WHITEPAPER

VERANTWORTUNG IM DATENSCHUTZ

Herausgeber:
eco – Verband der Internetwirtschaft e. V.

Autoren:
Kirstin Dauber
Rickert Rechtsanwaltsgesellschaft m.b.H
Jan Philip Lutterbach
Rickert Rechtsanwaltsgesellschaft m.b.H
Matthias Bendixen
Rickert Rechtsanwaltsgesellschaft m.b.H

INHALT

EINLEITUNG

Wie in allen rechtlichen Belangen stellt sich auch im Datenschutzrecht die Frage, wer sich um die Einhaltung der rechtlichen Verpflichtungen überhaupt kümmern muss. Diese Frage dürfte eng mit der Frage nach der Haftung im Falle eines Verstoßes gegen bestimmte Anforderungen verknüpft sein. Im Hinblick auf die rechtlichen Anforderungen, die die Datenschutzgrundverordnung (DS-GVO) an Unternehmen stellt, gilt es insoweit zunächst zu klären, welcher der an der Verarbeitung von Daten Beteiligten auch rechtlich verantwortlich im Sinne des Gesetzes ist und somit haftet, falls etwas fehlschlägt.

Auch wenn die DS-GVO bereits seit Mai 2018 in Kraft ist, bestehen in der Praxis weiterhin große Unsicherheiten wie die jeweiligen Datenverarbeitungsvorgänge umgesetzt werden müssen. Die DS-GVO stellt die Unternehmen dabei vor einige, neue wie alte, Herausforderungen, die von jedem Unternehmen bewältigt werden müssen. Diese Anforderungen treffen zwar größtenteils den sogenannten Verantwortlichen (Art. 4 Nr. 7 DS-GVO), aber auch der sogenannte Auftragsverarbeiter, der im Auftrag des Verantwortlichen tätig wird (Art. 4 Nr. 8 DS-GVO), soll durch die Regelungen der Verordnung stärker in die Verantwortung genommen werden als dies noch unter Geltung der ehemaligen Richtlinie 95/46/EG der Fall gewesen ist. Insoweit besteht für jedes Unternehmen - gerade auch im Hinblick auf die Haftung - das Bedürfnis die eigene Rolle in Bezug auf die stattfindenden Datenverarbeitungen zu identifizieren und mit der erforderlichen (vertraglichen) Grundlage zu versehen.

Dieser Beitrag soll dabei helfen, die Rollen der jeweils an der Verarbeitung beteiligten Parteien anhand von anschaulichen Beispielen aus der Praxis zu definieren. Dabei wird ein besonderes Augenmerk auf die Zusammenarbeit zwischen Unternehmen innerhalb einer Gruppe oder eines Konzerns gelegt.

A. UNTERSCHEIDUNG VERANTWORTLICHER UND AUFTRAGSVERARBEITER

Im Rahmen der Datenspeicherung und -verarbeitung spielt vor allem die Unterscheidung zwischen Verantwortlichen und Auftragsverarbeitern eine große Rolle, da an diese Stellungen unterschiedliche Anforderungen gestellt werden und sie durch unterschiedliche Pflichten und Haftungsrisiken gekennzeichnet sind.

Während die „für die Verarbeitung Verantwortlichen" die gesamte Verantwortung für die Verarbeitung personenbezogener Daten tragen, handeln die „Auftragsverarbeiter" lediglich im Auftrag und nach Weisung der Verantwortlichen und tragen dementsprechend eine geringere eigene Verantwortung. Eine richtige Einordnung der an der Verarbeitung personenbezogener Daten Beteiligten in diese Kategorien ist folglich sehr wichtig[1]. Die Bezeichnung der Beteiligten, zum Beispiel im Rahmen eines Vertrages, bestimmt jedoch nicht allein die rechtliche Stellung. Vielmehr ergibt sich diese aus den tatsächlichen Umständen[2]. Insoweit muss der Vertrag den tatsächlichen Umständen folgen. Um die jeweilige Stellung von den Beteiligten richtig einordnen zu können, müssen die Begriffe daher zunächst definiert werden.

I. Verantwortlicher

Verantwortlich sind diejenigen juristischen oder natürlichen Personen, Behörden, Einrichtungen oder andere Stellen, die eigenverantwortlich und unabhängig die Entscheidungen über den Zweck, also den Grund weshalb die personenbezogenen Daten überhaupt verarbeitet werden, sowie über die Art und Weise der Datenverarbeitung und schließlich auch über die Art der Daten selbst treffen[3].

1. Beispielsfälle

Beispiele für eine bestehende Verantwortlichkeit des datenverarbeitenden Beteiligten sind regelmäßig die Erhebung und Verarbeitung der Personaldaten der angestellten Mitarbeiter im Unternehmen in Form einer Personalakte. Hier bestimmt das Unternehmen, welches den Mitarbeiter angestellt hat, darüber, welche Daten es von seinen Mitarbeitern erhebt und verarbeitet, auch wenn dies teils durch rechtliche Vorgaben mitbestimmt ist. Jedenfalls verarbeitet das Unternehmen die Daten seiner Beschäftigten im eigenen Interesse im Rahmen der Personalführung, etwa um die Vergütung zu zahlen oder um den digitalen Arbeitsplatz des Mitarbeiters einrichten zu können.

[1] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 7.
[2] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 11.
[3] Paal/ Pauly: Datenschutz-Grundverordnung Bundesdatenschutzgesetz; 2. Aufl. 2018, Art. 4; Rdnr. 55.

Auch die Verarbeitung von Kundendaten im Rahmen von Kaufverträgen, wo das verkaufende Unternehmen ebenfalls ein eigenständiges Interesse an der Verarbeitung der Daten hat und über die Verarbeitung bestimmt, begründet eine Verantwortlichkeit in diesem Sinne.

Ein anderes Beispiel, welches eine Verantwortlichkeit begründet und nicht auf Vertragserfüllung fußt, ist die Verwendung von E-Mail-Adressen zum Versand eines Newsletters. Hier bestimmt das werbende Unternehmen über die Mittel und Zwecke der Verarbeitung der E-Mail-Adressen (Marketing) und ist somit verantwortlich für die Verarbeitung.

2. Was muss der Verantwortliche tun?

a) Information

Der Verantwortliche hat den Betroffenen umfassend über die Verarbeitung der personenbezogenen Daten zu informieren, sofern diese Daten bei dem Betroffenen selbst (Art. 13 DS-GVO) oder bei einer anderen Person erhoben wurden (Art. 14 DS-GVO). Diese Informationen haben in „präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache" zu erfolgen. Zudem müssen diese Informationen dem Betroffenen unverzüglich, also ohne unbillige oder schuldhafte Verzögerung, mitgeteilt werden[4]. Unter gewissen Umständen ist jedoch auch eine Fristverlängerung möglich. Dies soll sicherstellen, dass jeder Betroffene in die Lage versetzt wird, seine Rechte geltend machen zu können. Die Information muss bei Erhebung der Daten erfolgen; soweit die Daten, etwa im Online-Shop oder über ein Kontaktformular, über eine Webseite erhoben werden, eignet sich hierfür die Datenschutzerklärung der Webseite.

Für die Information der Beschäftigten empfiehlt es sich entsprechend Datenschutzerklärungen vorzuhalten, die den Beschäftigten bei Vertragsschluss zur Verfügung gestellt werden.

b) Umsetzung geeigneter technischer und organisatorischer Maßnahmen

Die Folge einer Klassifizierung als Verantwortlicher ist weiter, dass er als vorwiegender Normenadressat in vollem Umfang unmittelbar verantwortlich und dazu angehalten ist, die Anforderungen der DS-GVO zu befolgen, zu interpretieren, die Konformität sicherzustellen, im Unternehmen praxisorientiert umzusetzen und seine Datenverarbeitungen aktuell zu halten. Er ist also für die Einhaltung der Datenschutzbestimmungen zuständig und wird zur Rechenschaft gezogen, wenn diese nicht eingehalten werden.

Das heißt, der Verantwortliche muss insgesamt für die Rechtmäßigkeit der Datenverarbeitung einstehen.

[4] Heckmann/Paschke in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 12, Rdnr. 32.

Dies umfasst neben der Rechtmäßigkeit der Verarbeitung eines Datums zu einem bestimmten Zweck auch die Einrichtung und Aufrechterhaltung konkreter Maßnahmen, die die Einhaltung des Datenschutzes fördern, in technischer aber auch organisatorischer Sicht. Hierunter fällt zum Beispiel neben der Einrichtung und Prüfung von Berechtigungskonzepten für den Zugriff von Mitarbeitern auf Daten auch die Schulung der Mitarbeiter in datenschutzrechtlicher Sicht.

Bedient sich der Verantwortliche einer Stelle, welche die Daten im Auftrag des Verantwortlichen verarbeitet (Outsourcing), so hat er diesen sorgfältig auszuwählen und zu überwachen, da ihn dies nicht von der allgemeinen Verantwortung für die Rechtmäßigkeit der Verarbeitung entbindet.

c) Regelmäßige Überprüfung und Aktualisierung

Weiterhin hat der Verantwortliche seine eingesetzten technischen und organisatorischen Maßnahmen bei Bedarf zu überprüfen und zu aktualisieren. Anlässe für Überprüfungen stellen regelmäßig Gesetzesänderungen oder Änderungen in der Datenverarbeitung selbst dar[5].

d) Nachweispflicht (Rechenschaftspflicht)

Der Verantwortliche muss gemäß Art. 24 Abs. 1 S. 1 DS-GVO einen Nachweis über die Rechtmäßigkeit der Datenverarbeitung und die Wirksamkeit der dafür eingesetzten technischen und organisatorischen Maßnahmen, zum Beispiel durch ein Datenschutz-Management- System, erbringen. Hierzu ist es auch möglich die in Art. 40 DS-GVO näher bezeichneten Verhaltensregeln bzw. die in Art. 42 DS-GVO beschriebenen Zertifizierungsverfahren heranzuziehen[6].

II. Auftragsverarbeiter

Auf der anderen Seite gibt es die Stellung als Auftragsverarbeiter. Der Auftragsverarbeiter ist ein eigenständiger und vom Verantwortlichen abweichender Beteiligter, der auf Grundlage eines Vertrages personenbezogene Daten lediglich im Auftrag des Verantwortlichen und nicht selbst als Verantwortlicher verarbeitet. Dies kann sowohl ein Mitarbeiter des Verantwortlichen als auch ein eigenständiges externes Unternehmen sein[7]. Der Auftragsverarbeiter zeichnet sich durch starke Weisungsgebundenheit gegenüber dem Verantwortlichen und mangelnder selbstständiger Entscheidungsbefugnis bezüglich der Zwecke und der Mittel

[5] Bertermann in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 24, Rdnr. 8.
[6] Bertermann in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 24, Rdnr. 11.
[7] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 30.

der Verarbeitung aus, wobei der Verantwortliche dem Auftragsverarbeiter die Entscheidung über die Mittel auch übertragen kann. Hierbei darf es sich jedoch nicht, um Entscheidungen über wesentliche Aspekte der Mittel handeln, da diese Entscheidungen ausschließlich von dem Verantwortlichen zu treffen sind[8]. Der Auftragsverarbeiter kann jedoch alleine über die technischen und organisatorischen Mittel der Datenverarbeitung entscheiden, ohne dass er dadurch Verantwortlicher wird[9].

1. Beispielsfälle

Softwareunternehmen, die anderen ihre Software in der Cloud oder als Software-as-a-Service bereitstellen, sind regelmäßig nicht für die von ihrem Kunden verarbeiteten Daten zuständig, sondern fungieren als Auftragsverarbeiter, da sie die mit der Software verarbeiteten Daten nicht nach eigenem Ermessen verarbeiten können, sondern regelmäßig nur weisungsgebunden handeln, um die Software vertragsgemäß zur Verfügung zu stellen.

Ein weiteres Beispiel ist die Einschaltung eines Callcenters zum Abtelefonieren einer vom Auftraggeber zur Verfügung gestellten Kundenliste mit genauen Vorgaben zum Anruf oder als erste Anlaufstelle für Kundenanfragen. Das Callcenter hat dabei keinerlei eigene Entscheidungsbefugnis darüber welche Daten verarbeitet werden oder wie dies geschieht und darf die Kundendaten ausschließlich für den durch das auftraggebende Unternehmen vorgegebenen Zweck verarbeiten.

Beauftragt ein Unternehmen ein Drittunternehmen mit der technischen Wartung der eigenen IT-Infrastruktur erhält das Drittunternehmen auch Zugriff auf alle im System gespeicherten Daten und verarbeitet insoweit auch diese enthaltenen personenbezogenen Daten. Da die Verarbeitung durch das beauftragte Drittunternehmen ausschließlich dem angewiesenen Zweck - Wartung der Systeme - dient, handelt es sich um eine Auftragsverarbeitungssituation.

2. Was muss getan werden?

Der Auftragsverarbeiter schließt mit dem Verantwortlichen einen Vertrag in schriftlicher[10] oder elektronischer Form. Dieser Vertrag muss den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, sowie die Art der personenbezogenen Daten, die Kategorien Betroffener und die Pflichten und Rechte des Verantwortlichen festschreiben (Art. 28 Abs. 3 S. 1 DS-GVO).

[8] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 17.
[9] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 17.
[10] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 32.

Darf der Auftragsverarbeiter allein oder weit überwiegend allein über die eingesetzten Mittel der Datenverarbeitung entscheiden, so muss der Verantwortliche vom Auftragsverarbeiter zwar nicht im Detail, aber wenigstens über die wichtigsten Charakteristika informiert werden[11].

B. GEMEINSAM VERANTWORTLICHE (JOINT CONTROLLER)

Es gibt jedoch auch die Möglichkeit, dass mehrere Verantwortliche zusammen über die Datenverarbeitung entscheiden[12]. Art. 26 Abs. 1 DS-GVO zufolge ist von gemeinsam Verantwortlichen auszugehen, wenn zwei oder mehrere Verantwortliche gemeinsam die Zwecke und die Mittel der Datenverarbeitung festlegen. Hierfür ist erforderlich, dass jeder der Beteiligten bestimmenden Einfluss auf die Datenverarbeitung hat, nicht aber, dass auch jeder Beteiligte Kontrolle über jeden Verarbeitungsschritt hat oder alle Beteiligten gleichrangigen Einfluss haben. Besonderes Augenmerk ist dabei auf die gemeinsame Festlegung des Zweckes der Verarbeitung zu legen. Auch hier sind die Rollenbezeichnungen im Vertrag regelmäßig nur ein Indiz und immer die tatsächlichen Beziehungen zueinander ausschlaggebend[13].

Hiervon strikt abzugrenzen ist der Fall, dass mehrere Verantwortliche selbstständig nebeneinander handeln. In einem solchen Fall ist jeder von ihnen nur für seine Datenverarbeitung verantwortlich und hat keinerlei Einflussmöglichkeiten auf bzw. Kenntnis von der Datenverarbeitung des anderen. Es werden lediglich Daten untereinander ausgetauscht ohne dass gemeinsame Zwecke und Mittel vorliegen[14]. Ein Beispiel für eine solche Konstellation ist regelmäßig dann gegeben, wenn ein Unternehmen seine Forderungen an ein Inkassounternehmen abtritt, welches in der Folge personenbezogene Daten des Betroffenen zum Zwecke der Durchsetzung (dann) eigener Forderungen verarbeitet.

1. Beispielsfälle

a) Gruppenunternehmen

Häufig sind Unternehmen Teil einer Unternehmensgruppe innerhalb derer verschiedene Funktionen zentralisiert durch ein Gruppenunternehmen für die anderen Gruppenunternehmen übernommen werden. Hierzu finden Sie unter „D. Problemstellung bei der Datenverarbeitung im Konzernverbund" weitere Informationen.

[11] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 34.
[12] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 22.
[13] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 23.
[14] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 24.

b) Personalvermittler mit eigenem Pool an Bewerbern

Sind Personalvermittler laut Vertrag „im Auftrag" von Unternehmen auf der Suche nach geeigneten Bewerbern, sichten sie regelmäßig neben den Bewerbungen, die bei dem jeweiligen Unternehmen eingehen auch ihren eigenen Pool an Bewerbern, um die Wahrscheinlichkeit eines Vertragsabschlusses zu erhöhen. Im Verhältnis zu dem jeweiligen Unternehmen sind sie zwar im Auftrag tätig. Im Verhältnis zu den einzelnen Bewerbern sind sie jedoch als Verantwortliche anzusehen, weil sie über die Zwecke und Mittel der Datenverarbeitung entscheiden. Es liegt somit eine gemeinsame Verantwortlichkeit vor[15].

c) Facebook Fanpage

Viele Unternehmen pflegen verschiedene Social-Media-Kanäle für ihre digitale Außendarstellung. Hierunter fallen häufig auch Facebook Fanpages. Hierzu hat der Europäische Gerichtshof mit Urteil vom 05. Juni 2018 entschieden, dass eine gemeinsame Verantwortlichkeit zwischen dem Fanpagebetreiber und Facebook Inc. für das Erheben und Übermitteln von Daten an Facebook Inc. bestehe. In der Sache ging es darum, dass Facebook Cookies auf dem Rechner der Besucher einer Fanpage setzte, welche mit den Anmeldedaten solcher Nutzer, die bei Facebook Inc. registriert sind, verknüpft werden konnten.

Auszugsweise lautet das Urteil wie folgt:
"Es ist festzustellen, dass im vorliegenden Fall in erster Linie die Facebook Inc. [...] über die Zwecke und Mittel der Verarbeitung der personenbezogenen Daten der Facebook-Nutzer und der Personen entscheiden, die die auf Facebook unterhaltenen Fanpages besucht haben, und somit unter den Begriff des „für die Verarbeitung Verantwortlichen" [...] fallen, [...].[16] "

Dennoch kommt das Gericht zu dem Ergebnis, dass eine gemeinsame Verantwortlichkeit gegeben sei, da der Fanpagebetreiber durch Einrichten der Fanpage einen Beitrag zur Entscheidung über die Zwecke und Mittel der Verarbeitung leiste. Dies auch, weil der Fanpagebetreiber die mittels der eingesetzten Cookies erhobenen Analysedaten im Wege der Parametrierung mitgestalten könne.

Weiter heißt es:
"Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, kann diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien."

[15] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 23.
[16] EuGH C-210/16, Rdnr. 30.

2. Was muss getan werden?

a) Joint Controller Agreement

Vertraglich geregelt werden muss dabei, wer welche Aufgabe wahrnimmt, die ihm nach der Verordnung obliegen, und wer insbesondere die für die Erfüllung der Rechte der betroffenen Personen erforderlichen Maßnahmen ergreift. Diese Regelungen müssen dabei für den Betroffenen transparent sein, wobei der Betroffene seine Rechte dennoch bei und gegenüber jedem einzelnen Verantwortlichen geltend machen kann (Art. 26 Abs. 3 DS-GVO). Die Beurteilung, ob eine gemeinsame Verantwortung vorliegt, erfolgt anhand der gleichen Maßstäbe wie bei einem alleinigen Verantwortlichen[17].

b) Prüfung Rechtmäßigkeit

Es erfolgt keine Privilegierung der gemeinsamen Verantwortlichen, d.h. auch der Transfer von Daten zu einem gemeinsamen Verantwortlichen muss mit einer Rechtsgrundlage nach Art. 6 DS-GVO gerechtfertigt werden und den generellen Anforderungen aus Art. 5 DS-GVO entsprechen[18].

Soweit ein gemeinsamer Verantwortlicher außerhalb der EU sitzt, bedarf es der weiteren Rechtfertigung dieses Transfers entsprechend Artt. 44 ff. DS-GVO.

c) Informationspflichten

Im Rahmen der Vereinbarung zwischen den gemeinsamen Verantwortlichen ist insbesondere zu regeln, welcher der Beteiligten die Informationspflichten aus Art. 13 DS-GVO zu erfüllen hat. Hierbei ist selbstverständlich auch über die gemeinsame Verantwortlichkeit und gemäß Art. 26 DS-GVO auch über die wesentlichen Inhalte der Vereinbarung zu informieren.

Häufig hat einer der gemeinsamen Verantwortlichen den direkten Kontakt zu den Betroffenen und sollte diese Verpflichtung übernehmen. Der andere Verantwortliche muss diese Pflicht dann nicht zusätzlich erfüllen.

Dies kann beispielsweise mittels der Datenschutzerklärung desjenigen Verantwortlichen erfolgen, der die personenbezogenen Daten über die eigene Website erhebt und sodann an den mit ihm gemeinsam Verantwortlichen zu übermitteln beabsichtigt.

[17] Artikel-29-Datenschutzgruppe: Stellungnahme 1/2010 zu den Begriffen „für die Verarbeitung Verantwortlicher" und „Auftragsverarbeiter", S. 22.
[18] Kurzpapier Nr. 16 der Datenschutzkonferenz vom 19.03.2018.

C. HAFTUNG

In der DS-GVO gibt es mehrere Arten von Sanktionen, die im Falle eines Verstoßes gegen die Vorschriften der DS-GVO drohen. Vor allem von der Aufsichtsbehörde erhobene Bußgelder sowie zivilrechtliche Schadensersatzansprüche haben hierbei herausragende Bedeutung. Daneben kommen aber auch strafrechtliche Konsequenzen sowie Abmahnungen[19] durch Mitbewerber nach dem Gesetz gegen den unlauteren Wettbewerb (UWG) in Betracht.

Die Aufsichtsbehörden sind bei Verstößen gegen Vorschriften der DS-GVO ermächtigt, Bußgelder zu verhängen, die in „jedem Einzelfall wirksam, verhältnismäßig und abschreckend" sind (Art. 83 Abs. 1 DS-GVO). Hierzu steht den Aufsichtsbehörden ein Bußgeldrahmen von bis zu 20.000.000 Euro oder bis zu 4 % des weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres zur Verfügung[20]. Welcher Stelle gegenüber die Bußgelder im Einzelnen angedroht werden, hängt von der verletzten Norm ab. Grundsätzlich können Geldbußen sowohl gegen Verantwortliche als auch gegen Auftragsverarbeiter verhangen werden. Zu prüfen ist insoweit zunächst, welche Stelle Adressat der verletzten Norm ist. Einzig der einzelne Mitarbeiter selbst kann kein Adressat einer Geldbuße durch die Aufsichtsbehörde sein[21].

Im Falle von Geldbußen gegen Unternehmen wird der Unternehmensbegriff im Sinne des EU-Kartellrechts (Art. 101 und 102 AEUV) als Grundlage genommen[22]. Dies hat zur Folge, dass auch ein Mutterkonzern gesamtschuldnerisch in Anspruch genommen werden kann, ohne dass er selbst an der Datenverarbeitung beteiligt gewesen ist. Voraussetzung ist, dass der Mutterkonzern in einem gewissen Maße auf die Tochterunternehmen einwirken kann[23] und Mutterkonzern und Tochterunternehmen als eine wirtschaftliche Einheit betrachtet werden kann[24]. Liegen diese Voraussetzungen vor, richtet sich die Höhe der umsatzabhängigen Geldbuße nach dem gesamten Jahreskonzernumsatz und nicht nur nach dem Umsatz des einzelnen Tochterunternehmens[25].

Auf der anderen Seite kann auch der jeweils Betroffene gemäß Art. 82 Abs. 1 DS-GVO selbst einen Anspruch sowohl gegen den Verantwortlichen als auch gegen den Auftragsverarbeiter auf Schadensersatz haben. Voraussetzung hierzu ist das Vorliegen eines schuldhaften Verstoßes gegen die DS-GVO sowie ein durch die Verletzung entstandener Schaden beim Betroffenen[26].

[19] EuGH- Urteil vom 29.07.2019, Az. C-40-17, Rdnr. 63.
[20] Gola/Jaspers/Müthlein/Schwartmann: DS-GVO/BDSG im Überblick, Datakontext, 3. Aufl., 2018, S. 96.
[21] Gola DS-GVO/Gola, 2. Aufl. 2018, DS-GVO, Art. 83 Rdnr. 16.
[22] Erwägungsgrund DS-GVO Nr. 150.
[23] Gola DS-GVO/Gola, 2. Aufl. 2018, DS-GVO, Art. 83 Rdnr. 19.
[24] Faust/Spittka/Wybitul, ZD 2016, 120, 121.
[25] Faust/Spittka/Wybitul, ZD 2016, 120, 121.
[26] Nemitz in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 82, Rdnr. 11.

Bedient sich ein Verantwortlicher eines Auftragsverarbeiters, haftet in erster Linie der Verantwortliche für dem Betroffenen entstandene Schäden. Der Auftragsverarbeiter haftet eingeschränkt nur soweit er gegen eine ihm auferlegte Pflicht aus der DS-GVO oder der nach Art. 28 DS-GVO zu vereinbarenden Auftragsverarbeitungsvereinbarung verstoßen hat. Ein klassischer Verstoß gegen Pflichten aus der Auftragsverarbeitungsvereinbarung wäre die eigenmächtige Verarbeitung der vom Verantwortlichen zur Erfüllung des Auftrags überlassenen personenbezogenen Daten zu eigenen Zwecken des Auftragsverarbeiters. Sind sowohl der Verantwortliche als auch der Auftragsverarbeiter oder mehrere Verantwortliche an derselben Verarbeitung beteiligt, können sie zunächst jeweils für den gesamten Schaden haftbar gemacht werden und haben im Anschluss entsprechende Regressansprüche untereinander[27]. Mit dieser Regelung bezweckt die DS-GVO, dass zugunsten der Betroffenen ein wirksamer Schadensersatz sichergestellt ist.

Ersetzt verlangen können Betroffene sowohl materielle als auch immaterielle Schäden. Der Begriff des immateriellen Schadens wird im Rahmen der DS-GVO weit ausgelegt[28]. Ein immaterieller Schaden ist grundsätzlich dann anzunehmen, wenn das Persönlichkeitsrecht des Betroffenen verletzt wurde. Dies ist unter anderem dann der Fall, wenn die Datenverarbeitung zu einer Diskriminierung, einem Identitätsdiebstahl oder -betrug, einer Rufschädigung oder ähnlichen gesellschaftlichen Nachteilen geführt hat[29].

Die Bemessung des jeweiligen Schadensersatzes dürfte sich dabei nicht nur nach deutschen Vorgaben richten, sondern sich an europäischen Maßgaben orientieren, d.h. in der Regel etwas höher ausfallen als bei deutschen Gerichten[30].

1. Haftung des Verantwortlichen

Werden die Daten des Betroffenen unrechtmäßig, also insbesondere im Widerspruch zu Art. 6 DS-GVO, verarbeitet, haftet der Verantwortliche voll nach Art. 82 DS-GVO und ist dem Betroffenen zum Ersatz des daraus entstandenen Schadens verpflichtet. Diese Haftung tritt gemäß Art. 82 Abs. 4 DS-GVO auch dann ein, wenn mehr als ein Verantwortlicher oder neben dem Verantwortlichen auch ein Auftragsverarbeiter an der Datenverarbeitung beteiligt ist.

[27] Erwägungsgrund DS-GVO Nr. 146.
[28] Erwägungsgrund DS-GVO Nr. 146.
[29] Erwägungsgrund DS-GVO Nr. 75.
[30] Nemitz in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 82, Rdnr. 3.

2. Haftung des Auftragsverarbeiters

Da der Auftragsverarbeiter grundsätzlich nur im Auftrag und auf Weisung des Verantwortlichen handelt, haftet er dem Betroffenen gegenüber in der Regel nicht auf einen durch die Datenverarbeitung entstandenen Schaden. Verstößt der Auftragsverarbeiter jedoch gegen seine Pflichten, die sich aus dem mit dem Verantwortlichen geschlossenen Vertrag oder aus der DS-GVO direkt ergeben, sieht die DS-GVO eine Haftung des Auftragsverarbeiters vor. Sofern der Auftragsverarbeiter wiederum selbst weitere andere Auftragsverarbeiter einsetzt, haftet er gemäß Art. 28 Abs. 4 S. 2 DS-GVO dem Verantwortlichen gegenüber, wenn der von ihm eingesetzte Auftragsverarbeiter seinerseits gegen Pflichten verstößt.

3. Haftung der Joint Controller

Gemäß Art. 26 Abs. 3 DS-GVO haften die gemeinsam Verantwortlichen dem Betroffenen gegenüber gesamtschuldnerisch für alle Ansprüche. Das bedeutet, dass der Betroffene alle Ansprüche aus einer unrechtmäßigen Datenverarbeitung zunächst gegenüber jedem Verantwortlichen einzeln ersetzt verlangen kann. Um die Rechtmäßigkeit der Datenverarbeitung zu gewährleisten, muss jede einzelne Verarbeitung nach Art. 6 Abs. 1 DS-GVO rechtmäßig sein[31].

Sollte ein Verantwortlicher von dem Betroffenen wegen einer Datenschutzverletzung zur Verantwortung gezogen werden, so kann dieser bei dem anderen Verantwortlichen nach Art. 82 Abs. 5 DS-GVO Regress nehmen. Hierbei ist dann zu klären, in wessen Bereich die Verletzung des Betroffenen liegt[32], da jeder Verantwortliche nach Art. 82 Abs. 2 DS-GVO nur für den Schaden haftet „der durch eine nicht [der DS-GVO] entsprechende Verarbeitung verursacht wurde".

D. PROBLEMSTELLUNG BEI DER DATENVERARBEITUNG IM KONZERNVERBUND

Mehrere Verantwortliche, die als Unternehmen gelten, bilden gemäß Art. 4 Nr. 19 DS-GVO eine „Unternehmensgruppe", soweit diese Gruppe aus einem herrschenden und mehreren von diesem Unternehmen abhängigen anderen Unternehmen besteht. Auch und gerade in einem solchen Konzernverbund ist es gängige Praxis verschiedene Daten für Dienstleistungen, die zentral erbracht werden können, auch über die Grenzen der einzelnen Unternehmen hinweg zu verarbeiten und zu speichern, um einerseits Verantwortungen und Prozesse zu zentralisieren und andererseits Kosten zu sparen. Auf diese Weise können gewisse

[31] Bertermann in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 26, Rdnr. 14.
[32] Nemitz in: Ehmann/ Selmayr: Datenschutz-Grundverordnung, C. H. Beck Verlag, 2017, Art. 82, Rdnr. 31..

Prozesse, wie z.B. Human-Resources-Dienstleistungen, in weniger kostenintensive Auslandsniederlassungen verlegt werden, welche sodann den gesamten Konzern mit diesen Diensten versorgen. Die Muttergesellschaft gibt dabei meist die jeweiligen Rahmenbedingungen vor und diese werden in den einzelnen Tochtergesellschaften implementiert.

Im Bereich der konzerninternen Datenverarbeitung bzw. Datenübermittlung zwischen einzelnen Gesellschaften innerhalb eines Konzerns ist daher die richtige Qualifikation der datenschutzrechtlichen Zusammenarbeit entscheidend, um die Konformität mit der DS-GVO sicherzustellen und keinen Haftungsfall nach Art. 83 DS-GVO zu begründen.

Schon während der Geltung des BDSG-alt galten die allgemeinen Zulässigkeitsregeln für die Verarbeitung personenbezogener Daten. Wie bereits unter „C. Haftung" angedeutet, wird der Konzernverbund von der DS-GVO nicht als einheitliches Unternehmen angesehen. Vielmehr ist jede Konzerngesellschaft nach dem nunmehr geltenden Recht der DS-GVO selbständiger „Verantwortlicher" oder „Auftragsverarbeiter". Denkbar ist aber auch, dass Konzerngesellschaften die Merkmale der gemeinsamen Verantwortlichkeit nach Art. 26 DS-GVO erfüllen.

Jedenfalls sieht die DS-GVO im Konzernbereich einen Datenaustausch zwischen datenschutzrechtlich selbstständigen Rechtseinheiten vor. Jeder Datenaustausch ist damit ein Verarbeitungsvorgang, der einer Erlaubnisgrundlage nach Art. 6 DS-GVO bedarf. Im Bereich der DS-GVO gibt es also kein direktes „Konzernprivileg".

In Erwägungsgrund 48 zur DS-GVO findet sich allerdings doch ein „kleines Konzernprivileg". Dieser Erwägungsgrund sieht vor, dass „Verantwortliche, die Teil einer Unternehmensgruppe oder einer Gruppe von Einrichtungen sind, die einer zentralen Stelle zugeordnet sind, ein berechtigtes Interesse haben können, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln". Damit ist jedenfalls die Beurteilung der Rechtmäßigkeit von Datenverarbeitungen vereinfacht. Die Datenübermittlung von einer Gruppengesellschaft an eine andere Gruppengesellschaft muss im Ergebnis aber dennoch den gleichen Anforderungen genügen wie eine Übermittlung zwischen unabhängigen Kooperationspartnern.

Vertragliche Regelungsmöglichkeiten

Im Folgenden sollen mögliche Vereinbarungen, die zwischen den Gesellschaften einer Unternehmensgruppe getroffen werden können, damit ein Datenaustausch erfolgen darf, skizziert werden.

1. Auftrag oder gemeinsame Verantwortlichkeit

In der Praxis gehen viele Unternehmen davon aus, dass ein Transfer zwischen Gruppenunternehmen unproblematisch möglich sein müsste und entsprechend weder eine vollständige Prüfung der Rechtmäßigkeit notwendig ist noch vertragliche Grundlagen zu schaffen sind. Wie oben bereits beschrieben ist dies nicht korrekt. Vielmehr bedarf es auch unter den Unternehmen einer Gruppe hinreichender vertraglicher Grundlagen für die Datenverarbeitung.

In der Praxis wird hier vielfach der Weg über (teils wechselseitige) Auftragsverarbeitungsvereinbarungen gewählt. Dies ist selten der richtige Weg, da die Auftragsverarbeitungsvereinbarung einzelne ausgelagerte Verarbeitungen im Auge hat, in der einer der Beteiligten streng nach Weisung tätig wird. Gerade zwischen Unternehmen einer Gruppe ist die Situation aber eher kooperativ und weniger subordinativ ausgestaltet. Darüber hinaus dürfte die Einschätzung der Zusammenarbeit der verschiedenen Gruppenunternehmen regelmäßig eher in Richtung einer gemeinsamen Verantwortlichkeit gehen, da häufig beide Unternehmen gemeinsam entscheiden, wie der Prozess im Detail ausgestaltet werden soll. Dann wären Auftragsverarbeitungsvereinbarungen sogar das falsche Rechtsinstrument; vielmehr wäre dann ein Joint Controller Agreement angebracht.

2. Betriebsvereinbarungen

Gemäß der Öffnungsklausel in Art. 88 DS-GVO i. V. m. § 26 BDSG kann die Personaldatenübermittlung durch eine Betriebsvereinbarung zur Einführung und Nutzung von HR-Software zu rechtfertigen sein. Zu berücksichtigen ist hierbei, dass der Schutz der Interessen der Arbeitnehmer bei der konzerninternen Weitergabe ihrer personenbezogenen Daten sichergestellt ist.

3. Binding Corporate Rules bei Datenübermittlungen außerhalb der EU

Soweit eines der Gruppenunternehmen außerhalb der EU in einem Land sitzt, welches kein angemessenes Datenschutzniveau bietet, bedarf es neben der allgemeinen Prüfung der Rechtmäßigkeit der Verarbeitung und der Weitergabe an einen Dritten, einer weiteren Rechtfertigung für den Transfer über die Grenzen der

EU hinaus. Hier besteht die Möglichkeit der Rechtfertigung durch sogenannte „Binding Corporate Rules" (BCR). Hierbei handelt es sich um genehmigte verbindliche interne Unternehmensrichtlinien nach Art. 47 DS-GVO, die konzernweit gültige und verbindliche Vorgaben zur Regelung von Datenflüssen darstellen. Diese bewirken, dass ein einheitlicher Datenschutzstandard geschaffen wird. Damit die verbindlichen internen Datenschutzregelungen die entsprechende Wirkung entfalten können, müssen diese zuvor von der zuständigen Aufsichtsbehörde genehmigt werden.

E. ABSCHLIESSENDE WORTE

Da die korrekte Einordnung der Verantwortlichkeit im Datenschutz Auswirkungen auf allen Ebenen der datenschutzrechtlichen Rechtmäßigkeit hat, ist es zwingend erforderlich, diese bereits zu Beginn einer Prüfung eindeutig zu klären.

Dieser Artikel soll nicht als Anleitung zur Prüfung dienen, sondern lediglich ein besseres Verständnis für die verschiedenen Institutionen hervorrufen, die die DS-GVO für die Zusammenarbeit verschiedener Unternehmen bei einer Datenverarbeitung bietet. Die korrekte Einordnung von konkreten Prozessen in diese Institutionen hängt von verschiedenen individuellen Faktoren ab und sollte im Einzelfall jedenfalls aufmerksam und umfänglich geprüft werden. Am Ende hängt hiervon nicht nur die Haftung des Unternehmens sondern auch der Umfang der Prüfung des Prozesses auf seine Rechtmäßigkeit ab.

ÜBER DIE AUTOREN

Die Verfasser arbeiten für die Rickert Rechtsanwaltsgesellschaft in Bonn. Die Autoren Lutterbach und Bendixen sind zertifizierte Datenschutzbeauftragte.

Kirstin Dauber

Frau Ass. iur. Kirstin Dauber befasst sich mit dem Datenschutzrecht, insbesondere dem Teilgebiet des Beschäftigtendatenschutzes. Frau Dauber studierte Rechtswissenschaften an der Universität Bonn. Ihr Referendariat absolvierte sie am Oberlandesgericht Köln.

Jan Philip Lutterbach

Herr Rechtsanwalt Jan Philip Lutterbach berät nationale und internationale Mandanten schwerpunktmäßig in den Bereichen IT- und Datenschutzrecht. Zur Rechtsanwaltschaft zugelassen ist Herr Lutterbach seit 2013.

Matthias Bendixen

Herr Rechtsanwalt Matthias Bendixen berät nationale und internationale Mandanten in den Bereichen Datenschutzrecht und E-Commerce. Zur Rechtsanwaltschaft zugelassen ist Herr Bendixen seit 2017.

eco – Verband der Internetwirtschaft e. V.
Lichtstraße 43h
50825 Köln

fon: 0221 – 7000 48 – 0
fax: 0221 – 7000 48 – 111

E-Mail: info@eco.de
Web: https://www.eco.de

Vereinsregister Köln
Vereinsregisternummer: 14478

Umsatzsteueridentifikationsnummer:
VAT-ID: DE 182676944

Januar 2020