Zeitschrift für Datenrecht und Informationssicherheit

digma

www.digma.info

19. Jahrgang, Heft 3, September 2019

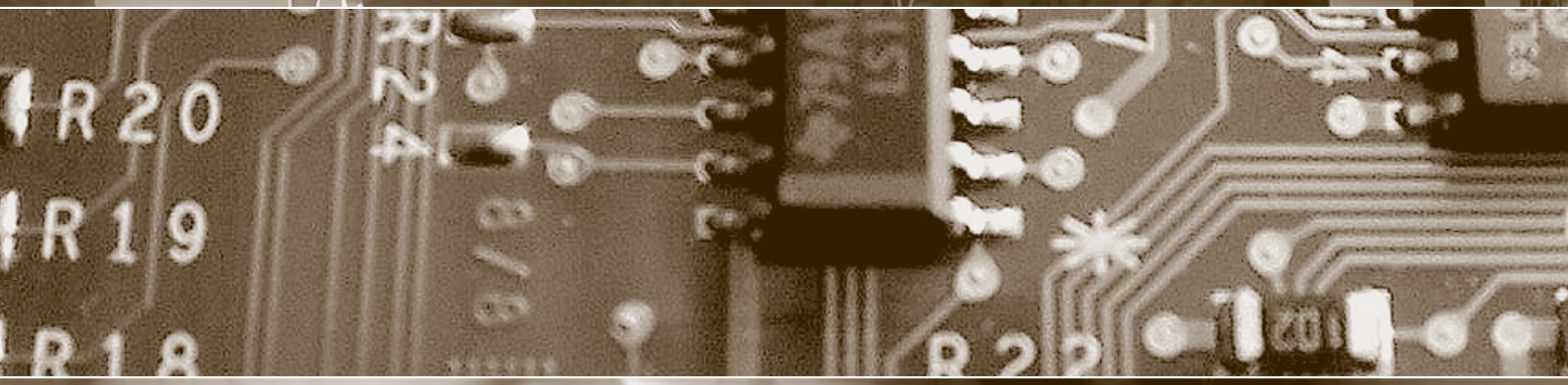
Schwerpunkt:

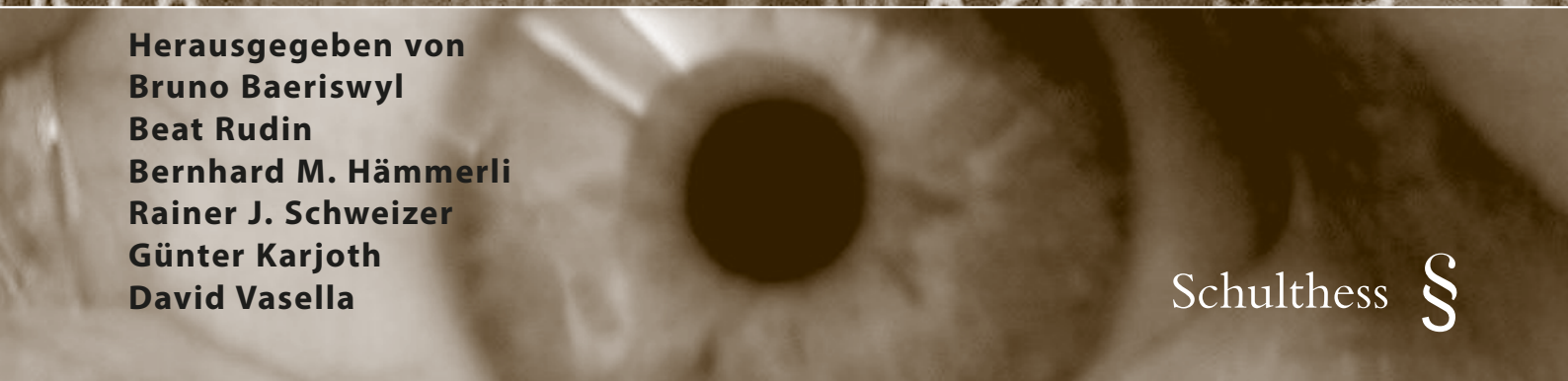
Auftragsdatenbearbeitung und Verantwortung

fokus: Verschlüsselung in der Cloud

report: Betrugserkennung auf Immobilienportalen

report: Schengen-Evaluation: Kopf in den Sand stecken?





Herausgegeben von
Bruno Baeriswyl
Beat Rudin
Bernhard M. Hämmerli
Rainer J. Schweizer
Günter Karjoth
David Vasella

Schulthess §

inhalt

fokus

Schwerpunkt:
Auftragsdatenbearbeitung und Verantwortung

auftakt
Ohne Vernetzung kein Fortschritt
von Andri Silberschmidt Seite 105

Outsourcing und Verantwortung
von Beat Rudin Seite 108

Auftragsbearbeitung im Privatbereich
von David Vasella Seite 110

Wenn die Rechtsauslegung «nebulös» wird
von Bruno Baeriswyl Seite 118

privatim-Merkblatt
Cloud-spezifische Risiken und Massnahmen
Seite 124

Verschlüsselung in der Cloud
von Michael Herfert/Benjamin Lange/
Dominik Spychalski Seite 128

zwischentakt
Kundenerlebnis für die Mülltonne
von Adrienne Fichter Seite134

Auftragsbearbeitung im Privatbereich

Wie ist bei arbeitsteiliger Datenbearbeitung die Verantwortung zuzuordnen? Wie unterscheiden sich die Rollen des Verantwortlichen (allenfalls der gemeinsam Verantwortlichen) von jener des Auftragsdatenbearbeiters? Viele Fragen in diesem Umfeld sind noch wenig geklärt.

Wenn die Rechtsauslegung «nebulös» wird

Die (Informations- und) Datenschutze enthalten Regelungen für die Auftragsdatenbearbeitung. Wenn dann noch Cloud-Technologie verwendet werden soll, wie sind die zusätzlichen oder akzentuierten Cloud-Risiken durch spezifische Massnahmen zu vermeiden oder zu reduzieren?

Verschlüsselung in der Cloud

Bei Cloud-Diensten bietet sich Verschlüsselung als Schutzmassnahme an. Nur: Was meint «Verschlüsselung»? Welchen Schutz bringen die verschiedenen Verschlüsselungslösungen? Was taugen neue Ansätze wie Hardware-basierte sichere Ausführungsumgebungen oder homomorphe Verschlüsselung? Und wie steht es mit der Langzeitverschlüsselung?

impressum

digma: Zeitschrift für Datenrecht und Informationssicherheit, ISSN: 1424-9944, Website: www.digma.info

Herausgeber: Dr. iur. Bruno Baeriswyl, Prof. Dr. iur. Beat Rudin, Prof. Dr. Bernhard M. Hämmerli, Prof. (em.) Dr. iur. Rainer J. Schweizer, Prof. Dr. Günter Karjoth, Dr. iur. David Vasella

Redaktion: Dr. iur. Bruno Baeriswyl und Prof. Dr. iur. Beat Rudin

Rubrikenredaktor(inn)en: Dr. iur. Barbara Widmer, Dr. iur. Dominika Blonski

Zustelladresse: Redaktion digma, c/o Stiftung für Datenschutz und Informationssicherheit, Postfach 205, CH-4010 Basel
Tel. +41 (0)61 201 16 42, redaktion@digma.info

Erscheinungsplan: 4-mal jährlich (März, Juni, September, Dezember)

Bezugsbedingungen: Jahresabonnement: CHF 178.00 (für Studierende: CHF 98.00), Einzelheft: CHF 48.00, zzgl. Versandkosten. Alle Abo-Preise inkl. 2,5% MWST, zzgl. Versandkosten von CHF 6.00 innerhalb der Schweiz (Versandkosten für Lieferung ins Ausland: CHF 31.00). Studentenpreis gegen Vorlage eines gültigen Nachweises. Abonnementkündigungen sind mit einer Frist von 8 Wochen zum Ende des berechneten Bezugsjahres möglich.

Anzeigenverkauf und -beratung: Fachmedien Zürichsee Werbe AG, Laubisrütistrasse 44, CH-8712 Stäfa, Tel. +41 (0)44 928 56 17, marc.schaettin@fachmedien.ch

Verlag und Kundenservice: Schulthess Juristische Medien AG, Zwingliplatz 2, Postfach 2218, CH-8021 Zürich
Tel. +41 (0)44 200 29 29, Fax +41 (0)44 200 29 28, service@schulthess.com, www.schulthess.com

Betrugserkennung auf Immobilienportalen

Unter der Vielzahl von Anzeigen auf Immobilienportalen befinden sich auch Betrugsinserate. Wie kann man diese unter verschleierter Identität erstellten Inserate automatisch erkennen?

Den (Kantons-) Kopf in den Sand stecken?

Die Empfehlungen zu den bei der Schengen-Evaluation 2018 festgestellten Mängeln sind publiziert. Wäre es gescheit von den Kantonen, jene Empfehlungen nicht zu beachten, welche nur die Datenschutzaufsicht des Kantons Luzern direkt ansprechen? Die nächste Schengen-Evaluation kommt bestimmt und die Prüfpunkte werden dieselben sein.

Der Verwaltungsrat in der Pflicht

Die Nichteinhaltung von Datenschutzvorgaben kann – zurzeit mindestens dann, wenn das Datenbearbeiten durch ein Schweizer Unternehmen unter die DSGVO fällt – Bussen zur Folge haben. Geht das den Verwaltungsrat etwas an?

Outsourcing

Tja, Outsourcing hat so seine Tücken, weiss unser Cartoonist.

report

Cyberkriminalität
Betrugserkennung auf Immobilienportalen
von Günter Karjoth Seite 136

Schengen-Evaluation
Den (Kantons-)Kopf in den Sand stecken?
von Beat Rudin Seite 140

agenda Seite 146

forum

privatim
Aus den Datenschutzbehörden
von Dominika Blonski Seite 148

Der Blick nach Europa und darüber hinaus
Der Verwaltungsrat in der Pflicht
von Barbara Widmer Seite 150

schlusstakt
Klassenkampf auf dem Datenschutzbuckel
von Beat Rudin Seite 152

cartoon
von Reto Fontana Umschlagseite 3

Auftragsbearbeitung im Privatbereich

Zu Begriff, Anforderungen und Rechtsfolgen der arbeitsteiligen Datenbearbeitung

David Vasella, Dr. iur., Rechtsanwalt, CIPP/E, Partner bei Walder Wyss AG, Zürich, Herausgeber david.vasella@walderwyss.com

Bei der datenschutzrechtlichen Rollenverteilung sind zahlreiche Fragen offen und in ihrer praktischen Handhabung zunehmend anspruchsvoll.

Arbeitsteilung ist auch bei der Datenbearbeitung unumgänglich. Gleichzeitig kann es keine Datenbearbeitung geben, ohne dass die Verantwortung für die Einhaltung des Datenschutzrechts den beteiligten Stellen zugewiesen wird. Diese Zuweisung erfolgt über die Rollen des Verantwortlichen, des gemeinsamen Verantwortlichen und des Auftragsbearbeiters, nach der DSGVO wie auch nach dem (heutigen und dem revidierten) DSG.

Zum Konzept des Verantwortlichen

Wer Personendaten bearbeitet, wird oft darauf angewiesen sein, auf Dienstleistungen weiterer Personen zurückzugreifen, seien es Arbeitnehmer, seien es andere Unternehmen. Das Datenschutzrecht akzeptiert diese Notwendigkeit, muss aber sicherstellen, dass die Anforderungen des Datenschutzrechts trotz der Arbeitsteilung und der damit verbundenen Gefahr einer gewissen Verantwortungsdiffusion eingehalten werden. Das Datenschutzrecht reagiert auf diese Gefahr dadurch, dass es Instrumente bereitstellt, mit der sich die arbeitsteilige Datenbearbeitung erfassen und Verantwortung zuweisen lassen. Dass die rechtlichen Instrumente nicht alle Nuancen eines Sachverhalts erfassen können, ist dabei unvermeidlich, weshalb bei der Anwendung dieser Instrumente eine gewisse Flexibilität erforderlich ist. Dabei bleiben aber *einige Grundsätze zu beachten,* die sich wie folgt vereinfachen lassen:

- Für jede Datenbearbeitung ist jemand verantwortlich, sei es allein, sei es gemeinschaftlich mit anderen. Eine Datenbearbeitung ohne Verantwortung ist ausgeschlossen.
- Der Verantwortliche ist für die Einhaltung des Datenschutzrechts verantwortlich. Ihm wird also die Hauptverantwortung zugewiesen. Bei der Datenbearbeitung darf er auf interne und externe Ressourcen zurückgreifen; die Verantwortung bleibt aber bei ihm.
- Solange der Verantwortliche die entsprechende Kontrolle sicherstellt, gehört der Auftragsbearbeiter datenschutzrechtlich zur Sphäre des Verantwortlichen. Sein Einbezug ist rechtlich daher grundsätzlich zulässig.
- Die Rollenteilung ist jeweils bezogen auf eine bestimmte Bearbeitung vorzunehmen. Eine Partei kann für unterschiedliche Bearbeitungen unterschiedliche Rollen haben.

Was ist ein Auftragsbearbeiter?

Ein Auftragsbearbeiter ist eine Hilfsperson, die lediglich bei der betreffenden Datenbearbeitung des Verantwortlichen mitwirkt. Der Begriff des Auftragsbearbeiters ist von folgenden Begriffen abzugrenzen:

- *Arbeitnehmer:* Arbeitnehmer gelten nicht als Auftragsbearbeiter, was sich schon aus dem Wortlaut von Art. 10*a* DSG und von Art. 4 Nr. 8 und Nr. 10 und Art. 29 DSGVO ergibt; und deshalb richtig ist, weil Arbeitnehmer dem Verantwortlichen definitionsgemäss subordiniert und datenschutzrechtlich ein Teil des Verantwortlichen sind. Eine ähnliche Stellung haben weisungsgebundene freie Mitarbeiter (Freelancer; z.B. Softwareentwickler), die Personendaten im Auftrag des Verantwortlichen bearbeiten. Aus Art. 29 DSGVO lässt sich in diesem Zusammenhang schliessen, dass ein Freelancer wie ein Arbeitnehmer zu behandeln ist, sofern er dem Verantwortlichen «unterstellt» ist. Im Ergebnis ergibt sich daraus nur die Selbstverständlichkeit, dass nicht die *rechtliche Einordnung* als Arbeitnehmer, sondern die *faktische Integration* in die Betriebsorganisation massgeblich ist. Freelancer ausserhalb der Arbeitsorganisation und der entsprechenden Weisungskompetenzen und Kontrollmöglichkeiten des Verantwortlichen fallen demgegenüber aus Art. 29 DSGVO heraus[1].

- (Andere) *Verantwortliche:* Eigenständige Verantwortliche sind als solche keine Auftragsverarbeiter; beide Eigenschaften schliessen sich aus. Dies gilt allerdings nur für dieselbe Bearbeitung. Für unterschiedliche Bearbeitungen kann eine Person gleichzeitig Auftragsbearbeiter und Verantwortlicher sein (z.B. der Dienstleister, der Personendaten des Auftraggebers für seine eigenen Analysezwecke verwendet).
- *Gemeinsam Verantwortliche:* Auch dann, wenn der Dienstleister nicht eigenständig, sondern mit dem Verantwortlichen gemeinsam verantwortlich ist, schliesst seine Eigenschaft als Verantwortlicher eine Auftragsbearbeitung aus. Die Unterscheidung zwischen gemeinsam Verantwortlichen und Auftragsbearbeitern ist allerdings nicht einfach und wird zunehmend anspruchsvoll.
- *Betroffene Person:* Die betroffene Person ist selbst weder Verantwortlicher noch Auftragsverarbeiter. Ein Dienstleister, der Personendaten der betroffenen Person bearbeitet, ist ihr gegenüber daher zwangsläufig Verantwortlicher und nicht etwa Auftragsverarbeiter, und zwar auch dann, wenn seine Tätigkeit im Übrigen jener eines Auftragsverarbeiters entspricht. Das führt bei bestimmten Geschäftsmodellen zu einer Spaltung der Rolle des Dienstleisters. Ein Hostinganbieter etwa ist ein Verantwortlicher, wenn er mit den Betroffenen direkt kontrahiert, aber ein Auftragsverarbeiter, wenn sein Kunde ein Unternehmen ist.

Abgrenzung zum Verantwortlichen

Praktisch wichtig ist vor allen Dingen die Unterscheidung zwischen Auftragsverarbeitern und Verantwortlichen. Geht man vom Normzweck aus – eine erweiterte Befugnis zur Datenübermittlung an unterstellte und damit in die Sphäre des Verantwortlichen einbezogene Dienstleister –, so muss die Weisungsbindung entscheidend sein. Auftragsverarbeiter ist daher, wer Personendaten ausschliesslich für den Verantwortlichen nach dessen Weisungen bearbeitet. Bei der Anwendung dieses Konzepts sind aber Differenzierungen erforderlich.

Vor allem unterscheidet die Praxis zwischen *Aufträgen, die gerade die Datenbearbeitung zum Gegenstand haben* (z.B. die Vernichtung eines Datenträgers oder die Bereitstellung von Speicherplatz in einer Cloud), und Aufträgen, *die auf andere Leistungen gerichtet sind,* bei deren Erfüllung der Dienstleister aber Personendaten bearbeitet (z.B. Angaben über Kontaktpersonen des Kunden). Massgeblich ist in dieser Sicht, in der Formulierung des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA), ob «eine Stelle von einer anderen Stelle im Schwerpunkt mit der Verarbeitung personenbezogener Daten beauftragt wird»[2]. Diese *«Schwerpunkttheorie»* geht davon aus, dass nur bei spezifischen Bearbeitungsaufträgen sichergestellt ist, dass der Dienstleister in seiner Datenbearbeitung den Weisungen des Auftraggebers unterworfen ist. Wer nur bei Gelegenheit eines Auftrags mit Personendaten in Berührung kommt, wird selbst entscheiden, wie er mit diesen Daten umgeht, und ist also eher ein Verantwortlicher[3].

Das Datenschutzrecht muss sicherstellen, dass die Anforderungen des Datenschutzrechts trotz der Arbeitsteilung und der damit verbundenen Gefahr einer Verantwortungsdiffusion eingehalten werden.

Diese Theorie wird nicht allen Konstellationen gerecht, liefert i.d.R. aber brauchbare Ergebnisse[4]. Sie zeigt etwa, dass der Anbieter einer kommerziellen Software, der lediglich Log-in-Daten von zugangsberechtigten Mitarbeitern bearbeitet, kein Auftragsbearbeiter ist, ebenso wenig wie eine Bank bei der Konto- oder der Anwalt bei der Mandatsführung[5] (der Auftrag betrifft im Kern jeweils nicht die Datenbearbeitung); demgegenüber sind ein Hostinganbieter oder der Anbieter eines elektronischen Datenraums jeweils ein Auftragsbearbeiter[6].

Indizien für die Bestimmung

Die Schwerpunkttheorie eignet sich als Faustregel. Es sind im Einzelfall aber weitere Aspekte einzubeziehen. Entscheidend ist dabei letztlich, dass diejenige Person verantwortlich

Kurz & bündig

Die arbeitsteilige Datenbearbeitung verlangt in erster Linie eine klare und praktisch handhabbare Zuordnung der Verantwortung. Dafür stellt das Datenschutzrecht die Instrumente der alleinigen oder gemeinsamen Verantwortlichkeit und der Auftragsverarbeitung zur Verfügung. Wichtig ist in erster Linie die Unterscheidung der Rolle des Verantwortlichen von jener des Auftragsverarbeiters. Als Faustregel bewährt sich dabei die Schwerpunkttheorie: Eine an der Verarbeitung eines Verantwortlichen beteiligte weitere Stelle ist Verantwortliche, wenn ihr Auftrag im Kern nicht die Datenverarbeitung betrifft, sondern eine andere Dienstleistung. Betrifft ihre Leistungspflicht dagegen gerade die Datenverarbeitung, ist sie eine Auftragsverarbeiterin. In vielen Fällen sind jedoch weitere Kriterien zu beachten. Sind mehrere Stellen jeweils Verantwortliche, stellt sich sodann die weitere Frage der gemeinsamen Verantwortlichkeit. Dies gilt für die DSGVO, in Kern aber auch das (heutige und revidierte) DSG. Viele Fragen in diesem Umfeld sind allerdings noch wenig geklärt.

ist, die tatsächlich in der Lage ist, die Einhaltung des Datenschutzrechts zu gewährleisten[7]. Für die *Qualifikation als Verantwortlicher* sprechen etwa die *folgenden Indizien*[8]:

- Entscheid über die Datenbearbeitung[9],
- … den Zweck bzw. das Ergebnis der Bearbeitung,
- … Art und Umfang der bearbeiteten Daten,
- … den Kreis der betroffenen Personen;
- Erzielung von Profit durch die Bearbeitung (abgesehen vom Entgelt für Dienstleistungen);
- Bearbeitung auf Basis eines Vertrags mit den betroffenen Personen oder im Rahmen einer direkten Beziehung mit ihnen;
- Fällung von Entscheidungen über betroffene Personen als Teil der Bearbeitung;
- Verwendung beruflichen Spezialwissens als Teil der Bearbeitung;
- völlige Freiheit in der Art der Bearbeitung;
- Einsatz eigener Auftragsbearbeiter.

Wichtig ist vor allem auch die Erwartung der betroffenen Person; sie sollte durch die rechtliche Zuweisung der datenschutzrechtlichen Hauptverantwortung nicht unterlaufen werden[10].

Praktisch wichtig ist vor allen Dingen die Unterscheidung zwischen Auftragsverarbeitern und Verantwortlichen.

Folgende Indizien sprechen demgegenüber *für die Eigenschaft eines Auftragsbearbeiters:*

- Die Bearbeitung folgt Weisungen eines anderen;
- die Daten werden von einem Kunden oder einer vergleichbaren Drittpartei erhalten oder nach deren Weisungen erhoben;
- fehlende Entscheidung über die Erhebung, die Art der erhobenen Daten, die Rechtsgrundlage der Bearbeitung, den Zweck der Bearbeitung, die Bekanntgabe von Daten an Dritte und die Speicherdauer;
- wenn Entscheidungen über die Bearbeitung getroffen werden, werden sie gemäss einem Drittvertrag umgesetzt;
- es besteht kein Interesse am Endergebnis der Bearbeitung.

Ferner wird der Auftragsbearbeiter, der zwar im Auftrag und nach Weisungen des Verantwortlichen tätig wird, bei der Ausgestaltung der Bearbeitung aber grosse Autonomie geniesst oder sich anmasst, aufgrund dieser Autonomie zum Verantwortlichen (vgl. Art. 28 Abs. 10 DSGVO). Das wird vor allem dann der Fall sein, wenn der Auftragsbearbeiter gerade diejenigen Modalitäten der Datenbearbeitung bestimmt, die das Risikoprofil der Bearbeitung prägen, oder wenn er Auftragsdaten für eigene Zwecke weiterverwendet, z.B. personenbezogene Kundendaten zur Verbesserung einer eigenen Software.

Exkurs: gemeinsame Verantwortung

Nach Art. 4 Nr. 7 DGSVO ist verantwortlich, wer über Zweck oder Mittel der Verarbeitung «allein oder gemeinsam mit anderen» entscheidet (ähnlich Art. 4 lit. i E-DSG). Nach Art. 26 DSGVO müssen gemeinsam Verantwortliche sodann die Pflichten zur Einhaltung der DSGVO einer Vereinbarung regeln und das Wesentliche ihrer Vereinbarung den betroffenen Personen zur Verfügung stellen (Art. 26 Abs. 2 DSGVO; eine Entsprechung fehlt im E-DSG)[11].

Diese Rechtsfigur der gemeinsamen Verantwortung hat in jüngster Zeit durch eine Folge bemerkenswerter Urteile des EuGH starken Auftrieb erhalten. Bspw. war im konzernintern Verhältnis fraglich, ob zwei Konzerngesellschaften gemeinsam verantwortlich sein können, wenn sie zwar gemeinsam über eine konzernintern genutzte Software entscheiden (z.B. ein HR-Management-System), die dadurch bearbeiteten Personendaten aber getrennt blieben, d.h. gegenseitig kein Datenzugriff möglich war. Diese Frage dürfte inzwischen geklärt sein: Die Verantwortlichkeit setzt keinen Datenzugriff voraus; verantwortlich kann also auch derjenige sein, der im Grundsatz nicht auf durch einen anderen bearbeitete Personendaten zugreifen kann[12].

In diesem und weiteren Urteilen hat der EuGH den Anwendungsbereich der gemeinsamen Verantwortung ausgedehnt, ihm aber erst wenig Kontur verliehen. Immerhin darf man folgende *vorläufige Schlüsse* ziehen:

- Ziel der Rechtsprechung des EuGH bleibt ein hohes Schutzniveau. Man wird auch in Zukunft mit datenschutzfreundlichen Urteilen zu rechnen haben, selbst wenn diese betroffene Unternehmen vor grosse Herausforderungen stellen.
- Die Verantwortlichkeit (und damit ggf. die gemeinsame Verantwortung) ist jeweils bezogen auf einen Verarbeitungsschritt zu beurteilen (z.B. die Erhebung und Weiterübermittlung von Daten), nicht bezogen auf eine gesamthafte Verarbeitung, die auch mehrere Einzelschritte umfassen kann[13].
- Eine Mitverantwortung einer Stelle für die Verarbeitung eines anderen Verantwortlichen liegt jedenfalls dann vor, wenn dieser die Verarbeitung jener veranlasst, d.h. sie anstösst. Wer Daten aus eigenem Antrieb erhebt und sie einem Dritten weitergibt, ist daher für die Erhebung und Weitergabe verantwortlich (und zwar gemeinsam mit dem Empfänger, sofern beide gemeinsame Zwecke verfolgen).

- Ein gemeinsamer Zweck kann schon dann vorliegen, wenn beide Verantwortlichen an sich eigene Zwecke verfolgen, diese aber wirtschaftlich zusammengehören[14].
- Eine Mitverantwortung kann sich für einen Verantwortlichen ferner daraus ergeben, dass er die Datenverarbeitung eines Dritten nicht gerade veranlasst, sie aber organisiert und koordiniert und dazu ermuntert[15].
- Auch der Verantwortliche, der die Art und Weise einer fremden Verarbeitung massgeblich beeinflusst, etwa durch Auswahl der Kategorien der verarbeiteten Personendaten, kann dadurch mit- bzw. gemeinsam verantwortlich werden[16].

Abgesehen von der Pflicht, eine Vereinbarung i.S.v. Art. 26 DSGVO zu schliessen und deren wesentlichen Inhalt den Betroffenen zur Verfügung zu stellen, dürfte der Status der gemeinsamen Verantwortlichkeit keine besonderen rechtlichen Auswirkungen haben. Insbesondere ist sie ohne direkten Einfluss auf die Betroffenenrechte (Art. 26 Abs. 3 DSGVO) und auf die Schadenhaftung. Nicht abschliessend geklärt ist allerdings die Frage der Privilegierung des Datenaustausches zwischen gemeinsam Verantwortlichen, d.h., ob dieser Austausch einer gesonderten Rechtsgrundlage bedarf. Aus dem Entscheid des EuGH i.S. Fashion ID kann aber geschlossen werden, dass eine solche Privilegierung nicht greift.[17] Angesichts des sehr weiten Anwendungsbereichs der gemeinsamen Verantwortung erstaunt das kaum.

In der *Praxis* bedeutet die Ausdehnung der gemeinsamen Verantwortung allerdings eine Erschwernis. Die Auftragsverarbeitung ist bekannt und verhältnismässig einfach zu regeln. Bei der gemeinsamen Verantwortung fehlen entsprechende Erfahrungen und eine einheitliche Praxis. Die starke Einzelfallbetrachtung erschwert die Rollenzuordnung sodann besonders bei starker Arbeitsteilung zwischen einer Mehrzahl von Unternehmen, z.B. im Konzern. Die Problematik kann dadurch etwas gemildert werden, dass im konzerninternen Verhältnis auch zwischen unabhängigen Verantwortlichen Vereinbarungen über den Datenschutz getroffen werden, z.B. Regeln, wie mit Betroffenen- oder Behördenanfragen umzugehen ist. Solche Regelungen sind generell sinnvoll, sorgen aber – als mögliche Vereinbarung i.S.v. Art. 26 DSGVO – auch für den Fall einer gemeinsamen Verantwortung vor.

Der Verantwortliche hat sicherzustellen, dass der Auftragsbearbeiter die Auftragsdaten nur in zulässiger Weise bearbeitet. Dieser erscheint datenschutzrechtlich als verlängerter Arm des Verantwortlichen.

Zulässigkeit der Auftragsbearbeitung

Der Auftragsbearbeiter ist definitionsgemäss der Weisungsgewalt des Verantwortlichen unterworfen, und der Verantwortliche hat sicherzustellen, dass der Auftragsbearbeiter die Auftragsdaten nur in zulässiger Weise bearbeitet (vgl. Art. 10*a* DSG und Art. 8 E-DSG; Art. 24 Abs. 1, Art. 28 Abs. 1 DSGVO). Ist dies gewährleistet, erscheint der Auftragsbearbeiter datenschutzrechtlich nicht als eigenständige Stelle, sondern als verlängerter Arm des Verantwortlichen. Als Folge dieser Konstruktion werden die Übermittlung von Personendaten an den Auftragsbearbeiter und dessen Weiterbearbeitung *«privilegiert»,* sind also *unter erleichterten Voraussetzungen zulässig.* Das ergibt sich im Anwendungsbereich des DSG implizit aus dem Begriff des «Dritten» etwa in Art. 12 Abs. 2 lit. c DSG oder Art. 4 Nr. 10 DSGVO, der den Auftragsbearbeiter nicht umfasst. In der DSGVO lässt sich die in der Sache unbestrittene Privilegierung am ehesten dadurch begründen, dass

Literatur, weiterführende Links

- Bergt Matthias, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München 2018.
- Bertermann Nikolaus, in: Ehmann Eugen/Selmayr Martin, Datenschutz-Grundverordnung, 2. Aufl., München 2018.
- Brehm Franziska, in: Simitis Spiro/Hornung Gerrit/Spiecker Indra (Hrsg.), Datenschutzrecht, Baden-Baden 2019.
- Conrad Sebastian Conrad, Freelancer als Auftragsverarbeiter?, DuD 2019, 134 ff.
- Hartung Jürgen, in: Kühling Jürgen/Buchner Benedikt (Hrsg.), Datenschutz-Grundverordnung, Bundesdatenschutzgesetz, 2. Aufl., München 2018.
- Rosenthal David, Controller oder Processor: Die datenschutzrechtliche Gretchenfrage, Jusletter vom 17. Juni 2019.
- Vasella David, Zum Anwendungsbereich der DSGVO, digma 2017, 220 ff.
- Ziegenhorn Gero/Fokken Martin, Rechtsdienstleister: Verantwortliche oder Auftragsverarbeiter?, ZD 2019, 194 ff.

die Auftragsverarbeitung als zulässiges Mittel der Verarbeitung des Verantwortlichen verstanden wird[18].

Insbesondere sind beide Stufen gestützt auf die Rechtsgrundlage der ausgelagerten Bearbeitung des Verantwortlichen zulässig *(«the lawfulness of the processor's data processing activity is determined by the mandate given by the controller»)*[19]. Der Arbeitgeber, der für die Verwaltung der Mitarbeiterdaten einen Dienstleister einsetzt, muss die Übermittlung der Mitarbeiterdaten an diesen daher nicht gesondert rechtfertigen, und der Dienstleister kann sich ebenfalls auf die Rechtsgrundlage des Verantwortlichen berufen – er ist ja, datenschutzrechtlich, Teil der Sphäre des Verantwortlichen.

Im schweizerischen Recht «wirkt» der Auftragsbearbeiter bei der Datenbearbeitung «mit» und ist demzufolge für Ansprüche aus der Verletzung des Datenschutzrechts passivlegitimiert.

Anforderungen an die Einbindung des Auftragsbearbeiters

Die erwähnte Privilegierung setzt allerdings voraus, dass die Einbindung korrekt erfolgt[20]. Im Anwendungsbereich der DSGVO sind insbesondere folgende Anforderungen zu beachten (insb. nach Art. 28 DSGVO):

- *Auswahl:* Der Verantwortliche darf nur Auftragsverarbeiter beiziehen, die die Einhaltung des Datenschutzes gewährleisten.
- *Vertragliche Einbindung:* Der Verantwortliche und der Auftragsverarbeiter müssen (schriftlich oder in Textform) eine Vereinbarung mit den Mindestinhalten von Art. 28 Abs. 3 DSGVO schliessen («Auftragsdatenverarbeitungsvereinbarung», «ADV» oder «AV-Vereinbarung».
- *Überwachung und Kontrolle:* Die Tätigkeit des Auftragsverarbeiters muss angemessen überwacht werden.
- *Auslandsbekanntgabe:* Im Fall einer Datenbekanntgabe ins Ausland (auch etwa aufgrund einer Zugriffsmöglichkeit aus dem Ausland) sind die Anforderungen von Art. 44 ff. DSGVO (bzw. Art. 6 DSG und Art. 13 ff. E-DSG) zu beachten. In der Regel schliessen der Verantwortliche und der Auftragsverarbeiter die EU-Standardvertragsklauseln ab, für schweizerische Verantwortliche oft mit bestimmten Anpassungen an das schweizerische Recht.
- In *regulierten Branchen* können weitere Anforderungen zu beachten sein, wobei der Beizug in aller Regel auch dort zulässig ist.

Mit Bezug auf die ADV sei anstelle einer Aufzählung anschliessend eine *Klausel* aufgeführt, die diese Mindestinhalte so knapp wie möglich (und für viele Konstellationen zu knapp) abdeckt, z.B. in AGB eines Dienstleisters:

«[AV] ist bei der Bearbeitung von [Auftragsdaten] verpflichtet, sie nur auf dokumentierte Weisung des [Kunden] zu bearbeiten; nur Personen beizuziehen, die einer angemessenen Verschwiegenheitspflicht unterliegen, und ohne Zustimmung des Kunden keinen Unterbeauftragten hinzuzuziehen; den Kunden soweit zulässig vorab zu informieren, falls AV nach anwendbarem Recht zu einer abweichenden Bearbeitung verpflichtet sein sollte; angemessene Massnahmen zur Sicherheit zu ergreifen; den Kunden auf geeignete Weise bei der Bearbeitung datenschutzrechtlicher Anliegen von betroffenen Personen, bei angemessenen Datensicherheitsmassnahmen, beim korrekten Umgang mit Datensicherheitsverletzungen und bei der Durchführung allfälliger Datenschutz-Folgenabschätzungen und entsprechenden Konsultationen zu unterstützen; dem Kunden auf Anfrage Informationen zur Verfügung zu stellen, damit dieser die Einhaltung seiner Pflichten bei der Einbindung von AV nachweisen kann; und im notwendigen Umfang [auf Kosten des Kunden] Überprüfungen durch oder für den Kunden zu dulden und dazu angemessen beizutragen.»

In den meisten Fällen enthalten Auftragsbearbeitungsvereinbarungen wesentlich detailliertere und zudem *weitere optionale Klauseln,* z.B. folgende:

- Genauere Regelung des Weisungsrechts (z.B. Umgang; Art und Weise der Weisungserteilung, z.B. über Schnittstellen; Direktweisungen an Mitarbeiter des Auftragsbearbeiters; Dokumentation der Weisungen; Anwendung im Konzernverhältnis; Vorgehen bei vertrags- oder rechtswidrigen Weisungen usw.);
- Zusicherungen des Verantwortlichen (z.B. betr. Einhaltung des Datenschutzrechts);
- Regelung des Beizugs von Unterbeauftragten (z.B. des Vetorechts bzw. des Widerspruchsrechts im laufenden Betrieb);
- Regelung der Kooperations- und Unterstützungspflichten (ggf. über das gesetzliche Minimum hinaus, z.B. Herausgabe des Verfahrensverzeichnisses oder Teile der Verträge mit Unterbeauftragten; Mindestinhalte von Mitteilungen usw.);
- Bestimmungen zur Auslandsbekanntgabe (z.B. zum Abschluss von Standardvertragsklauseln des Auftragsbearbeiters und/oder des Unterbeauftragten mit dem Verantwortlichen);

- Bestimmungen zur Datensicherheit (z.B. durch Verweisungen auf Massnahmekataloge; Recht oder Pflicht zur Anpassung im Lauf der Zeit);
- detailliertere Auditregelungen (z.B. durch Vorlage interner oder externer Auditberichte; Umgang mit Auditberichten des Verantwortlichen);
- Regelung zur Kostentragung (z.B. Weisungen ausserhalb des Vertragsgegenstands, bei Audits oder bei Mitwirkungspflichten);
- Vertraulichkeitsregelungen;
- Regelung der Haftung (z.B. durch Begrenzung[en] der Haftung des Auftragsbearbeiters im Innenverhältnis; Haftung für weisungswidriges Verhalten von Unterbeauftragten; etc.);
- Bestimmungen zum Verhältnis zu parallelen Leistungsvereinbarungen;
- Beendigungsregeln (Retention; Löschpflichten; Archivkopien etc.).

Zur Stellung des Auftragsbearbeiters

Wie eingangs ausgeführt, liegt die Hauptverantwortung für die Einhaltung des Datenschutzrechts beim Verantwortlichen. Der Auftragsbearbeiter ist datenschutzrechtlich aber keineswegs ein Nullum. Im schweizerischen Recht «wirkt» er bei der Datenbearbeitung «mit» und ist demzufolge für Ansprüche aus der Verletzung des Datenschutzrechts passivlegitimiert (Art. 28 Abs. 1 ZGB i.V.m. Art. 15 DSG). Daran ändert der Entwurf des DSG nichts (Art. 28 Abs. 2). – Nach der DSGVO ist die Verantwortung des Auftragsbearbeiters eine geringere, doch treffen ihn die vertraglich zu überbindenden Pflichten, die überwiegend auch *ex lege* gelten, und die folgenden *weiteren, gesetzlichen Pflichten:*

- Einschränkung der Bekanntgabe ins Ausland (Art. 44 ff.);
- Führung eines Verarbeitungsverzeichnisses (Art. 30 Abs. 2);
- ggf. Bestimmung eines EU-Vertreters (Art. 27);
- ggf. Bestellung eines Datenschutzbeauftragten (Art. 37);
- Kooperation mit Aufsichtsbehörden (Art. 58 und Art. 83 Abs. 5).

Bei einer Verletzung seiner Pflichten drohen jeweils Bussen (Art. 83 DSGVO). Der *Putativauftragsverarbeiter,* also der Verantwortliche, der sich zu Unrecht für einen Auftragsbearbeiter hält, bleibt ein Verantwortlicher mit den entsprechenden Pflichten, weshalb eine falsche Zuordnung auch für den Auftragsbearbeiter Risiken mit sich bringt.

Zu ergänzen ist hier, dass das anwendbare Recht für den Verantwortlichen und den Auftragsverarbeiter gesondert zu prüfen ist. Es ist durchaus möglich, dass der schweizerische Verantwortliche nur dem schweizerischen Recht, der EWR-Auftragsverarbeiter aber der DSGVO und seinem nationalen Recht untersteht.[21]

Haftungsrisiken

Die begrenzte Verantwortung des Auftragsverarbeiters zeigt sich auch in der Schadenhaftung gegenüber Dritten. Wird der Datenschutz verletzt, haftet grundsätzlich der dafür (alleine oder gemeinsam) Verantwortliche. Dabei genügt schon die «Beteiligung» an der rechtswidrigen Verarbeitung (Art. 82 Abs. 2 DSGVO), sofern der Verantwortliche nicht nachweist, dass ihn kein Verschulden trifft (Art. 82 Abs. 3 DSGVO). Das kann im Extremfall eine Haftung des Verantwortlichen 1 für Verstösse des Verantwortlichen 2 begründen, wenn man die Datenübermittlung bereits als Beteiligung ansieht.[22]

Demgegenüber haftet der Auftragsverarbeiter gegen aussen nur dann, wenn er die *spezifisch dem Auftragsverarbeiter auferlegten Pflichten* verletzt oder eine *Weisung* des Verantwortlichen missachtet hat (Art. 82 Abs. 2 DSGVO).[23]

Der Auftragsverarbeiter haftet gegen aussen nur dann, wenn er die spezifisch dem Auftragsverarbeiter auferlegten Pflichten verletzt oder eine Weisung des Verantwortlichen missachtet hat.

Eine Haftung kommt daher nicht in Betracht, wenn der Auftragsverarbeiter an einer widerrechtlichen Verarbeitung zwar beteiligt war, dabei aber keine seiner gesetzlichen, vertraglichen oder durch Weisung begründeten Pflichten mit datenschutzrechtlichem Gehalt verletzt hat (z.B. bei mangelnder Transparenz oder einer unvollständigen Datenschutzauskunft, sofern der Auftragsverarbeiter seine Mitwirkungspflichten eingehalten hat). Sobald dem Auftragsverarbeiter aber seinerseits eine Pflichtverletzung vorzuwerfen ist (z.B. aufgrund mangelhafter Sicherheitsmassnahmen), haftet er mit, und zwar grundsätzlich *solidarisch* (Art. 82 Abs. 4 DSGVO).[24]

Es bleibt im Fall einer überschiessenden Aussenhaftung immerhin der Rückgriff (Art. 82 Abs. 5 DSGVO), der – trotz der zwingenden Natur der *Aussen*haftung – wohl vertraglich modifiziert werden kann, bspw. die interne

Pflichtenverteilung oder Haftungsbegrenzungen. In der Praxis wird der Auftragsverarbeiter etwa häufig versuchen, seine Haftung im Innenverhältnis auf ein Vielfaches (z.B. 100–300%) des im Vorjahr bezogenen Leistungsentgelts zu begrenzen, was im Rahmen des zwingenden nationalen Haftungsrechts wirksam sein dürfte. ■

Fussnoten

1 Ähnlich, aber etwas liberaler Hartung, Art. 29 DSGVO N 13 und im Anschluss an Hartung auch Rosenthal, Rz. 104 ff. Eine auf Art. 29 DSGVO gestützte Privilegierung kann allerdings nur dann greifen, wenn die Stellung des Freelancers faktisch derjenigen eines Arbeitnehmers entspricht. Eine Ausdehnung dieser Kategorie umgeht die Anforderungen entweder an die Auftragsverarbeitung oder an die Rechtsgrundlage für die Weitergabe von Personendaten an andere Verantwortliche.

2 So die FAQ zur DS-GVO des BayLDA, <https://www.lda.bayern.de/media/FAQ_Abgrenzung_Auftragsverarbeitung.pdf>.

3 Vgl. Rosenthal, Rz. 17.

4 Dass Faustregeln berechtigt sind, stellt auch die Artikel-29-Datenschutzgruppe fest, WP169, 9: *«[…] the need to ensure effectiveness requires that a pragmatic approach is taken with a view to ensure predictability with regard to control. In this perspective, rules of thumb and practical presumptions are needed to guide and simplify the application of data protection law.»*

5 Ziegenhorn /Fokken, 194 ff.

6 Rosenthal hat als Beilage seines hier zitierten Aufsatzes im Jusletter eine Tabelle mit der vorgeschlagenen Einordnung diverser Anwendungsfälle veröffentlicht; die Beilage ist hier abrufbar: <https://bit.ly/2KG1uhm>.

7 Rosenthal, Rz. 15.

8 Vgl. die Hinweise der englischen Aufsichtsbehörde ICO, <https://datenrecht.ch/ico-leitlinien-fuer-verantwortliche-und-auftragsbearbeiter-kriterien-zur-rollenbestimmung>.

9 Das ist letztlich die Hauptfrage; vgl. auch Artikel-29-Datenschutzgruppe, Opinion 1/2010 on the concepts of «controller» and «processor», WP169, 8: *«why is this processing taking place? Who initiated it?».*

10 Artikel-29-Datenschutzgruppe, WP169, 12.

11 Eine entsprechende Vereinbarung ist zwischen eigenständigen Verantwortlichen nicht zwingend vorgegeben, sehr häufig aber sinnvoll und in der Praxis üblich.

12 EuGH vom 5. Juni 2018 i.S. Facebook Fanpage, Rs. C-210/6, Rz. 38 (mit Bezug auf die gemeinsame Verantwortung, aber dass die Verantwortlichkeit keinen Datenzugriff voraussetzt, muss wohl auch für die Verantwortung als solche gelten).

13 EuGH vom 29. Juli 2019, i.S. Fashion ID, Rs. C-40/17, Rz. 74.

14 EuGH vom 29. Juli 2019, i.S. Fashion ID, Rs. C-40/17, Rz. 78; EuGH vom 5. Juni 2018 i.S. Facebook Fanpage, Rs. C-210/6, Rz. 77 f.

15 EuGH C-25/17 vom 10. Juli 2018 i.S. Zeugen Jehovas, Rz. 73.

16 EuGH vom 5. Juni 2018 i.S. Facebook Fanpage, Rs. C-210/6, Rz. 35 ff.

17 EuGH vom 29. Juli 2019, i.S. Fashion ID, Rs. C-40/17, Rz. 96.

18 So Bertermann, Art. 28 N 7.

19 Artikel-29-Datenschutzgruppe, WP169, 25.

20 Ob eine fehlende oder mangelhafte Einbindung des Auftragsverarbeiters dazu führt, dass eine Auftragsverarbeitung fehlt, oder ob diese bloss widerrechtlich wird, ist allerdings strittig.

21 Artikel-29-Datenschutzgruppe, Guidelines 3/2018 on the territorial scope of the GDPR (Article 3) – Version for public consultation, 16. November 2018, 9; vgl. auch Vasella, 220 ff.

22 So etwa Bergt, Art. 82 DSGVO N 22; eher a.A. Brehm, Art. 82 DSGVO N 16.

23 Im Innenverhältnis haftet er zudem für Unterbeauftragte (Art. 28 Abs. 4 DSGVO). Dies gilt aber nur gegenüber dem Verantwortlichen. Gegen aussen kann der Auftragsverarbeiter daher einwenden, dass ein Schaden nicht durch ihn, sondern einen Unterbeauftragten verursacht wurde; so jedenfalls Bergt, Art. 82 N 39.

24 Die Solidarität wird allenfalls durch Erwägungsgrund 146 infrage gestellt. Danach kann das Gericht Schadenersatz bereits im Erstprozess anteilmässig zuteilen, wenn der Verantwortliche und der Auftragsverarbeiter im selben Verfahren Partei sind.

Zeitschrift für Datenrecht und Informationssicherheit
digma
www.digma.info
erscheint vierteljährlich

Meine Bestellung

❑ 1 Jahresabonnement **digma** (4 Hefte des laufenden Jahrgangs) à **CHF 178.00**
(Versandkosten: Schweiz inklusive)

Name _____ Vorname _____

Firma _____

E-Mail _____

Strasse/Nr. _____

PLZ _____ Ort _____

Datum _____ Unterschrift _____

Bitte senden Sie Ihre Bestellung an:
Schulthess Juristische Medien AG, Zwingliplatz 2, CH-8001 Zürich
Telefon +41 44 200 29 29
Telefax +41 44 200 29 28
E-Mail: zeitschriften@schulthess.com
Homepage: www.schulthess.com

Schulthess §