliche Person unter der Aufsicht und Weisungsgewalt («authority») des Verantwortlichen bzw. Auftragsdatenbearbeiters steht und jede Datenbearbeitung nur diesem dient.[128] So ist auch der Mitarbeiter eines Reinigungsinstitut, der bei einem Kunden tätig ist und dort in den Büros nach den Vorgaben des Kunden den Abfall entsorgt, welcher auch Personendaten auf den Couverts und Dokumenten enthält, eine unter der Aufsicht des Kunden tätige Person, auch wenn die Anweisungen an die Reinigungskraft vom Kunden via Reinigungsinstitut erfolgen und höchstens ausnahmsweise direkt. Sollte bei diesem Kunden versehentlich heikle Unterlagen im Abfalleimer landen und die Reinigungskraft entsorgt sie daher datenschutzwidrig, wäre denn auch der Kunde alleine dafür verantwortlich. Verletzt die Reinigungskraft hingegen die Vorgaben des Kunden, ist sie analog zum vertragsbrüchigen Auftragsbearbeiter Verantwortliche.

b. Kein ADV erforderlich

[Rz 107] Im Unterschied zu Art. 28 DSGVO ist bei solchen Personen kein ADV erforderlich; es genügt ein Vertrag mit den entsprechenden Weisungsrechten und die Ausübung dieser Weisungsrechte, um die Datenschutzkonformität der Datenbearbeitung sicherzustellen, da es sich um eine originär gesetzliche und damit auch unmittelbar sanktionierte Pflicht handelt.[129] Solche Weisungsrechte können sich aus der Natur des Vertrags auch ohne besondere Vereinbarung ergeben wie etwa beim Arbeitsvertrag, oder aber sie werden spezifisch festgehalten.

[Rz 108] Weder das DSG noch E-DSG kennen eine analoge Bestimmung zu Art. 29 DSGVO. Unter dem DSG sind auch die internen und externen, aber in die eigene Arbeitsorganisation integrierten Mitarbeiter strenggenommen als Auftragsbearbeiter qualifiziert, doch geht die herrschende Lehre und Praxis davon aus, dass sie weder das eine noch das andere sind, sondern sie letztlich dem Verantwortlichen bzw. Auftragsdatenbearbeiter schlicht zugerechnet werden. Die Erwartung an ihn ist, dass er sie im Rahmen seines Weisungsrechts kontrolliert und ihnen nur jene Datenbearbeitung erlaubt, die auch ihm selbst erlaubt ist, d.h. sie *analog* einem Auftragsdatenbearbeiter behandelt. Sie gelten wie der Auftragsdatenbearbeiter nicht als «Dritte». Im Ergebnis gilt das gleiche wie unter der DSGVO: Jeder Verantwortliche und Auftragsbearbeiter muss sicherstellen, dass die Personen, die er zur Bearbeitung von Personendaten beizieht – wie in Art. 10a DSG heute schon festgehalten –, nur das tun, was er selbst auch tun darf und die Datensicherheit wahren. Dies erfordert typischerweise ein umfassendes vereinbartes Weisungsrecht und eine Verpflichtung zur Geheimhaltung, soweit sich dies nicht bereits anderweitig wie z.B. aus Gesetz ergibt.

128 Hartung (Fn. 125), Art. 29 N 17 f.

129 Hartung (Fn. 125), Art. 29 N 5;

18. Zusammenfassung und Fazit

a. Verantwortlich ist, wer über Zweck und Parameter der Datenbearbeitung entscheidet

[Rz 109] Zusammenfassend lässt sich festhalten, dass wann immer das datenschutzrechtliche Verhältnis zwischen Kunde und seinem Dienstleister zu ermitteln ist, zunächst zu bestimmen ist, welches die Datenbearbeitungen sind, die jeweils eine logische Einheit bilden, und wer für die einzelnen Datenbearbeitungen die datenschutzrechtliche *Verantwortung* trägt. Letztere bestimmt sich nicht danach, für wen die Datenbearbeitung durchgeführt wird oder wem die Verantwortung auf dem Papier zugewiesen wurde, sondern wer die Datenbearbeitung im Innen- oder Aussenverhältnis faktisch oder rechtlich kontrolliert: Verantwortlich ist zunächst jeder, der die Datenbearbeitung veranlasst oder zumindest ihr Ziel mitbestimmt («Entscheid über Zwecke»). Verantwortlich ist sodann jeder, der die datenschutzrechtlichen Parameter der Datenbearbeitung in eigener Regie mitbestimmt («Entscheid über Mittel»). Gemeint sind die materiellen Parameter der Datenbearbeitung, die für die Bestimmung der datenschutzrechtlichen Zulässigkeit oder datenschutzrechtlichen Risiken der Bearbeitung von Relevanz sind (welche Kategorien von Daten bearbeitet werden, woher sie stammen, wie sie ausgewertet und verknüpft werden, wie lange sie aufbewahrt werden, wem sie mitgeteilt werden, etc.), nicht jedoch andere Aspekte wie etwa die eingesetzte Infrastruktur, die Mittel zur Gewährleistung der Datensicherheit oder die Massnahmen zur Wahrung der Betroffenenrechte.

b. Es kann sein, dass mehrere Stellen relevante Entscheide treffen

[Rz 110] Die Kontrolle kann bei ein und derselben Datenbearbeitung auf mehrere Stellen verteilt sein, d.h. es können mehrere Personen, mithin Kunde *und* Dienstleister mitbestimmen, in welchem Falle eine *gemeinsame Verantwortlichkeit* vorliegt; in diesem Fall müssen nicht alle Verantwortlichen Zugang zu den Personendaten haben. Es ist aber auch denkbar, dass der Kunde und der Dienstleister jeweils eigenständige Verantwortliche für die in ihrer Sphäre stattfindenden Datenbearbeitungen sind. Die Sphären können durchaus eng miteinander verknüpft sein. Überlagern sie sich, kommt das *Ebenenmodell* zum Zug: Findet die vom Dienstleister kontrollierte Datenbearbeitung auf einer logisch anderen Ebene statt als jene, die der Kunde kontrolliert und ist es das Verständnis, dass der eine jeweils nicht in die Ebene des anderen eingreifen soll,[130] so gelten sie als eigenständige Verantwortliche. Sind die beiden Datenbearbeitungen hingegen aus der Distanz betrachtet als logische Einheit zu verstehen,[131] so sind sie gemeinsame Verantwortliche.

[Rz 111] Der Dienstleister ist insbesondere dort *eigenständiger Verantwortlicher*, wo die Datenbearbeitung «nur» Mittel zum Zweck seiner Leistung ist oder damit er eine ihm auferlegte gesetzliche Pflicht erfüllen kann, es also seine Datenbearbeitung und nicht jene des Kunden ist – auch wenn natürlich alles, was er tut, primär dem Kunden dient und er sogar abgesehen von der Datenbear-

130 So wie der Fernmeldedienstanbieter sich nicht darum kümmert, was seine Kunden übermitteln, während diese sich nicht darum kümmern, wie es der Anbieter tut.

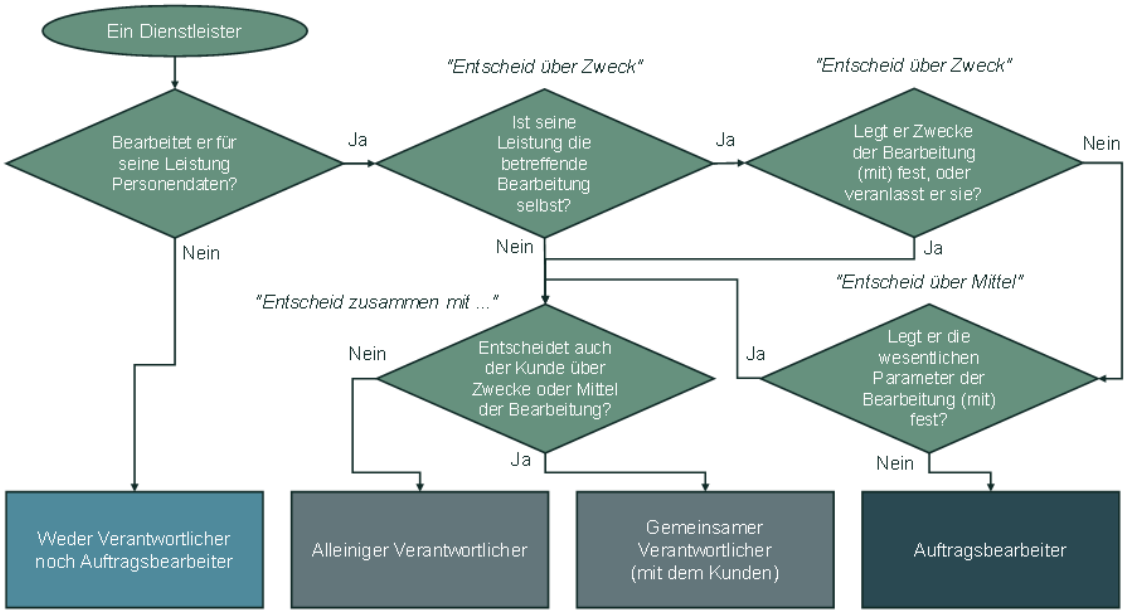
131 Eine logische Einheit kann z.B. bilden, was demselben Zweck dient und allenfalls sogar weitere datenschutzrechtliche Parameter teilt, was von derselben Person oder einheitlich kontrolliert wird, was in der Aussenwirkung hin als Einheit erscheint, was datenschutzrechtlich einheitlich zu behandeln ist, was untrennbar miteinander verkettet ist.

beitung unter seiner Weisung agiert. Auch dort, wo ein Dienstleister die ihm von seinen Kunden anvertrauten Daten auch für eigene Zwecke nutzt oder selbst festlegen will, was seine Kunden damit tun können, ist er Verantwortlicher. Ist der Kunde selbst die betroffene Person, ist der Dienstleister ohnehin der Verantwortliche, weil das Datenschutzrecht nichts anderes vorsieht.

c. Wer nur über die Ausführung entscheidet, ist nicht Verantwortlicher

[Rz 112] Ist der Dienstleister nicht Verantwortlicher, weil er lediglich die Datenbearbeitung seines Kunden durchführt, auch wenn ihm dabei die Auswahl der technischen und organisatorischen Massnahmen und restlichen, nicht wesentlichen Mittel überlassen ist, gilt er als *Auftragsbearbeiter*. Es steht ihm als solcher zwar frei, sein Leistungsangebot zur Durchführung der Datenbearbeitung des Kunden selbst zu definieren. Es ist aber der Kunde, der entscheidet, ob und wie lange er es einsetzen will und damit Verantwortlicher der Datenbearbeitung bleibt. Hat ein Dienstleister zwar Zugang zu Personendaten (d.h. er kann sie zur Kenntnis nehmen), aber nicht den Auftrag, sie zu bearbeiten (d.h. er tut nichts damit), so scheidet er als Auftragsbearbeiter allerdings aus; es genügt, wenn in solchen Fällen sichergestellt ist, dass er die Vertraulichkeit wahrt und die Daten nicht doch bearbeitet.

[Rz 113] Vereinfacht dargestellt ergibt sich damit folgendes Prüfschema:



d. Vor- und Nachteile der möglichen Rollen

[Rz 114] Die Qualifikation des Dienstleisters als Verantwortlicher oder Auftragsbearbeiter hat gewichtige Folgen. Ist der Dienstleister …

a. *Auftragsbearbeiter*, so darf er mit den Daten nur tun, was ihm sein Kunde angewiesen hat, ist dafür aber jedenfalls unter der DSGVO von Haftung für Datenschutzverstösse weitgehend

geschützt, soweit er sich an diese Anweisungen und Vorgaben des Auftragsdatenbearbeitungsvertrags (ADV) hält, der zwingend vorgeschrieben ist (siehe Anhang «*Was in einen ADV gehört*»). Als Auftragsbearbeiter darf er die für seinen Kunden bearbeiteten Personendaten nicht für eigene Zwecke benutzen. Er muss seinem Kunden Datensicherheitsverletzungen sofort melden und ihn bei seiner Compliance unterstützen. Der Kunde braucht unter der DSGVO keinen separaten Rechtsgrund, um den Auftragsbearbeiter beizuziehen und muss sich auch um den Grundsatz der Zweckbindung und Transparenz in aller Regel keine Sorgen machen. Aber er übernimmt mit dem Auftragsbearbeiter das Risiko, dass dieser sich nicht an die Weisungen hält und muss sich vergewissern, dass er die nötige Datensicherheit bietet. Er haftet für ihn, seine Handlungen und seine Unzulänglichkeiten. Immerhin muss ihm der Auftragsbearbeiter am Ende alle Daten zurückgeben.

b. *eigenständiger Verantwortlicher*, so verlangt das Gesetz weder einen ADV, noch ist der Kunde für die Handlungen seines Dienstleisters datenschutzrechtlich direkt verantwortlich, ausser, er übergibt ihm Daten im Wissen darum, dass der Dienstleister damit datenschutzwidrig umgeht. Einen Vertrag wird der Kunde trotzdem meist abschliessen wollen, um die Zweckbindung und die Vertraulichkeit bzw. Datensicherheit sicherzustellen. Denn weil der Dienstleister im Verhältnis zum Kunden ein Dritter ist, darf er ihm Daten nur geben, wenn dieser sie nicht für andere, eigene Zwecke bearbeitet oder aber die betroffenen Personen darüber bei der Datenbeschaffung informiert wurden oder dem zugestimmt haben; oft ist der Dienstleister aber Verantwortlicher, gerade weil er die Daten für eigene Zwecke verwendet und nicht wie ein Auftragsbearbeiter vom Kunden umfassend kontrolliert werden will, was den Beizug datenschutzrechtlich komplizierter macht. Das gilt unter der DSGVO erst recht, wo jede Datenbearbeitung einen Rechtsgrund braucht. Immerhin muss der Dienstleister als eigenständiger Verantwortlicher alle Pflichten aus dem Datenschutz selbst erfüllen, einschliesslich die Erfüllung der Betroffenenrechte (Informationspflicht, Auskunftsrechte, Löschpflicht, etc.) und etwaige Meldepflichten. Er kann nicht wie der Auftragsbearbeiter auf den Kunden weiterverweisen oder davon ausgehen, dass er sich um diese Dinge kümmert.

c. *gemeinsamer Verantwortlicher*, so ist jedenfalls unter der DSGVO ein Vertrag vorgeschrieben, der im Innenverhältnis die datenschutzrechtlichen Verantwortlichkeiten regelt (z.B. wer sich um die Information der betroffenen Personen kümmert[132]). Einen solchen Vertrag werden der Kunde und Dienstleister schon aus eigenem Interesse abschliessen: Datenschutzrechtlich stehen die beiden im selben Rang, können einander keine Weisungen erteilen. Doch den Pflichten aus dem Gesetz wie etwa die Informationspflicht, das Auskunftsrecht, Meldepflichten, Pflicht zur Datenschutz-Folgenabschätzung und sowieso die Einhaltung des Datenschutzes unterliegen beide. Verletzt einer die Vorgaben, haftet der andere grundsätzlich solidarisch mit, es sei denn, er kann zeigen, dass er in keinerlei Hinsicht verantwortlich ist. Immerhin kann vertreten werden, dass der Austausch von Daten zwischen Kunde und Dienstleister analog der Situation beim Auftragsbearbeiter datenschutzrechtlich erleichtert ist. Benutzt der Dienstleister Daten für andere Zwecke als jene des

132 Vgl. etwa das Muster des Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg, abrufbar unter https://bit.ly/2K0UYBZ.

Kunden, erfordert dies wie beim eigenständigen Verantwortlichen eine entsprechende Information und unter der DSGVO einen eigenen Rechtsgrund, was kompliziert sein kann.

[Rz 115] Vor diesem Hintergrund ist klar, dass jede der Konstellationen ihre Vor- und Nachteile hat. Der Unterschied zwischen den drei Konstellationen besteht vor allem im Mass an Autonomie, die der Dienstleister im Rahmen der Datenbearbeitung hat, die in seiner Sphäre stattfindet. Je mehr Autonomie ein Dienstleister hat, desto grösser ist allerdings auch seine datenschutzrechtliche Verantwortung.

e. Auf das Bauchgefühl hören

[Rz 116] In der Praxis hat sich ein gesamtheitlicher Ansatz bewährt: Die Frage, ob ein Dienstleister Verantwortlicher oder bloss Auftragsbearbeiter ist, sollte nicht losgelöst von den dargestellten Vor- und Nachteilen beurteilt werden. Stattdessen sollte umgekehrt gefragt werden, wo die Verantwortung für und die Entscheidungsgewalt bzw. Autonomie über eine bestimmte Datenbearbeitung angesichts der Umstände am besten angesiedelt ist, damit sowohl die Anliegen des Datenschutzes (wie z.B. Erfüllung von Betroffenenrechten, Sicherstellung der Einhaltung der Bearbeitungsgrundsätze) als auch die wirtschaftlichen Interessen der Beteiligten am besten erfüllt sind. Die Frage an das Bauchgefühl hilft hier oft weiter: Wen sehen die betroffenen Personen am ehesten als für die inhaltlich korrekte Behandlung ihrer Daten als Verantwortlich an? Wen würden sie bei Datenschutzanliegen kontaktieren? Diese Person sollte auch rechtlich mindestens mitverantwortlich sein. Ist die Beziehung zwischen Kunde und Dienstleister entsprechend ausgestaltet, zeichnet der Vertrag nur noch nach, was ohnehin gilt.

David Rosenthal, lic. iur., Konsulent, Homburger AG, Zürich, Schweiz, Lehrbeauftragter an der Universität Basel und der eidg. Technischen Hochschule Zürich, david.rosenthal@homburger.ch.

Interessenbindung: Dieser Beitrag diskutiert zahlreiche Beispiele auch aus der Beratungspraxis des Autors. Der Autor dankt herzlich David Vasella, Barbara Epprecht, Luca Dal Molin, Robert Bächtiger, Sergio Greco, Ralph Gramigna, Maria Winkler, Michal Cichocki, Renate Lang, Heribert Grab und allen weiteren Personen in meinem Umfeld, insbesondere im Verein Unternehmens-Datenschutz (VUD), für die fruchtbaren Diskussionen zum Thema und Unterstützung zu diesem Beitrag.

Anhang: Was in einen ADV gehört

In der Schweiz regelt das Datenschutzgesetz (**DSG**) nicht, was genau in einen Auftragsdatenbearbeitungsvertrag (**ADV**) gehört. Art. 10a DSG besagt nur, dass der Auftraggeber sicherstellen muss, dass der Auftragsbearbeiter die Daten so bearbeitet, wie er dies selbst auch tun dürfte, und er muss sich vergewissern, dass die Datensicherheit gewährleistet ist. Im revidierten DSG soll Art. 8 zusätzlich vorsehen, dass der Auftragsbearbeiter die Datenbearbeitung nur dann an weitere Personen delegieren darf, wenn dem der Auftraggeber schriftlich zugestimmt hat, wobei es analog zur Regelung unter der DSGVO genügen soll, dass dem Auftraggeber ein Widerspruchsrecht eingeräumt wird. Der Begriff der Schriftlichkeit meint zudem nicht eine solche nach Art. 14 OR; auch online soll der Abschluss eines ADV möglich sein.

Im Kern muss ein ADV nach Schweizer Recht daher in erster Linie vorsehen, dass der Auftragsbearbeiter die Personendaten für den Auftraggeber nur nach dessen Weisungen bearbeitet. Der Auftraggeber hat solche selbstredend DSG-konform zu erteilen, weshalb in dem meisten Fällen ein ADV auch noch weitere Bestimmungen zu diversen Themen wie Datensicherheit, Export von Daten, Bearbeitungszweck und Unterstützungspflichten enthält. Die flexible Lösung im Schweizer Recht bedeutet allerdings auch, dass ein ADV je nach den Umständen unterschiedlich ausführlich sein darf und kann, oder je nach Situation sogar ganz fehlen kann, wenn sich das Weisungsrecht auch anders ergibt und genutzt wird.

Anders verhält es sich unter der DSGVO. Hier schreibt Art. 28 acht Punkte vor, die jeder ADV abdecken muss, nebst einer allgemeinen Umschreibung der Datenbearbeitung. Der Vertrag muss schriftlich erfolgen, was auch die elektronische Form umfasst. Die 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;
- 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 DSGVO macht keine Vorgaben darüber, wer die mit den Pflichten verbundenen Kosten zu tragen hat, ebenso nicht zu den Themen Haftungsausschlüsse oder Schadloshaltung im Innenverhältnis. Die DSGVO macht auch keine Vorgaben zu den Pflichten des Verantwortlichen, sondern lediglich, dass sie irgendwo festzuhalten sind. Hier sind beliebige Regelungen denkbar, jedenfalls soweit sie dem Schutzzweck der DSGVO nicht zuwiderlaufen. In der Praxis führen sie regelmässig zu Diskussionen, da Kunden oft eine umfassende Freistellung wünschen, Dienstleister diese aber nicht zu geben bereit sind.

Liegt kein besonders heikler Fall vor, kann ein ADV knapp gehalten sein; es wird in vielen Fällen sogar genügen, sich bezüglich der acht Punkte an den knappen Wortlaut des Art. 28 DSGVO zu halten. Es zirkulieren unterschiedlichste ADV, und teils auch solche mit sehr ausführlichen Regelungen.[133] Die Praxis zeigt allerdings auch, dass Unternehmen ADV vielfach ohne tatsächliche Befassung mit ihrem Inhalt abschliessen und die Vorgaben von Art. 28 DSGVO daher faktisch zu einer Formalität und bürokratischen Übung verkommen. Insofern erscheint das Schweizer Vorgehen – einmal mehr – wesentlich vernünftiger.

Ein direktes Übernehmen von Verträgen nach Art. 28 DSGVO kann zwar sinnvoll sein, ist aber nicht unproblematisch. Üblicherweise sind für die Schweiz Anpassungen erforderlich, da die einzelnen Pflichten auf die DSGVO und deren Bestimmungen ausgerichtet sind und diese in aller Regel auch direkt referenzieren (z.B. Verweis auf Kapitel III der DSGVO und Art. 32 bis 36 DSGVO). Untersteht der Verantwortliche (auch) dem DSG, muss in diesen Fällen eine Referenz auf die entsprechenden Bestimmungen des DSG aufgenommen werden. Dies ist insbesondere auch in jenen Fällen zu beachten, indem ein Vertrag nach Art. 28 DSGVO deshalb zur Anwendung gelangt, weil der Auftragsbearbeiter (und nicht der Verantwortliche) der DSGVO untersteht und daher zum Abschluss eines solchen Vertrags verpflichtet ist. Die Erfahrung zeigt, dass sich Auftragsbearbeiter aus dem EWR oft nicht bewusst sind, dass ihre Verträge für Kunden in der Schweiz nicht ohne Weiteres passen, auch wenn die Schweizer Regelungen sehr ähnlich sind. Anpassungen können ferner mit Bezug auf die Bestimmungen zum Datenexport erforderlich sein, wie sie sich in vielen ADVs finden. Hier ist sicherzustellen, dass nicht nur der Export aus dem EWR, sondern auch der Export aus der Schweiz geregelt ist.

Befindet sich der Auftragsbearbeiter in einem Land ohne angemessenen Datenschutz und greift nichts anderes, wird es allerdings erforderlich sein, zusätzlich die Musterklauseln der Europäischen Kommission für Auftragsbearbeiter abzuschliessen. An sich lassen sich die Vorgaben von Art. 28 DSGVO ausschliesslich mit den Musterklauseln erfüllen, wenn die darin heute verlangten Massnahmen zur Datensicherheit auch das Datengeheimnis abdecken und die Pflicht zur Unterstützung des Verantwortlichen bezüglich seiner Anfragen breit verstanden würde. In der Praxis geschieht dies allerdings nicht; für Art. 28 DSGVO wird in aller Regel ein eigener Wortlaut verwendet, der sich stärker an Art. 28 DSGVO anlehnt. In beiden Fällen – dem ADV und den Musterklauseln – muss die Datenbearbeitung im Vertrag ebenfalls umschrieben werden, wobei Art. 28 DSGVO etwas mehr verlangt als der Anhang der Musterklauseln dazu standardmässig vorsieht.[134]

Das Weisungsrecht sorgt in der Praxis für die meisten Diskussionen, da es erstens Kostenfolgen mit sich bringen kann (wenn der Dienstleister angewiesen wird, etwas anderes zu tun, als der Vertrag vorsieht) und zweitens den Eindruck vermittelt, dass ein Dienstleister von jedem Kunden individuelle Weisungen erhalten kann. Es ist heute allerdings weitgehend akzeptiert, dass ein Dienstleister festhalten kann, dass sich die Weisungen des Kunden darin erschöpfen, dass der Kunde genau das tut, was im Vertrag von Anfang an vorgesehen ist, der Vertrag als die verbindlichen und abschliessenden Weisungen darzustellen. Will der Kunde sie ändern und ist der Dienstleister nicht einverstanden, muss er kündigen. Wie weit der Dienstleister dabei gehen kann, wird sich allerdings erst noch zeigen müssen.

Anhang: Die Tabelle mit Beispielen aus der Praxis finden Sie hier.

133 Vgl. etwas das Muster 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/.

134 So z.B. die Dauer der Datenbearbeitung und deren Art und Zweck der Bearbeitung sowie die Rechte und Pflichten des Verantwortlichen. Der Anhang zu den Musterklauseln sieht diesbezüglich nur eine Beschreibung der Bearbeitungsaktivitäten des Auftragsbearbeiters vor.

Anhang: Beispiele aus der Praxis: Controller oder Processor?

Gehört zum Jusletter-Beitrag «Controller oder Processor: Die datenschutzrechtliche Gretchenfrage» von David Rosenthal; die angegebenen Randziffern befinden sich im betreffenden Beitrag.

Illustrativ ist auch die Auflistung des BayLDA unter https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf, deren Zuordnung und Begründung vorliegend allerdings nicht durchgängig geteilt wird (vgl. insb. Rz. 102).

Fallkonstellation	Verantwortlichkeit	Rz.
Eine Bank führt **Zahlungsaufträge** ihrer Kunden aus.	Die Bank und ihre Kunden sind jeweils eigenständige **Verantwortliche**.	31
Ein Unternehmen betreibt einen **Handelsplatz** oder eine Börse, der bzw. die allen Teilnehmern, welche die definierten Voraussetzungen erfüllen, offensteht. Der Betreiber legt fest, wie und was bei ihr gehandelt werden kann und welche Personendaten hierzu wie bearbeitet werden.	Der Betreiber und die Teilnehmer sind jeweils eigenständige **Verantwortliche**.	
Eine **Versicherung** versichert für Unternehmen Risiken im Zusammenhang mit deren Mitarbeitern und erhält diesbezüglich Daten über die Mitarbeiter und Dritte.	Die Versicherung ist eigenständige **Verantwortliche** auch bezüglich der Daten, die sie von ihren Kunden erhält.	30
Ein Finanzintermediär delegiert die Erfüllung von GwG-Sorgfaltspflichten im Bereich der **Identifizierung von Kunden (KYC)** an einen anderen Finanzintermediär, der denselben Kunden hat.	Beide Finanzintermediäre sind eigenständige **Verantwortliche**. Der ausführende Finanzintermediär agiert bereits aufgrund eigener gesetzlicher Verpflichtung und bestimmt damit zunächst alleine über Zweck und Mittel der Datenbearbeitung. Es handelt sich nicht um die Datenbearbeitung des anderen und der andere bestimmt auch nicht mit. Er erfährt lediglich das Ergebnis.	32
Ein **Zahlungsdienstleister** bietet einem Online-Shop-Betreiber die Möglichkeit, Kreditkartenzahlungen entgegenzunehmen.	Der Zahlungsdienstleister ist eigenständiger **Verantwortlicher**. Seine Leistung ist nicht das Bearbeiten von Personendaten, sondern die Entgegennahme von Zahlungen. Die Datenbearbeitung dient ihm lediglich als Mittel zu seinem Zweck, und er legt die dazu nötigen Datenbearbeitungen fest.	31

Fallkonstellation	Verantwortlichkeit	Rz.
Ein Finanzinstitut hat eine **Vertriebsvereinbarungen** mit einer ausländischen Post abgeschlossen, um den Kunden im betreffenden Land den Zugang zu seinen Kontodienstleistungen zu ermöglichen. An den Schaltern greifen die Mitarbeiter der Post direkt auf die Systeme des Finanzdienstleisters zu.	Das Finanzinstitut ist **Verantwortlicher**, während die ausländische Post als sein **Auftragsbearbeiter** auftritt, soweit seine Leistung darin besteht, die Kundendaten in den Systemen des Finanzinstituts zu bearbeiten. Es ist für den Kunden klar, dass der Mitarbeiter am Schalter das Finanzinstitut vertritt und die Daten nicht für sich selbst bearbeitet; es hat diesbezüglich auch klare Vorgaben zu befolgen, was zu tun ist.	
Ein **Anwalt** berät seinen Klienten oder vertritt ihn in einem Prozess.	Der Anwalt ist eigenständiger **Verantwortlicher**.	9
Eine Anwaltskanzlei betreibt für einen Unternehmensverkäufer einen **virtuellen Datenraum** für eine M&A-Transaktion. Die Kanzlei hat hierzu im eigenen Namen einen Dienstleister beauftragt.	Der Anwalt ist mit Bezug auf den Datenraum ein **Auftragsbearbeiter**, der Dienstleister sein **Unterauftragsbearbeiter**. Die Leistung des Anwalts besteht nicht in einer anwaltlichen Leistung, sondern dem Bereithalten von Unterlagen und den darin enthaltenen Personendaten im Namen des Klienten.	29
Eine Versicherung beauftragt einen externen Arzt, ein **Fachgutachten** zu einer bestimmten medizinischen Frage zu erstellen. Der Arzt erhält Unterlagen von der Versicherung, untersucht die betroffene Person aber auch.	Der Arzt ist eigenständiger **Verantwortlicher**, da er bestimmt, zu welchen Datenbearbeitungen es in welcher Weise kommt, damit er das Gutachten verfassen kann. Er erhält zwar auch Unterlagen von der Versicherung; was er aber schlussendlich wie verwertet und noch zusätzlich erhebt, bestimmt er. Der Arzt tritt gegenüber dem Patient ebenfalls eigenverantwortlich auf und ist mangels einer Enthebung an seine Schweigepflicht gebunden.	
Der vertrauensärztliche Dienst einer Krankenkasse lädt immer wieder **externe Ärzte** zu sich ein, um mit diesen Falldossiers zu besprechen. Die Ärzte dürfen diese Dossiers nicht mitnehmen, sondern lediglich ihre Meinung dazu abgeben.	Die Krankenkasse bleibt alleine Verantwortliche. Die externen Ärzte fallen unter die Regelung nach **Art. 29 DSGVO**.	105
Eine Aktiengesellschaft beauftragt einen Dienstleister, ihr **Aktienregister** zu führen und die jährliche **Generalversammlung** für das Unternehmen zu organisieren und durchzuführen.	Der Dienstleister ist mit Bezug auf das Aktienregister ein **Auftragsbearbeiter**; es bleibt das Register des Unternehmens, und der Dienstleister führt es in dessen Namen und nach dessen Weisungen. Hingegen bestimmt bei der Generalversammlung der Dienstleister, welche Datenbearbeitungen es	

Fallkonstellation	Verantwortlichkeit	Rz.
	braucht und wie diese durchzuführen sind. Hier ist er **Verantwortlicher**.	
Die Post **versendet Briefe und Pakete** für ihre Kunden, hält sie zur Abholung bereit, leitet Post um und nimmt **Nachsendeaufträge** an, wobei sie Grosskunden auf angepasste Adressen hinweist, damit diese ihre Post selbst richtig adressieren können.	In allen Fällen tritt die Post als eigenständige **Verantwortliche** auf. Sie bearbeitet Personendaten (Adressen der Empfänger), um ihre Transportleistungen zu erbringen. Sie legt damit den Zweck fest. Ferner bestimmt sie autonom, was sie mit diesen Daten tut, auch wenn es sich um Daten des Kunden handelt. Das gilt auch dann, wenn sie ihren Grosskunden angepasste Adressen aus Nachsendeaufträgen mitteilt; sie tut dies nicht im Auftrag, sondern mit Einwilligung der Personen, die ihr einen Nachsendeauftrag erteilen. Ohnehin kann die Post nicht Auftragsbearbeiter sein, soweit der Auftraggeber die betroffene Person selbst wäre.	87
Ein Logistikunternehmen **verpackt, adressiert und versendet Waren im Auftrag** von Versandhändlern, die diese beim Unternehmen lagern. Es nimmt auch Retouren zurück und verarbeitet diese im Auftrag der Händler.	Das Logistikunternehmen ist **Auftragsbearbeiter,** soweit es um das Adressieren der Pakete und Ausdrucken der Lieferscheine geht, da es hier eine vom Versandhändler bestimmte Datenbearbeitung ausführt und bezüglich der datenschutzrechtlichen Parameter keine Autonomie hat. Dies gilt auch, wenn das Unternehmen personenbezogene Daten aus den Retouren für einen Versandhändler in dessen System erfasst. Bezüglich der Datenbearbeitung für den Versand ist das Logistikunternehmen **Verantwortlicher**.	
Eine **Druckerei** erstellt Prospekte, die auch Personendaten enthalten (Namen, Fotos). Die Druckerei betreibt aber auch eine Versandstrasse, wo sie Rechnungen für ihre Kunden druckt, verpackt und der Post zum Versand übergibt.	Bezüglich dem Erstellen der Prospekte ist die Druckerei, soweit überhaupt eine Datenbearbeitung vorliegt, eine **Verantwortliche**. Im Falle des Rechnungsversands übernimmt die Druckerei jedoch eine Datenbearbeitung ihres Kunden, nämlich die Erstellung persönlicher Rechnungen und deren Adressierung und Versand. Hier wird sie zur **Auftragsbearbeiterin**. Der Kunde bestimmt, wozu und wie die Personendaten bearbeitet werden; die Druckerei führt bloss aus.	
Eine **Telefongesellschaft** ermöglicht es	Die Telefongesellschaft ist **Verantwortliche**,	31

Fallkonstellation	Verantwortlichkeit	Rz.
Unternehmen, zu Firmentarifen Mobiltelefonabos auf die Namen der Mitarbeiter auszustellen. Die Unternehmen können die Abos über ein Online-Portal zentral verwalten. Soll ein neues Abo gelöst werden, gibt das Unternehmen den Namen des Mitarbeiters ein.	auch wenn sie Mitarbeiterdaten des Unternehmens erhält und diesem die Verwaltung seiner Abos anbietet. Es ist die Telefongesellschaft die bestimmt, wozu sie welche Daten wie bearbeitet, auch im Rahmen des Portals. Die Funktionen des Portals beschränken sich darauf, die Vertragsleistungen der Telefongesellschaft für den Kunden nutzbar zu machen und ihm Auswertungen zu erlauben.	
Ein **Reisespezialist** bietet Unternehmenskunden die Buchung von Dienstreisen über ein eigenes Portal an. Als besondere Dienstleistung können die Mitarbeiter über das Portal auch ihre Spesenabrechnungen vornehmen.	Mit Bezug auf die Buchung von Dienstreisen ist der Reisespezialist ein eigenständiger **Verantwortlicher**, da er bestimmt, welche Daten er wozu braucht und erhebt. Soweit er jedoch den Mitarbeitern des Unternehmens erlaubt, ihre Spesenabrechnungen für das Unternehmen online zu erfassen, führt er eine Datenbearbeitung des Unternehmens aus und ist diesbezüglich **Auftragsbearbeiter**.	
Eine Krankenkasse ermöglicht es ihren Versicherten, eine **Fitnessapp** zu nutzen, die ihre täglichen Aktivitäten auswertet. Für diese Aktivitäten erhalten sie von der Krankenkasse Bonuspunkte. Die Fitnessapp wurde von einem Drittunternehmen selbst entwickelt und wird auch von diesem betrieben; die Krankenkasse ist lediglich Lizenznehmerin und erfährt von diesem Unternehmen nur, wieviele Bonuspunkte die Benutzer gesammelt haben. Das Drittunternehmen bestimmt, welche Datenbearbeitungen im Rahmen der App stattfinden und wie. Auf der Fitnessapp erscheint zwar das Logo der Krankenkasse, aber das Drittunternehmen gibt sich als Betreiberin zu erkennen.	Die Krankenkasse ist mit Bezug auf die Bearbeitung der Bonuspunkte eine **Verantwortliche**, die Betreiberin der Fitnessapp hingegen eine eigenständige **Verantwortliche** mit Bezug auf das Tracking der täglichen Aktivitäten. Die Krankenkasse könnte die Fitnessapp allerdings auch in Form einer Auftragsbearbeitung anbieten; in diesem Falle müsste sie sich als Verantwortliche den Zugang zu den Personendaten mindestens für den Ausnahmefall vorbehalten, was sie aus Opportunitätsgründen aber nicht will.	40
Ein Unternehmen **misst** im Auftrag diverser Medienkunden unabhängig die **Online-Reichweite** von deren Internetangeboten. Hierzu ist auf den Websites der Kunden jeweils ein Code installiert, der die zuverlässige Zählung jedes Besuchers erlaubt.	Soweit hierbei überhaupt Personendaten anfallen, bearbeitet das Unternehmen die Daten als eigenständiger **Verantwortlicher**. Zwar veranlassen und ermöglichen die Medienkunden die Zählungen jeweils mit Bezug auf ihre Website. Da die Zählungen jedoch Medium-übergreifend erfolgen und sie in keiner Weise beeinflussen können und sollen, wie das Unternehmen zählt und seine	71, 76

Fallkonstellation	Verantwortlichkeit	Rz.
	Daten bearbeitet, ist der Einfluss der einzelnen Medienkunden zu gering, um ihn als gemeinsame Verantwortlichen zu qualifizieren. Die Erhebung nutzt zwar auch dem einzelnen Medienkunden, dient aber einem übergeordneten Zweck.	
Ein Internetunternehmen bietet einen Service an, mit welchem Betreiber von Websites **Statistiken zur Websitebenutzung** erheben können. Das Internetunternehmen verwendet die Daten nicht für eigene Zwecke.	Das Internetunternehmen ist **Auftragsbearbeiter** der Website-Betreiber, da diese bestimmen, ob und welche Daten von den Benutzern der Websites erhoben werden, soweit überhaupt Personendaten vorliegen. Die Daten werden nur für den Zweck des Website-Betreibers bearbeitet. Es bleibt somit seine Datenbearbeitung.	
Ein **Cloud-Provider** betreibt Server, auf welchem Kunden Speicherplatz und virtuelle Server für den Betrieb ihrer eigenen Anwendungen «mieten» können.	Der Cloud-Provider ist **Auftragsbearbeiter** seiner Kunden, da diese bestimmen, welche Datenbearbeitungen er mit ihren Daten vornehmen soll. Soweit ihm jedoch nur verschlüsselte Daten vorliegen, aus denen er selbst keinen Personenbezug ableiten kann, oder er keinen Zugriff auf den Inhalt der virtuellen Server hat, nimmt er überhaupt keine Datenbearbeitung vor und ist auch kein Auftragsbearbeiter. Mit Bezug auf die Daten zur Inanspruchnahme seiner Dienstleistung (z.B. wer darf zugreifen, da Trouble-Ticket-System), ist er eigenständiger **Verantwortlicher**. Dies ist theoretisch auch dann der Fall, wenn dem Cloud-Provider nur Personendaten des Kunden selbst vorliegen, da der Kunde bezüglich seiner eigenen Daten nie Verantwortlicher sein kann, es ohne einen Verantwortlichen aber auch keine Auftragsbearbeitung gibt.	23, 26, 54, 98
Eine **Maschinenbaufirma** vertreibt ihre Produkte über verschiedene lokale Landesgesellschaften; diese schliessen die Verträge mit den Kunden. Wo diese Landesgesellschaften über keine eigenen Mitarbeiter verfügen, führen Mitarbeiter des **Mutterhauses** dessen Geschäfte; sie stehen diesem im Sinne einer Entsendung zur Verfügung.	Die Landesgesellschaften sind mit Bezug auf die Daten der Mitarbeiter ihrer Kunden, die sie zur Vertragsabwicklung benötigen, **eigenständige Verantwortliche**. Alle Entscheide bezüglich der Datenbearbeitungen werden zwar von Mitarbeitern des Mutterhauses getroffen, aber deren Handlung sind den jeweiligen Landesgesellschaften zuzurechnen, für die sie tätig sind. Sie unterstehen letztlich deren Weisungen. Soweit allerdings das Mutterhaus	

Fallkonstellation	Verantwortlichkeit	Rz.
	relevante Vorgaben an die Datenbearbeitung der Landesgesellschaften macht, ist es mit diesen als **gemeinsame Verantwortliche** zu betrachten.	
Der Betreiber einer Website erlaubt es einem **Werbenetzwerk**, auf seinen Seiten Cookies zu setzen, damit sie diesen Personen über die konkrete Website hinaus nachverfolgen und ihr personalisierte Werbung anzeigen können.	Der Betreiber der Website ist zunächst eigenständiger **Verantwortlicher** mit Bezug auf seine Website. Der Betreiber des Werbenetzwerkes ist ebenfalls eigenständiger **Verantwortlicher**, soweit ihm überhaupt Personendaten vorliegen; sein Netzwerk und die damit verbundenen Datenbearbeitungen betreibt er für sich, auch wenn er es seinen Kunden zur Verfügung stellt. Soweit sein Kunde (also z.B. der Website-Betreiber) jedoch mitbestimmt, von welchen Benutzern Daten erhoben werden oder wie dies geschieht (etwa indem er nicht nur die Werbefläche des Werbenetzwerks in seine Website integriert, sondern diesem selbst Angaben zu den Benutzern übermittelt oder dessen Parameter der Datenerhebung mitsteuert), wird er zum **gemeinsamen Verantwortlichen** mit dem Werbenetz.	71
Ein Fernmeldeanbieter stellt einem Unternehmen **Datenverbindungen** zur Vernetzung der diversen Standorte des Unternehmens zur Verfügung.	Der Fernmeldeanbieter ist eigenständiger **Verantwortlicher**, und zwar nicht nur bezüglich der Randdaten, sondern auch der von ihm transportierten Daten. Er hat bezüglich der dafür nötigen Datenbearbeitungen weitgehende Autonomie. Das Unternehmen bleibt **Verantwortlicher** für die Datenbearbeitungen, die durch die Vernetzung ermöglicht werden.	83
Ein unabhängiger **Versicherungsmakler** berät Kunden beim Abschluss von Versicherungen und hilft diesen, ihre Anträge auf den Online-Systemen der Versicherer zu erfassen. Alternative Konstellation: Ein **Autohändler** hilft dem Kunden beim Abschluss einer Autoversicherung für seinen Neuwagen.	Versicherungsmakler und Autohändler sind eigenständige **Verantwortliche**. Sie erhalten zwar von der Versicherung eine Provision, führen aber keine Datenbearbeitung in deren Auftrag aus. Sie helfen vielmehr dem Kunden, seinen Antrag zu erfassen. Damit werden sie allerdings auch nicht zum Auftragsbearbeiter des Kunden, da der Kunde selbst die betroffene Person ist. Soweit jedoch die Versicherungsgesellschaft den Makler beauftragt, für sie gewisse Arbeiten im Rahmen der Abwicklung der Versicherungsverträge zu übernehmen und	

Fallkonstellation	Verantwortlichkeit	Rz.
	auch Weisungen betreffend die Datenbearbeitung erteilen, die dem Makler diesbezüglich kaum Autonomie lassen, würde er zum **Auftragsbearbeiter**.	
Ein Krankenhaus bietet **Belegärzten** die Möglichkeit, ihre Patienten bei sich behandeln zu lassen. Ferner arbeitet das Krankenhaus mit **selbständigen Therapeuten** zusammen, denen es Patienten überweist, deren Honorar aber über das Krankenhaus abgerechnet wird.	Mit Bezug auf die Bearbeitung der Daten ihrer Patienten durch die Ärzte sind diese wie auch andere freiberufliche Ärzte **eigenständige Verantwortliche**. Mit Bezug auf die Therapeuten ist die Situation insofern anders, als sie Unterakkordanten des Krankenhauses sind. Für die datenschutzrechtliche Verantwortlichkeit ist dies allerdings nicht relevant. Entscheidend ist, welchen Spielraum sie haben: Führen sie eigene Patientenakten und unterstehen sie auch bezüglich der Behandlung der Patienten nicht den Weisungen des Krankenhauses, sind sie diesbezüglich wie die freiberuflichen Ärzte zu behandeln. Soweit sie und das Krankenhaus sich die Krankengeschichten der Patienten auf demselben System teilen, liegt eine **gemeinsame Verantwortlichkeit** vor; dasselbe wäre der Fall, wenn eine Praxisgemeinschaft von mehreren Ärzten eine gemeinsame Patienkartei führt. Sind die Therapeuten in die interne Organisation eingegliedert und arbeiten sie auch fachlich nach Weisung des Krankenhauses, wird in der Regel ein Fall von **Art. 29 DSGVO** vorliegen.	
Eine Person entschliesst sich dazu, eine **Blockchain** oder ein anderes, auf verschiedenen Computer verteiltes Datenbanksystem (*Distributed Ledger Technology*) zur Speicherung von Informationen zu nutzen.	Diese Person wird heute als **Verantwortlicher** betrachtet, soweit die Daten auf einem verteilten Register überhaupt Personendaten darstellen (z.B. der Public Key, der einer einzelnen, identifizierbaren Person zugeordnet werden kann).[1] Kontrolliert hingegen eine einzelne Stelle die Daten, die dem verteilten Register hinzugefügt werden können (z.B. eine *private blockchain*), so gilt diese als **Verantwortliche**. All jene, die ein verteiltes Register bei sich für die Gemeinschaft speichern (und ggf. auch weiterverschlüsseln, d.h. sog. *Miner*), müssen gemäss heutigem Verständnis normalerweise als **Auftragsbearbeiter** gelten, soweit das	

[1] Vgl. die Ausführungen der französischen Datenschutzbehörde CNIL zum Thema (https://www.cnil.fr/en/blockchain-and-gdpr-solutions-responsible-use-blockchain-context-personal-data).

Fallkonstellation	Verantwortlichkeit	Rz.
	Register aus ihrer Sicht Personendaten enthält. Allerdings fehlen in aller Regel die gesetzlich erforderlichen Verträge, und bei nicht zentral kontrollierten DLT-Registern auch ein Verantwortlicher, in dessen Auftrag sie arbeiten können.	
Ein Automobilhersteller bietet seinen Kunden einen Online-Service in seinen Fahrzeugen an, der u.a. die **automatische Benachrichtigung** der vom Kunde voreingestellten **Werkstatt** beinhaltet, sobald es ein Problem gibt oder der Kunde sonst einen Termin will. Die Werkstatt ruft dann den Kunden an, um mit ihm einen Termin zu vereinbaren. Der Hersteller lässt vom Importeur allerdings auch ein **Call Center** für telefonische Anfragen betreiben.	Der Automobilhersteller ist mit Bezug auf den Online-Service selbst eigenständiger **Verantwortlicher**. Die Werkstätten sind ebenfalls eigenständige **Verantwortliche.** Sie haben zwar einen Vertrag mit dem Hersteller und ihre Kontaktaufnahme wird durch seinen Service Lead ausgelöst, sie treten gegenüber dem Kunden aber im eigenen Namen auf und bestimmen selbst über die für den Werkstatttermin erforderlichen Datenbearbeitungen; sie legen Zweck und Mittel fest. Der Importeur ist hingegen **Auftragsbearbeiter**, solange er das Call Center im Namen des Herstellers betreibt.	
Ein Hersteller bietet zu seinen Waren zusätzlich **Online-Dienste** an. Um deren Absatz zu fördern, teilt er seinen Vertriebspartnern mit, welche Kunden sich für diese Dienste bereits registriert haben und welche nicht, damit der Vertriebspartner seine Mitarbeiter entsprechend belohnen bzw. ihnen zusätzliche **Anreize** setzen kann.	Der Hersteller wie auch der Vertriebspartner sind jeweils in ihrem Bereich eigenständige **Verantwortliche**; sie bestimmen in ihrem Bereich jeweils selbst, ob und wie sie die Kundendaten bearbeiten. Es handelt sich um zwei separate Bearbeitungsvorgänge. Anders wäre es, wenn der Vertriebspartner vom Hersteller beauftragt wäre, bestimmten Mitarbeitern direkt gewisse Boni auszubezahlen. In diesem Fall kann der Vertriebspartner zum **Auftragsbearbeiter** werden, oder sie sind **gemeinsame Verantwortliche**, soweit der Vertriebspartner mitbestimmt, wie die Daten bearbeitet werden.	
Ein internationales **Schiedsgericht** bestehend aus drei Schiedsrichtern und einem Sekretär ist konstituiert, über einen Fall mit zwei Parteien zu urteilen. Der Prozess folgt nach den Regeln einer Schiedsinstitution und wird von dieser administriert. Im Prozess kommen auch Experten des Schiedsgerichts zum Einsatz.	Die Parteien sind eigenständige **Verantwortliche** ihrer eigenen Akten und Bearbeitungen, deren Anwälte wiederum jene ihrer Akten und Bearbeitungen. Die einzelnen Schiedsrichter sind – da technisch gesehen individuell mandatiert – jeweils **gemeinsam Verantwortliche** mit Bezug auf die Akten und Bearbeitungen des Schiedsgerichts; soweit die Parteien die Datenbearbeitungen des Schiedsgerichts im	

Fallkonstellation	Verantwortlichkeit	Rz.
	Rahmen der *Terms of Reference* mitbestimmt haben, können sie mit ihnen gemeinsame Verantwortliche werden. Dienstleister wie z.B. *Court Reporters* sind **Auftragsbearbeiter** der beiden Parteien als gemeinsame Verantwortliche oder der Schiedsrichter. Der Sekretär des Schiedsgerichts fällt in der Regel unter **Art. 29 DSGVO**, die Zeugen und Sachverständige in der Regel auch, soweit es um ihre Aussagen an einem vom Schiedsgericht kontrollierten Hearing geht. Experten sind in der Regel eigenständige **Verantwortliche** mit Bezug auf ihre Datenbearbeitungen, die Schiedsinstitution ebenso.	
Eine **Pensionskassenstiftung** beauftragt eine Servicegesellschaft mit der Durchführung der zweiten Säule. Diese greift auf **Rückversicherungen** und **Broker** (die beide teilweise Aufgaben der Servicegesellschaft übernehmen) sowie **Vertrauensärzte** zurück, übermittelt aber auch Angaben an Behörden.	Die Stiftung selbst wird (und darf) in aller Regel keine Personendaten bearbeiten und legt auch nicht fest, welche Datenbearbeitungen stattfinden. Sie erteilt der Servicegesellschaft lediglich ein Mandat, die zweite Säule durchzuführen. Alle Entscheide bezüglich der Datenbearbeitungen, trifft typischerweise die Servicegesellschaft, auch wenn sie dies im Rahmen eines Mandats der Stiftung tut; es ist die Servicegesellschaft, welche die Bearbeitung veranlasst. Die Servicegesellschaft ist daher in aller Regel eigenständige **Verantwortliche**. Soweit sie Aufgaben an eine Rückversicherung oder einen Broker delegiert, sind diese **Auftragsbearbeiter**. Soweit die Rückversicherung jedoch ihre Rückversicherungsleistung anbietet, ist sie eine eigenständige **Verantwortliche**, wie auch die Vertrauensärzte und die Behörden. Erhält der Stiftungsrat trotz allem Personendaten (z.B. als Rekursinstanz), ist er ebenfalls **Verantwortlicher**.	
Sozialpartner vereinbaren einen **Gesamtarbeitsvertrag** (GAV), den sie von einer **Paritätischen Kommission** (PK) vollziehen lassen. Diese lässt die Kontrollen in den Betrieben durch eine spezialisierte **Kontrollinstitution** nach ihren Weisungen durchführen. Die PK speichert ihre Angaben	Die PK erfüllt zwar die Vorgaben gemäss GAV und ist mit Vertretern der Sozialpartner besetzt, hat aber eine eigene Rechtspersönlichkeit und ist in der Regel jene Stelle, die entscheidet was wozu und wie an Daten bearbeitet wird. Sie ist daher eine eigenständige **Verantwortliche**. Die	

Fallkonstellation	Verantwortlichkeit	Rz.
in einer Datenbank, die ein spezialisierter **Lösungsanbieter** betreibt.	Kontrollinstitution ist ihre **Auftragsbearbeiterin**; sie kann zwar über die technischen und organisatorischen Aspekte der Kontrollen entscheiden, aber der Rahmen ist ihr von der PK vorgegeben. Soweit die Sozialpartner in Eigenregie Daten bearbeiten (z.B. Mitgliederverzeichnisse) und nicht bloss in Ausführung von Aufträgen einer PK, sind sie eigenständige **Verantwortliche**.	
Ein **Übersetzer** nimmt Übersetzungen von Texten im Auftrag sein Kunden vor. Ein Konkurrenzunternehmen hat eine Übersetzungssoftware entwickelt und bietet diese als Software-as-a-Service ihren Kunden online an.	Soweit in den Texten Personendaten enthalten sind und es daher auch seitens des Übersetzers zu einer Bearbeitung solcher kommt, bestimmt der Kunde die Zwecke der Datenbearbeitung. Er veranlasst sie und bestimmt damit den Zweck, überlässt es jedoch typischerweise dem Übersetzer, wie er zum Ergebnis kommt. Der Übersetzer wird die Texte zudem für eigene, interne Zwecke nutzen wollen (z.B. für spätere Übersetzungen). Damit bestimmt auch er einen Zweck der Datenbearbeitung sowie die Art und Weise, wie sie erfolgt. Der Übersetzer ist daher **gemeinsamer Verantwortlicher** mit dem Kunden. Anders im Falle der Software: Zwar definiert der Anbieter, was die Software kann und wie sie funktioniert, aber der Kunde entscheidet sich für dieses definierte Paket und benutzt es, um seine Texte bearbeiten zu lassen. Er bestimmt damit auch die Mittel der Bearbeitung. Soweit der Dienstleister sie für ihn betreibt, ist ersterer **Auftragsbearbeiter**. Immerhin kann der Service auch so ausgestaltet sein, dass der Dienstleister **Verantwortlicher** ist, etwa, wenn er die Texte des Kunden für das Training seiner Software (und damit für einen eigenen Zweck) einsetzen möchte.	36
Ein Unternehmen bietet für die von ihm verkauften Kopierlösungen auch **Wartung** an. Die Techniker vor Ort sehen zwangsläufig immer wieder die Dokumente, die kopiert werden oder die Dokumente, die auf der Festplatte des Kopierlösungen zwischengespeichert sind.	Das Unternehmen ist **kein Auftragsbearbeiter**, denn seine Techniker sind nicht mit der Bearbeitung von Personendaten des Kunden beauftragt. Daran ändert die Tatsache, dass sie mit Personendaten in Berührung kommen, nichts. Soweit ein Techniker vor Ort angewiesen wird, dort gleich gewisse Einstellungen an den Geräten vorzunehmen, die die Bearbeitung von Personendaten	100, 101, 103

Fallkonstellation	Verantwortlichkeit	Rz.
	erfordert (z.B. Programmierung der Benutzer mit Zugangscode, Löschen des Festplattenspeichers), fällt er unter **Art. 29 DSGVO**, da er wie ein Mitarbeiter in der eigenen Organisation zu betrachten ist. Sollte das Unternehmen Geräte oder Speicher von den Kunden mitnehmen, damit es sie in eigener Verantwortung entsorgen, wiederverkaufen oder anderweitig selbst verwenden, wird es diesbezüglich zur **Verantwortlichen**. Sollte das Unternehmen jedoch mit der Durchführung konkreter Datenbearbeitungen beauftragt werden (z.B. sichere Vernichtung der Festplatten im Auftrag des Unternehmens), so ist er **Auftragsbearbeiter**.	
Eine Bank fordert seinen Dienstleister, der Zugang zu Bankkundendaten hat, auf, seine Mitarbeiter vorgängig einer **Sicherheitsüberprüfung** (sog. **Vetting**) nach gewissen Mindeststandards des Unternehmens (z.B. wie weit zurück ein Mitarbeiter zu prüfen ist) zu unterziehen (ggf. unter Beizug eines Vetting-Dienstleisters) und ihm auf Verlangen das Ergebnis zu zeigen bzw. Einblick in die Unterlagen zu gewähren	Der Dienstleister und die Bank sind **gemeinsame Verantwortliche**. Die Bank legt die Mindeststandards für das Vetting fest und damit dessen Mittel, während der Dienstleister den Zweck der für das Vetting erforderlichen Datenbearbeitungen definiert. Die Datenbearbeitung ist das Mittel dazu, damit der Dienstleister seine Pflicht erfüllen kann, der Bank nur sicherheitsgeprüfte Mitarbeiter zur Verfügung zu stellen. Soweit die Bank auf die Personendaten aus dem Vetting zugreift, tut sie dies zur Erfüllung ihrer aufsichts- und vertragsrechtlichen Sorgfaltspflichten und bestimmt diesbezüglich den Zweck einer solchen Datenbearbeitung. Der beigezogene Vetting-Dienstleister ist hingegen **Auftragsbearbeiter** des Dienstleisters, der dessen Dienste zur Überprüfung seiner Mitarbeiter in Anspruch nimmt.	
Ein Finanzunternehmen gibt einem Service-Provider pseudonymisierte Kundendaten, damit dieser die Daten bearbeitet und mit Sachdaten aus anderen Quellen (z.B. Daten aus amtlichen Statistiken) ergänzt, die **Kundendaten also veredelt**. Diese gibt der Provider dann dem Finanzunternehmen zurück. Das Finanzunternehmen weiss, um welche Kunden es sich handelt, der Provider jedoch nicht, da die Daten codiert sind.	Das Finanzunternehmen ist zunächst **Verantwortlicher**. Der Service-Provider ist mit Bezug auf die pseudonymisierten Kundendaten **kein Auftragsbearbeiter**, da ein solcher nur sein kann, wer Personendaten bearbeitet, und im vorliegenden Fall aus seiner Sicht keine solchen vorliegen. Gibt er die Daten dem Finanzunternehmen zurück, kommt es bezüglich der veredelten Daten zwar zu einer Bekanntgabe von	98

Fallkonstellation	Verantwortlichkeit	Rz.
	Personendaten, aber auch dies macht den Provider nicht zum Auftragsbearbeiter. Im Schweizer Recht ist er für eine etwaige Datenschutzverletzung im Rahmen seiner «Mitwirkung» an dieser rechtlich erfasst. Unter der DSGVO kommt er als **gemeinsamer Verantwortlicher** in Frage, soweit er bestimmenden Einfluss auf die Datenbearbeitung hat. Die Daten braucht er nicht im Klartext zu kennen.	
Ein Hersteller von Elektrofahrzeugen stattet seine **Autos mit einer Software** aus, die auch Personendaten des Fahrers speichert (z.B. Geotracking). Um diese Funktion vollumfänglich nutzen zu können, muss der Fahrer ein Konto mit der jeweiligen **Landesgesellschaft** einrichten, da diese den dazu passenden, Cloud-basierten Service anbietet.	Die jeweiligen Landesgesellschaften sind **Verantwortliche** mit Bezug auf die Daten jener Benutzer, die bei ihnen ein Konto eingerichtet haben. Der Hersteller der Software bestimmt jedoch wesentlich mit, was die Software an Personendaten bearbeitet und wie sie dies tut; die Landesgesellschaften müssen dies übernehmen. Er ist damit mit jeder Landesgesellschaft **gemeinsamer Verantwortlicher**.	27
Ein Anbieter von öffentlichen **Telefon- und Adressverzeichnissen** bietet diverse Zusatzdienste an. So ermöglicht er es, dass Unternehmen ihre Adressbestände aktualisieren können, um wegen Umzügen geänderte Adressen nachführen zu können. Die Kunden liefern dazu ihre Adressen und erhalten allfällig nachgeführte Adressen zurück. In seinem öffentlichen Verzeichnis bietet er die Zusatzfunktion an, dass interessierte Dritte an im Verzeichnis enthaltenen Unternehmen gleich online Terminanfragen senden können, falls sie nicht anrufen möchten (dem Anbieter liegt kein Auftrag des Unternehmens vor). Den eingetragenen Unternehmen wiederum bietet der Dienst die Möglichkeit, zum eigenen Eintrag eine eigene Website zu gestalten und aufzuschalten.	Das Verzeichnis führt der Anbieter zunächst als eigenständiger **Verantwortlicher**. Es ist sein Produkt, und er bestimmt, zu welchem Zweck und mit welchen Mitteln es geführt wird. Anders wäre es, wenn er ein Telefonverzeichnis im Auftrag einer Telefongesellschaft führt, weil diese zur Führung eines solchen Verzeichnisses gesetzlich verpflichtet ist (diesfalls wäre er **Auftragsbearbeiter**). Gleicht der Anbieter die Adressen eines Kunden mit seiner eigenen Datenbank ab, so ist er als **Auftragsbearbeiter** tätig soweit er die ihm übergebe Datenbank aufdatiert, stellt die aufdatierten Adressen aber als **Verantwortlicher** zur Verfügung. Wenn er eine Terminanfrage für ein eingetragenes Unternehmen entgegennimmt, tut er das als **Verantwortlicher**, denn er wurde nicht vom Unternehmen beauftragt, solche Termine entgegenzunehmen. Erhält er den Auftrag, eine Website eines Unternehmens bereitzuhalten (Hosting), wird er **Auftragsbearbeiter**, soweit die Website Personendaten enthält; es ist die Datenbearbeitung des Kunden, die er durchführt.	

Fallkonstellation	Verantwortlichkeit	Rz.
Ein **Kreditkartenherausgeber** (der *Issuer*) gibt den Mitarbeitern seiner Unternehmenskunden Geschäftskreditkarten aus. Sie lauten auf den Namen der Mitarbeiter und werden vom Unternehmen bezahlt. Als einen Service bietet der Issuer erweitere Rechnungsinformationen an (z.B. bei Flugreisen nebst den Kosten auch Details zu den Flügen), um den Unternehmenskunden die Spesenabrechnungen zu erleichtern. Diese Daten werden von Kartennetzwerken wie Mastercard oder Visa (die *Card Networks*) bei den betreffenden Händlern (die *Merchants*) über deren Banken (die *Acquirer*) beschafft. Als weiteren Service bieten die Kartennetzwerke an, Merchants darüber zu informieren, wenn ein Karteninhaber eine Nachfolgekarte erhält, damit die Karteninhaber ihre Datenbanken automatisch mit den neusten Kartendaten aufdatieren können und der Kunde dies nicht melden muss.	Issuer und Acquirer sind jeweils **Verantwortliche**, da sie selbst über ihre für die Abwicklung von Zahlungen nötigen Datenbearbeitungen entscheiden; die Datenbearbeitungen sind Mittel zum Zweck ihrer Bezahldienstleistungen. Auch die Merchants und Unternehmen sind in ihrem Bereich jeweils **Verantwortliche** mit Bezug auf ihre Datenbearbeitungen. Die Kartennetzwerke sehen sich zwar gern als Auftragsbearbeiter. Da sie jedoch wesentliche Aspekte der im Netzwerk stattfindenden Datenbearbeitung bestimmen und über weitgehende Autonomie in Bezug auf ihre eigene Datenbearbeitung haben, sind sie als jeweils **Verantwortliche** zu betrachten. Da ihre Datenbearbeitungen auf einer anderen Ebene stattfinden als jene der Issuer und Acquirer, können sie als eigenständige Verantwortliche betrachtet werden. Soweit ein Merchant oder Acquirer einen Service-Provider zur technischen Anbindung von Kartenterminals am Point-of-Sale und Systeme des Acquirers einsetzt, sind diese typischerweise **Auftragsbearbeiter**.	
Ein **medizinisches Labor** untersucht Blutproben, die es von Ärzten erhält. Auf den Blutproben sind die Namen der Patienten vermerkt. Diese erscheinen auch in den Ergebnisberichten. Es bietet den Ärzten als Zusatzservice eine Online-Datenbank an, mit welchem diese die Ergebnisse aus all ihren Aufträgen auf Dauer speichern, mit eigenen Kommentaren versehen und auswerten können.	Das medizinische Labor ist eigenständige **Verantwortliche**, da es selbst den Zweck und die Mittel der Datenbearbeitungen bestimmt, die erforderlich sind, um seine Leistungen zu erbringen. Mit Bezug auf den Zusatzservice liegt eine **Auftragsbearbeitung** vor, da das Labor sich hier um die Datenbearbeitung der jeweiligen Ärzte kümmert. Der Arzt hat damit quasi einen Teil der Führung seiner Krankengeschichten an das Labor ausgelagert.	
Ein Anbieter von **Managed-Security-Services** sucht den E-Mail-Verkehr seiner Kunden auf Bedrohungen hin ab und reagiert auf diese entsprechend; ferner steuert und unterhält er von seinen Kontrollzentren aus die beim Kunden zur Netzwerksicherheit eingesetzten Firewalls und anderen Systeme. Er wertet die bei den Kunden erkannten Bedrohungsmuster (Viren, Internet-Angriffsschemen, etc.) allerdings	Die E-Mails scannt der Provider für seinen jeweiligen Kunden und ist diesbezüglich **Auftragsbearbeiter**. Soweit es im Rahmen der Steuerung und des Unterhalts der beim Kunden eingesetzten Infrastruktur zu einer Datenbearbeitung kommt, ist jedoch er selbst der **Verantwortliche**; seine Leistung ist nicht die Datenbearbeitung, sondern der Unterhalt und die Steuerung der Systeme, mit welchen sie (beim Kunden) erfolgt. Verantwortlicher	

Fallkonstellation	Verantwortlichkeit	Rz.
auch für eigene Zwecke aus, um neue Bedrohungen auch bei anderen Kunden bekämpfen zu können.	ist er auch, soweit er die dabei erfassten Personendaten auch für seine eigene Zwecke auswertet (was er in der Regel tut, wenn er sie anderen Kunden zur Verfügung stellen will).	
Eine **Werbefirma** übernimmt für einen Kunden einerseits die **Pressearbeit** (inklusive Versand von Pressemitteilungen an ihre Kontakte bei den Medien) und organisiert andererseits **Direktmarketingkampagnen**. Im Rahmen der Kampagnen entwirft die Werbefirma zwar die Werbung, aber für den Versand benutzt sie die Adressdatenbank des Kunden, der auch sonst über die Kampagne bestimmt.	Die Werbefirma ist mit Bezug auf die Direktmarketingkampagne eine **Auftragsbearbeiterin**, da sie lediglich ausführt, was ihr Kunde von ihr verlangt, auch wenn sie gewisse Mittel (wie z.B. die von ihr eingesetzte Software für den Versand) selbst bestimmt. Im Bereich der Pressearbeit ist sie jedoch selbst ebenfalls **Verantwortliche**, jedenfalls was die Ansprache der Journalisten betrifft, weil sie hierzu ihren eigenen Verteiler benutzt, sie dem Kunden ihre Adressen gewissermassen für seine Pressemitteilungen «leiht». Sollte die Werbefirma sich ausbedingen, die Adressen des Kunden auch für andere Kunden nutzen zu können, so ist sie diesbezüglich in aller Regel ebenfalls **Verantwortliche**.	
Ein **Reisebüro** nimmt im Auftrag seiner Kunden bei Fluggesellschaften und Hotels Buchungen vor und sendet diesen dazu deren Personendaten, damit sie ihre Leistungen erbringen können. Ein anderes Reisebüro will eine Internet-Reise-Plattform lancieren, über welche Hotels und Fluggesellschaften mit ihren Kunden kommunizieren und von ihnen Buchungen entgegennehmen können. Um dies erfolgreich zu tun, spannt es sich mit einer Hotelkette und einer Fluggesellschaft zusammen; die drei definieren gemeinsam fest, wie die Plattform funktionieren soll, auch bezüglich der Datenbearbeitung.	Das Reisebüro ist in jedem Fall **Verantwortlicher**. Soweit Hotels und Fluggesellschaften Personendaten von Reisenden entgegennehmen, um ihre eigenen Verträge abzuwickeln, sind sie ebenfalls (eigenständige) **Verantwortliche**. Die Hotelkette und Fluggesellschaft, die mit dem Reisebüro zusammen festlegen, wie die Internet-Reise-Plattform funktioniert, sind **gemeinsame Verantwortliche**.	93
Eine Firma betreibt eine **Online-Kontaktbörse**. Jeder, der sich registriert, kann Kontaktanzeigen aufgeben und mit anderen Teilnehmern kommunizieren. Wie in einem **sozialen Netzwerk** üblich, können auch Inhalte mit anderen Teilnehmern geteilt und Gruppendiskussionen geführt werden.	Die Betreiberin ist **Verantwortliche**. Die Teilnehmer können, soweit sie Personendaten anderer bearbeiten, ebenfalls **Verantwortliche** sein.	20, 22, 23

Fallkonstellation	Verantwortlichkeit	Rz.
Diverse Versicherungen betreiben über eine Gesellschaft zusammen einen **Informationspool gegen Versicherungsbetrug**, in welchem jede Versicherung Angaben zu Fahrzeugen speichert, welche in Unfälle verwickelt worden sind. Tauchen nach einem Unfall zum selben Fahrzeug mehrere Berichte unterschiedlicher Versicherungen auf, so ist dies ein Hinweis auf ein «Autobumser»-Fahrzeug. Die teilnehmenden Versicherer legen die Rahmenbedingungen der Datenbearbeitung fest.	Die Betreiberin der Datenbank und die beteiligten Versicherern sind **gemeinsame Verantwortliche**, da sie zusammen den Zweck bestimmen (nämlich den Einsatz für sich) und die datenschutzrechtlichen Parameter festlegen.	
Ein **Bonitätsdienst** bietet seinen Kunden die Möglichkeit, Angaben zur Bestimmung der Kreditwürdigkeit seiner Kunden abzurufen (z.B. Betreibungen), solche aber ihrerseits auch einzuliefern (z.B. Zahlungserfahrungen), damit andere Kunden darauf zurückgreifen können.	Der Bonitätsdienst ist eigenständiger **Verantwortlicher**. Er betreibt die Datenbank als die Seine, legt selbst die Rahmenbedingungen für sein Angebot und deren Betrieb fest. Die Kunden sind ihrerseits eigenständige **Verantwortliche**, soweit sie Daten abrufen oder einliefern.	
Ein Pharmaunternehmen gibt als «Sponsor» eine **klinische Arzneimittelstudie** in Auftrag. Die Aufbereitung und Auswertung der Daten übernimmt eine *Clinical Research Organization* (CRO), die Studie selbst wird an einzelnen Studienzentren durchgeführt.	Der Sponsor ist **Verantwortlicher**, da er den Zweck der Datenbearbeitungen bestimmt. Die Studienzentren sind jedoch üblicherweise mit ihm **gemeinsame Verantwortliche**, da sie zwar nicht (alleine) über den Zweck bestimmen, aber trotzdem über viel Autonomie verfügen und so nebst dem Sponsor ebenfalls über wesentliche Aspekte der Datenbearbeitung bestimmen. Die CRO führt jedoch üblicherweise nur aus und ist daher **Auftragsbearbeiterin**.	35
Ein Dienstleister betreibt ein **medizinisches Register**, über welches die teilnehmenden Krankenhäuser ihre Falldaten in standardisierter Form für Forschungszwecke bereitstellen können. Jedes Krankenhaus entscheidet, ob und in welcher Form es seine Daten anbietet.	Der Dienstleister ist **Auftragsbearbeiter** der Krankenhäuser: Sie veranlassen jeweils die Bearbeitung ihrer Daten und bestimmen, wie sie zur Verfügung gestellt werden. Dies geschieht zudem in ihrem Namen. Anders wäre es, wenn der Dienstleister ihnen die Daten «abkaufen» würde, um sie selbst konsolidiert anzubieten oder für sich zu verwerten.	44
Der private Eigentümer eines Wohnhauses überträgt dessen Verwaltung an eine **Immobilienverwaltungsgesellschaft**. Diese sucht Mieter, administriert die Verträge,	Der Eigentümer und die Immobilienverwaltung sind **gemeinsame Verantwortliche**. Der Eigentümer veranlasst die Bearbeitung der Daten und bestimmt	

Fallkonstellation	Verantwortlichkeit	Rz.
zieht die Mieten und Nebenkosten ein und kümmert sich auch sonst um alle Belange rund um die Vermietung. Die Verträge laufen auf den Namen des Eigentümers, ebenso die Einzahlungsscheine. Auf der Nebenkostenabrechnung und der Korrespondenz erscheint der Name der Gesellschaft.	deren Zweck; es sind seine Mietverträge, die administriert werden, und dies geschieht in seinem Namen. Jedoch hat die Immobilienverwaltung eine weitgehende Autonomie, wie sie die zur Erfüllung ihrer Aufgaben nötigen Datenbearbeitungen durchführt (z.B. welche Fragen sie den Mietinteressenten stellt, wie lange sie deren Daten aufbewahrt, wen sie zur Datenbearbeitung beizieht). Damit bestimmt sie die Mittel der Datenbearbeitung mit.	
Ein Dienstleister betreibt in der Cloud eine **Online-Anwendung zur Arzneimittelsicherheit**, mit welcher ein Arzt von dieser prüfen lassen kann, ob sich die seinem Patienten verschriebenen Medikament vertragen. Er erfasst diese und die weiteren, von ihm für sinnvoll befundenen Angaben in der Applikation. Die Krankenkassen der Patienten spielen mit deren Vollmacht ihrerseits die ihnen bekannten Medikamente des Patienten ein, damit das Bild ein möglichst vollständiges ist. Die von ihm getätigten Abfragen kann er sich immer wieder ansehen, und er entscheidet auch, wie lange sein Patient in der Datenbank verzeichnet bleibt. Auf die Daten seines Patienten kann nur er zugreifen, nicht auch andere Ärzte, bei denen der Patient ebenfalls in Behandlung ist.	Der Dienstleister ist mit dem jeweiligen Arzt **gemeinsamer Verantwortlicher**. Die Anwendung und damit die Datenbearbeitung veranlasst hat zwar der Dienstleister; er legt auch wesentliche datenschutzrechtlichen Parameter fest, wie z.B. welche Daten er für seine Beurteilung benötigt. Allerdings bestimmt der Arzt, ob die Daten seiner Patienten damit bearbeitet werden, mit welchen Angaben und wie lange. Mit Bezug auf die Daten seiner Patienten bestimmt er über den Zweck und die Mittel der Bearbeitung mit. Er vertritt ihren Einsatz gegenüber den betroffenen Personen und wird von diesen als Ansprechpartner angesehen; mit ihm (und nicht dem Dienstleister) haben die Patienten ihre Vereinbarung. Die Krankenkassen sind hingegen eigenständige **Verantwortliche**; sie liefern Daten lediglich ein. Der Cloud-Provider ist **Auftragsbearbeiter**; es genügt, wenn der Dienstleister einen Vertrag mit diesem unterhält. Würde der Dienstleister die Daten der Patienten Ärzte-übergreifend verwalten, wäre er eigenständiger Verantwortlicher.	
Ein **Meinungsforschungsinstitut** führt eine Umfrage zur Kundenzufriedenheit oder Markenbekanntheit zwar im Auftrag seines Kunden durch, aber als Profi legt es im Wesentlichen selbst fest, wie es dies tut (welche Personen es befragt, wie die Daten analysiert werden, etc.).	Das Forschungsinstitut ist, zusammen mit dem Kunden, ein **gemeinsamer Verantwortlicher**. Der Kunde veranlasst die Datenbearbeitung, aber das Forschungsinstitut bestimmt wesentliche datenschutzrechtliche Parameter mit.	38
Ein Unternehmen beauftragt eine **Konditorei**, seinen besten Kunden im	Das Unternehmen und die Konditorei sind jeweils eigenständige **Verantwortliche**. Anders	

Fallkonstellation	Verantwortlichkeit	Rz.
Namen des Unternehmens zu Weihnachten einen süssen Gruss mit Weihnachtskarte zu senden und übergibt dafür der Konditorei deren Adressen. Die Auslieferung erfolgt unter dem Namen der Konditorei.	als etwa die Logistikfirma, die für einen Online-Shop das Warenlager und den Versand und die Retouren betreut, ist die Leistung der Konditorei das Versenden von Süssigkeiten, nicht eine Datenbearbeitung, und es nimmt diese im eigenen Namen (mit eigenem Absender vor), wenn auch mit Hinweis auf den Auftraggeber. Darum liegt keine Auftragsbearbeitung vor, im Übrigen genauso wenig wie im Fall, dass ein Kunde einen Blumenhändler bietet, das Bouquet einer anderen Person als Geschenk zu überbringen. Kunde und Dienstleister (Konditorei, Blumenhändler) sind auch keine gemeinsame Verantwortlichen, weil der Dienstleister sowohl über den Zweck als auch die Mittel der relevanten Datenbearbeitung (Betrieb des Lieferdienstes) allein entscheidet. Demgegenüber entscheidet der Kunde über den Zweck der Lieferung (also nicht den Zweck der damit verbundenen Datenbearbeitung), und den Zweck seiner eigenen Datenbearbeitung (Weihnachtskartenversand), für die er denn auch verantwortlich ist. Freilich wäre es möglich, den Auftrag auch im Sinne einer Auftragsbearbeitung auszugestalten. Das Unternehmen müsste die Konditorei anweisen, die von ihm gelieferten Adressen auf Etiketten zu drucken, ihm vorgeben, was in die Pakete gehört (seine Weihnachtskarten, Süssigkeiten), sie anweisen, die Adressen an die Pakete anzubringen und sie der Post zu übergeben. Das könnte dort sinnvoll sein, wo das Unternehmen nicht will, dass die Konditorei unter eigenem Namen auftritt (und vielleicht sogar Werbung von sich beilegt), und wo die üblichen Zustellmöglichkeiten der Konditorei für das Unternehmen nicht passen und es diese selbst gestalten will. Dies dürfte freilich der Ausnahmefall sein, und auch wenn die Konditorei Verantwortliche ist, ist es für seine Unternehmenskunden möglich von ihr zu verlangen, dass die Adressdaten vertraulich behandelt und nicht zweckentfremdet werden, ohne in eine Auftragsbearbeitung zu	

Fallkonstellation	Verantwortlichkeit	Rz.
	kippen.	