

Conrad Sebastian Conrad

Die Verantwortlichkeit in der Realität

Ist das DS-GVO-Modell noch zeitgemäß?

Dreh- und Angelpunkt der Datenschutz-Grundverordnung ist die Bestimmung der Verantwortlichkeit. Angesichts der sich ständig weiterentwickelnden Datenverarbeitungsmöglichkeiten, erscheint jedoch eine Anwendung auf zumeist vielfältige Sachverhalte zunehmend schwerer zu werden. Die vielleicht etwas provokante Frage könnte daher lauten: Ist die DS-GVO nun wirkungslos?

1 Einleitung

Dreh- und Angelpunkt der Datenschutz-Grundverordnung (DS-GVO) ist die Bestimmung der Verantwortlichkeit. Der Verantwortliche im Sinne von Art. 4 Nr. 7 DS-GVO hat ausweislich des Regelungsgehalts der Datenschutz-Grundverordnung die Einhaltung der datenschutzrechtlichen Vorschriften zu gewährleisten. Als Adressat von Pflichten¹ aus der Verordnung und Ansprechpartner für Betroffene, ebenso aber auch nach den Rechenschaftspflichten gegenüber den Aufsichtsbehörden, wird damit die zentrale Rollenverteilung etabliert. Als „Gegenspieler“ des Betroffenen drohen dem Verantwortlichen bei Missachtung der datenschutzrechtlichen Normen verschiedene Risikoszenarien, insbesondere Schadensersatz sowie Bußgelder und weitere Sanktionen der Aufsichtsbehörden.

Obwohl diese klaren Rollenbilder vermeintliche Rechtssicherheit bringen und für Transparenz der Datenverarbeitung sorgen sollen, kommen jüngst immer mehr Zweifel an diesem geradlinigen Modell auf. Die provokante Frage könnte daher lauten: Ist die Datenschutz-Grundverordnung nun wirkungslos?

2 Fälle der Verantwortlichkeiten

Der Ordnungsgeber sah bereits bei der Gestaltung der Datenschutz-Grundverordnung verschiedene Fallkonstellationen der Verantwortlichkeit vor, die es hierzulande in dieser Form nicht gab. Doch die notwendigen, im Folgenden dargestellten Abgrenzungen drohen immer mehr aufzuweichen.

¹ Raschauer, in: Sydow, Art. 4 DS-GVO, Rn. 114.



Conrad Sebastian Conrad

Justiziar – datenschutz nord GmbH

E-Mail: cconrad@datenschutz-nord.de

2.1 Der Verantwortliche

Als Adressat der Datenschutz-Grundverordnung gilt grundsätzlich der Verantwortliche, der sowohl eine natürliche Person als auch eine juristische Person, Behörde, Einrichtung oder „andere Stelle“ sein kann. Diese Formulierung eröffnet einen weiten Anwendungsbereich.

2.1.1 Definition

Nach der Legaldefinition in Art. 4 Nr. 7 DS-GVO gilt als Verantwortlicher, wer allein oder gemeinsam mit anderen „über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“. Die Definition ist nahezu identisch mit Art. 2 lit. d) der vorherigen Datenschutzrichtlinie und daher auf europäischer Ebene nicht neu.²

Dem Verantwortlichen kommt eine zentrale Bedeutung in der Datenschutz-Grundverordnung zu, indem er an vielen Stellen der Verordnung in die Pflicht genommen wird. Schließlich zielt diese durch eine weite Bestimmung des Begriffs des „Verantwortlichen“ darauf ab, einen wirksamen und umfassenden Schutz der betroffenen Personen zu gewährleisten,³ wie es auch der Europäische Gerichtshof mehrfach in der jüngsten Rechtsprechung bestätigte und damit insgesamt festigte.⁴

2.1.2 Kriterien

Wer sich in der Rechtsanwendung mit den zwei Kriterien der Festlegung der Mittel und Zwecke bemüht, wird bald feststellen müssen, dass diese Merkmale erhebliche Fragen aufwerfen. Was versteht sich unter „Mittel“ der Datenverarbeitung? Gemeint sein kann damit die „Art und Weise“, wie ein Ergebnis oder Ziel erreicht werden soll.⁵ Hiermit kann der konkrete technische Rahmen, z. B. die konkrete Datenbankstruktur und deren Mechanismen, oder aber allgemein der beabsichtigte Verarbeitungsprozess

² Hartung, in: Kühling/Buchner, Art. 4 Nr. 7 DS-GVO, Rn. 2.

³ Petri, in: Simitis/Hornung/Spiecker, Art. 4 Nr. 7 DS-GVO, Rn. 21.

⁴ Unter anderem: EuGH, Urteil vom 5.6.2018, Az.: C-210/16; EuGH, Urteil vom 13.05.2014, Az.: C-131/12.

⁵ So die Definition von „Mittel“ der Art.-29-Gruppe, Working Paper 169 (vom 16. Februar 2010), S. 15.

als solcher bezeichnet werden. Diesbezüglich sind die Vorgaben leider sehr unpräzise. Im Hinblick auf diese „Mittel“ soll nach der Datenschutz-Grundverordnung verantwortlich sein, wer über die wesentlichen Aspekte der Verarbeitungsmittel entscheidet oder zumindest mitentscheidet.⁶

Hingegen dürfte Einigkeit darüber bestehen, was unter dem „Zweck“ zu verstehen ist, also das jeweilige Ziel der Verarbeitung. Die Art.-29-Gruppe konkretisierte dieses Merkmal als „*erwartetes Ergebnis, das beabsichtigt ist oder die geplanten Aktionen leitet*“.⁷ Aus jener Vorgabe wird eben auch die Rechtsgrundlage und somit die Rechtmäßigkeit der Datenverarbeitung abzuleiten sein. Deshalb soll dem zweiten Kriterium größere Bedeutung beigemessen werden, da sich bei der (Mit-)Bestimmung des Verarbeitungszwecks maßgeblich die rechtliche und tatsächliche Entscheidungsbefugnis⁸ bzw. die bewusst oder unbewusst ausgewählte Entscheidungsgewalt niederschlägt.⁹ Maßgeblich soll sein, wem die Entscheidungsbefugnis hinsichtlich des Zwecks und der Mittel der Datenverarbeitung zukommt.¹⁰ Immerhin hat der Verantwortliche während einer Datenverarbeitung jederzeit „Herr der Daten“ zu bleiben.¹¹

2.2 Gemeinsame Verantwortlichkeit

Doch lässt sich der Datenschutz-Grundverordnung noch ein weiterer Sonderfall entnehmen; eine Abwandlung von dem Rollenbild, die in letzter Zeit neue Berühmtheit erlangen durfte.

Nach Art. 26 DS-GVO können auch mehrere Verantwortliche zusammenwirken und sich die ihnen zukommenden Pflichten aufteilen. Die EuGH-Entscheidung¹² zum Betrieb einer Facebook-Fanpage aus dem Jahre 2018 kristallisierte heraus, wie in der Praxis eine gemeinsame Verantwortlichkeit begründet werden kann. Gemäß Art. 26 Abs. 1 S. 1 DS-GVO sind zwei oder mehrere Verantwortliche dann gemeinsam verantwortlich, wenn sie die Zwecke und die Mittel zur Verarbeitung gemeinsam festlegen, wobei beide Kriterien erfüllt sein müssen.¹³

Des Weiteren lässt sich dem Erwägungsgrund 79 der Datenschutz-Grundverordnung entnehmen, dass eine gemeinsame Verantwortlichkeit auch eine gemeinsame Festlegung von Verarbeitungszweck und -mittel „*zum Schutz der Rechte und Freiheiten der betroffenen Personen sowie bezüglich der Verantwortung und Haftung der Verantwortlichen und der Auftragsverarbeiter*“ bedingt.

Und auch die Wortlautauslegung des Art. 26 Abs. 1 DS-GVO soll eindeutig ergeben, dass „*nur bei kumulativem Bestimmen beider Tatbestandsmerkmale, also dem „Zweck“ und „Mittel“ der Verarbeitung eine gemeinsame Verantwortlichkeit anzunehmen ist.*“¹⁴

Allerdings ist damit immer noch unklar, ab welchem „*Grad der Mitgestaltung und -entscheidung überhaupt von einer gemeinsamen Verantwortlichkeit ausgegangen werden kann.*“¹⁵

Die Verordnung spricht jedenfalls von einer „gemeinsamen“ und nicht von einer „gleichwertigen“ Verantwortlichkeit.¹⁶ Das ergibt auch einen Sinn. Es wäre schließlich lebensfremd davon auszugehen, dass beide oder mehrere Verantwortliche per se gleichrangig agieren. Vielmehr dürften unterschiedliche Eigentums-/Sachherrschaftsverhältnisse bestehen und auch die konkreten Aufgaben bewusst unterschiedlich verteilt werden. Möglicherweise soll es darauf gar nicht ankommen und auf die juristische Kontrolle bzw. Einflussnahme und Aufteilung der Pflichten abgestellt werden. Dieses würde der modernen IT-Infrastruktur und Abhängigkeit von technischen Ressourcen angemessen Rechnung tragen. Die jüngste Rechtsprechung lehnt sich an diesen Gedanken an.¹⁷ Bereits die Möglichkeit der Parametrisierung von Nutzersauswertungen einer Internetseite, z. B. bei einer Facebook-Fanpage, kann für einen Grad der Mitverantwortlichkeit des Betreibers sprechen,¹⁸ auch wenn Facebook die gesamte technische Infrastruktur diktiert und sich nicht einmal umfassend in den Quellcode blicken lässt. Die deutschen Aufsichtsbehörden versperren sich – wohl auch deshalb – einer abschließenden Liste an Anwendungsfällen der gemeinsamen Verantwortlichkeiten und stellen im Kurzpapier 16 der DSK fest: „*vielmehr bedarf es einer gewissen Flexibilität, um einen effektiven Schutz der Rechte und Freiheiten der betroffenen Personen zu gewährleisten.*“¹⁹ Mit Blick auf die Abgrenzung zur Auftragsverarbeitung²⁰ dürfte in diesem Kontext die „objektive Qualifikation“ der Datenverarbeitungsabläufe entscheidend sein, weshalb der Grad der Verantwortung nicht durch die Parteien frei bestimmbar sein, sondern objektiv messbaren Maßstäben unterliegen sollte.²¹

2.3 Bestimmung der Verantwortung

Die aufgezeigten Konstellationen sollten bei der (zukünftigen) Bestimmung der Verantwortung nach der Datenschutz-Grundverordnung herangezogen werden. Per Definitionem gilt als Verantwortlicher, wer über die Mittel und Zwecke der Verarbeitung von personenbezogenen Daten entscheidet und in Abgrenzung zum „Auftragsverarbeiter“ (Art. 4 Nr. 8 DS-GVO) oder aber „Dritten“ (Art. 4 Nr. 10 DS-GVO) handelt.

Im Falle der Auftragsverarbeitung nach Art. 28 DS-GVO ist ein entsprechender Vertrag zu schließen, der die gesetzlich vorgegebenen Rechte und Pflichten der Akteure skizziert und gegebenenfalls näher ausgestaltet. Im Wesentlichen betrifft dies die Kontrollrechte, Umsetzung der Betroffenenrechte, Melde- bzw. Mitwirkungspflichten bei Datenpannen, Regelung zum Umgang mit Unterauftragnehmern sowie die Einbeziehung und Darstellung der technisch-organisatorischen Maßnahmen nach Art. 32 DS-GVO. Der Verantwortliche ist bei dieser Rechtsbeziehung jederzeit ersichtlich und kann als solcher seine Kontrollrechte durchsetzen. Zudem werden häufig – deklaratorisch oder aber in unzulässiger Weise – die Haftung der Parteien im Innenverhältnis untereinander und der Regress in einem AV-Vertrag geregelt.

6 Petri, in: Simitis/Hornung/Spiecker, Art. 4 Nr. 7 DS-GVO, Rn. 20.

7 Artikel-29-Gruppe, Working Paper 169 (vom 16. Februar 2010), S. 15.

8 Vgl. Schreiber, ZD 2019, 55, 56.

9 Vgl. im Hinblick auf die Abgrenzung zum Auftragsverarbeiter: Hartung, in: Kühling/Buchner, DS-GVO 2. Auflage 2016, Art. 4 Nr. 7 Rn. 13, 14.

10 Wagner, ZD 2018, 307, 308.

11 Raschauer, in: Sydow, Art. 4 DS-GVO, Rn. 123.

12 EuGH, Urteil vom 5.6.2018, Az.: C-210/16.

13 Piltz, in: Gola, DSGVO 2. Auflage, 2018, Art. 26 Rn. 3.

14 Kartheuser/Nabulsi, MMR 2018, 717, 720.

15 Petri, in: Simitis/Hornung/Spiecker, Art. 26 DS-GVO, Rn. 14.

16 Härtling/Gössling, NJW 2018, 2523, 2525.

17 EuGH, Urteil vom 10.07.2018, Az.: C-25/17.

18 Siehe dazu auch bei Härtling/Gössling, NJW 2018, 2523, 2524.

19 DSK, Kurzpapier Nr. 16, S. 4, Stand 19.03.2018, https://www.ida.bayern.de/media/dsk_kpnr_16_gemeinsam_verantwortliche.pdf. (letzter Abruf: 10.5.2019).

20 Vgl. dazu mit Blick auf die Abgrenzung zur Auftragsverarbeitung VGH München, Beschluss v. 26.09.2018, Az.: 5 CS 18.1157.

21 Schreiber, ZD 2019, 55, 58.

Liegt hingegen eine gemeinsame Verantwortlichkeit im Sinne von Art. 26 DS-GVO vor, bedarf es einer konkreten internen Festlegung und Zuweisung von Verantwortlichkeiten (z. B. durch Verantwortlichkeitsmatrizen), um den Schutz natürlicher Personen zu erreichen.²² Deshalb gilt es zunächst, untereinander die Verteilung von Aufgaben und Pflichten abzustimmen und im Einklang mit dem Erwägungsgrund 79 der DS-GVO durch klare Zuteilung vertraglich zu regeln.²³ Vor dem Hintergrund der Rechtsfolge der gemeinsamen Verantwortung (und gemeinsamen Haftung) kann ein solcher Vertrag nur dann für hinnehmbar und zielführend erachtet werden, wenn alle beteiligten Parteien jeweils einen bestimmenden Einfluss auf die Datenverarbeitung ausüben und daher eine Aufteilung/Regelung der unterschiedlichen Verantwortlichkeiten aus Gründen der Transparenz erforderlich wird.²⁴ Dessen sollten sich die Vertragsparteien auch bewusst sein, was ebenso für die Dokumentation mittels einer Verantwortungsmatrize spricht. Schließlich ergibt sich trotz der nach außen hin geltenden gesamtschuldnerischen Haftung im Innenverhältnis zwischen den Verantwortlichen ein Schadensausgleich nach „ihrem Anteil an der Verantwortung für den Schaden“ gemäß Art. 82 Abs. 5 DS-GVO.²⁵ Mithin hat der Anspruchsberechtigte die freie Wahl, von welcher Partei er den Schaden ersetzt haben möchte und zwar unabhängig des Verschuldens oder der Finanzkraft der einen oder anderen Partei.²⁶ Die Aufklärung und Transparenz der Verteilung hat auch gegenüber dem Betroffenen bzw. Dritten zu erfolgen.

Obleich es den Akteuren gewissermaßen nach dem Datenschutzrecht obliegt, die Verantwortlichkeiten (untereinander) zu regeln bzw. einseitig zu verteilen, dürfte für die datenschutzrechtliche Beurteilung – wie konstatiert – eine objektive Betrachtung der tatsächlichen Gegebenheiten maßgeblich sein.²⁷

Die einzig erwähnenswerte Einschränkung des Regelungsgehaltes der DS-GVO könnte sich aus dem sog. Haushaltsprivileg ergeben, wonach bei Datenverarbeitungen bei ausschließlich persönlichen oder familiären Tätigkeiten und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit²⁸ die DS-GVO wohl nicht zur Anwendung kommen soll (vgl. Art. 2 Abs. 2 lit. c) DS-GVO). Doch dürfte diese Ausnahme sehr eng zu fassen sein.²⁹ Wenn die Datenverarbeitung gegenüber einer unbestimmten Zahl von Personen im Internet³⁰ (z.B. Webseite oder Video-Portal)³¹ oder über Cloud-Server außerhalb der EU oder bei solchen Personen stattfindet, die nicht zum engsten Familienkreis zählen, greift diese Ausnahme zumeist nicht.³² Gleiches gilt, wenn bereits die Intensität der Datenverarbeitung und dessen Zwecke aus dem Anwendungsbereich der Ausnahmeregelungen fallen, wie es bei der Nutzung von Smart Cars, Smart Glasses oder Drohnen in

der Öffentlichkeit bestehen kann³³ und auch durch die technische Entwicklung immer häufiger anzunehmen ist.

2.4 Exkurs: Pflichten des Verantwortlichen

Der Verantwortliche hat für die Einhaltung der datenschutzrechtlichen Bestimmungen geradezustehen. Aus der DS-GVO ergeben sich deshalb zahlreiche Pflichten, wie die Prüfung und Dokumentation der relevanten Vorgänge (z.B. im Verzeichnis der Verarbeitungstätigkeiten) und der technisch-organisatorischen Maßnahmen sowie ggfs. das Hinwirken auf den Abschluss von Verträgen über die Auftragsverarbeitung (Art. 28 DS-GVO) oder gemeinsame Verantwortlichkeit (Art. 26 DS-GVO).

Zu den wesentlichen Aufgaben des oder der Verantwortlichen zählen ferner die Umsetzung der Informationspflichten wie auch der Betroffenenrechte (Artt. 12-23 DS-GVO). Zum einen muss der Verantwortliche nach Artt. 12-14 DS-GVO über die konkrete Datenverarbeitung aufklären, beispielsweise mit Hilfe einer Datenschutzerklärung auf einer Webseite bzw. innerhalb einer App oder einem Aushang / Info-Blatt in Papierform. Zum anderen hat er als Ansprechpartner für den Betroffenen zur Verfügung zu stehen und dessen legitimes Begehren wie z. B. den Anspruch auf Auskunft (Art. 15 DS-GVO) oder Löschung (Art. 17 DS-GVO) seiner ihn betreffenden personenbezogenen Daten nachzukommen. Nicht zuletzt wäre gegebenenfalls eine Datenschutz-Folgenabschätzung bei sensiblen Prozessen vorzunehmen (Art. 35-DSGVO). Ein Verstoß gegen diese Vorgaben ist weitestgehend mit Bußgeld bedroht (Art. 83 DS-GVO) und sollte daher durch eine angemessene Umsetzung vermieden werden. Untermauert wird diese Aufgabe durch die „Rechenschaftspflichten“ aus Art. 5 Abs. 2 DS-GVO.

In Ansehung der gemeinsamen Verantwortlichkeit aus Art. 26 DS-GVO lässt sich jedoch eine Verteilung der originären Pflichten des Verantwortlichen ausgestalten. Diese könnte unter anderem vorsehen, dass nur einer der mehreren Verantwortlichen primär die Informationspflichten und Umsetzung der Betroffenenrechte erfüllt, sofern dies in der Vereinbarung nach Art. 26 DS-GVO bestimmt wurde.³⁴ Dem Betroffenen sind dann aber, beispielsweise auf einer Webseite nachvollziehbare Beschreibung des Zusammenwirkens und der Rollen zur Verfügung zu stellen.³⁵ Ein derartiger Weg setzt allerdings in der Praxis ein standfestes Konzept mit klar definierter Rollenverteilung sowie ein wirksames Handling derselben voraus. Dem sollte nicht nur die detaillierte, individuelle und freiwillige Absprache inklusive tatsächlicher Umsetzungsmöglichkeit, sondern überhaupt erst das Schaffen des Bewusstseins dieser zwingenden Vorgaben vorausgehen, was mit Blick auf die tatsächlichen Gegebenheiten im Internet wie auch der Monopolstellung der großen Anbieter (wie z. B. Microsoft, Facebook, Google oder Amazon) jedoch kritisch hinterfragt werden könnte.

Ein denkbare Szenario wäre also, dass der Betroffene sich mit seinen ihm durch die Datenschutz-Grundverordnung verliehenen Ansprüchen an einen oder mehrere Verantwortliche richtet und aufgrund fehlender interner Organisation und Aufgabenverteilung oder mangels Verständnisses diesem Begehren nicht oder

22 Jung/Hansch, ZD 2019, 143.

23 Vgl. Martini; in: Paal/Pauly, Art. 26 DS-GVO, Rn. 1.

24 Kartheuser/Nabulsi, MMR 2018, 717, 720.

25 Martini, in: Paal/Pauly, DS-GVO, Art. 26 DS-GVO, Rn. 5 f.; Vgl. Bergt, in: Kühling/Buchner, Art. 82 DS-GVO, Rn. 60.

26 Boehm, in: Simitis/Hornung/Spiecker, Art. 82 DS-GVO, Rn. 33.

27 Vgl. Bay. VG, Urteil – VGH München, Beschl. v. 26.9.2018 – Az.: 5 CS 18.1157.

28 Gola, in: Gola, Art. 2 DS-GVO, Rn. 19.

29 Vgl. EuGH, Urteil vom 14.2.2019, Az.: C-345/17; EuGH, Urteil vom 27.9.2017, Az.: C-73/16; EuGH, Urteil vom 10.7.2018, Az.: C-25/17.

30 Vgl. EuGH, Urteil vom 06.11.2003, Az.: C-101/01 (Lindqvist).

31 EuGH, Urteil vom 14.2.2019, Az.: C-345/17.

32 Vgl. Erwägungsgrund 18 der DS-GVO, der auch von „Online-Tätigkeiten“ spricht, im Ergebnis jedoch vage bleibt.

33 Vgl. Roßnagel, in: Simitis/Hornung/Spiecker, Art. 2 DS-GVO, Rn. 31 f.; Rose, DuD 2017, 137, 138.

34 Bertermann, in: Ehrmann/Selmayr, DS-GVO, 2. Auflage 2018, Art. 26 Rn. 13.

35 DSK, Kurzpapier Nr. 16, S. 4, Stand 19.3.2018, https://www.lida.bayern.de/media/dsk_kpnr_16_gemeinsam_verantwortliche.pdf.

nicht rechtzeitig Folge geleistet wird. Es droht in komplexen Sachverhalten mit mehreren Verantwortlichen dann sogar die Aushöhung der Betroffenenrechte.³⁶

Positiv hervorzuheben ist, mit Blick auf die allseits gefürchteten Bußgelder der Aufsichtsbehörden gegenüber dem oder den gemeinsam handelnden Verantwortlichen, die sich aus der Verordnung ergebende Bußgeldbemessung unter Berücksichtigung des konkreten Einzelfall, bei dem nach dem Umfang tatsächlicher Einflussnahmemöglichkeiten und dem Versuch einer vertraglichen oder tatsächlichen Maßnahme zur Verhinderung des in Rede stehenden Datenschutzrechtsverstoßes gefragt wird.³⁷ Eine nach Art. 26 DS-GVO getroffene Vereinbarung mit klarer Aufgabenverteilung kann demnach bei der Festlegung des Bußgeldes heranzuziehen sein, ohne zwangsweise hierfür ausschlaggebend zu sein.

3 Die Realität überholt das Recht

Trotz oder gerade wegen der vielfältigen Fallkonstellationen aus der Datenschutz-Grundverordnung stellt die Realität das Datenschutzrecht vor neue Probleme. Denn komplexe Sachverhalte aus der Praxis veranschaulichen die Abgrenzungsschwierigkeiten, wenn verzahnte Plattformen im Internet, Apps bzw. IoT-Geräte oder auf die Künstliche Intelligenz (KI) basierende Anwendungen mehrere datenschutzrechtliche Verantwortlichkeiten nach der bereits dargestellten Definition oder aber sogar neue faktische Rollen begründen.

Es entsteht dann ein Geflecht aus verschiedenen Verantwortlichkeiten, die in den seltensten Fällen konkret vertraglich untereinander geregelt werden. Als Beispiel kann die Facebook-Fanpage Entscheidung des Europäischen Gerichtshofs³⁸ angeführt werden, der eine gemeinsame Verantwortlichkeit des Betreibers und Facebook nach Art. 26-DSGVO – etwas überraschend – aufzeigte, während der Betreiber tatsächlich kaum Steuerungsmittel gegenüber dem Internetgiganten aus den USA besitzt bzw. auch keinen Vertrag durchsetzen kann. In ähnlichen Sachverhalten³⁹ könnte es sogar an einer entsprechenden Vereinbarung zwischen Betreiber/Mitglied und Diensteanbieter scheitern. Im Ergebnis dürfte es regelmäßig an der gewünschten Verantwortlichkeitsverteilung und Transparenz (mangels Kenntnis) fehlen.

Dabei ist ins Felde zu führen, dass allen gemeinsam handelnden Verantwortlichen ein Bußgeld durch die Aufsichtsbehörde droht, wenn keine Vereinbarung im Sinne von Art. 26 DS-GVO getroffen wird.⁴⁰ Dieses Erfordernis besteht zwar auch bei der Auftragsverarbeitung, würde jedoch bei der oftmals nicht erkennbaren gemeinsamen Verantwortlichkeit die kleineren Unternehmen oder sogar Privatpersonen als Nutzer benachteiligen.⁴¹ Kontroverse Szenarien dürften bestehen, wenn selbst der Nutzer oder ein Forum-Moderator hiervon ohne Kenntnis dieser Rechtslage erfasst werden würde.

Ferner könnte auch die Verantwortlichkeit der Nutzer bei einer Blockchain angenommen werden.⁴² Mithin lässt sich auch die (eigene) Verantwortlichkeit einer WEG⁴³ oder des Betriebsrats diskutieren.⁴⁴ Und auch in der modernen Arbeitswelt bestehen unterschiedliche Szenarien der Verantwortlichkeit bei Freelancern⁴⁵ oder „Bring Your Own Device“-Regelungen.⁴⁶

Sogar beim Internet of Things (IoT) zeichnen sich derartige Risiken ab. Wird der Privatbürger nun durch sein connected car, dem vernetzten Lautsprecher oder sogar einem intelligenten und App-gesteuertem Wasserhahn zum datenschutzrechtlichen Verantwortlichen, der sich deshalb Ansprüchen auf Schadensersatz bzw. den Pflichten der Datenschutz-Grundverordnung ausgesetzt sieht?⁴⁷

Führt man dieses Szenario fort, könnte der Privatanutzer zum Verantwortlichen werden, wenn vernetzte Geräte eine Datenverarbeitung hervorrufen bzw. teilen und ihm hierbei ein großes Maß an Steuerung und Auswertung derselbigen in die Wiege gelegt wird. Es ist wahrlich der Konflikt zwischen vermeintlich individueller Freiheit des Benutzers, die Anwendungen eigenständig zu beherrschen oder zu erweitern und zwingenden technischen Vorgaben der Monopolisten à la Google, Amazon, Facebook und Co. zu beobachten. Daher wäre es wünschenswert, die gemeinsame Verantwortlichkeit nicht ausufern zu lassen.

Wäre dieses Bild nicht schon abstrus genug, lassen sich mit Fokus auf die Zukunft sogar noch neue Fälle konstruieren, die das Modell der Datenschutz-Grundverordnung gänzlich zum Schwanken bringt. Zu denken wäre an die Künstliche Intelligenz (bzw. deren Figur) als eigener Verantwortlicher innerhalb einer Anwendung oder einer Plattform (Alexa, Smartphone).⁴⁸ So mag der Entwickler oder der Betreiber von KI-Anwendungen ein grobes Konzept entworfen haben, um beispielsweise anhand der deepLearning Technologie zukünftige Verbrechen,⁴⁹ Krankheiten⁵⁰ oder Gefühle von Autofahrern⁵¹ erkennen bzw. vorhersagen zu können. Derartige Systeme finden bereits in vielen Lebensbereichen mit steigender Anzahl Einzug. Doch wohnt dem KI-Konzept der Gedanke inne, die Technologie könne irgendwann einmal in einem Blackbox-Verfahren (und als elektronische Person des Rechts⁵²) selbstlernende Züge einnehmen und neue Muster/Berechnungen für ergebnisoffene Zielvorhaben generieren. Zu denken wäre an einen digitalen Assistenten, der mit fortschreitendem Wissen und angesichts langwieriger Lernprozesse am/mit dem Betroffenen in Zukunft auch noch zum Arzt, Banker oder Anwalt des Nutzers wird. Wenn Alexa den Nutzer in dessen Wohnraum „husten“ hört und später nicht nur entsprechen-

42 Vgl. *Erbguth/Fasching*, ZD 2017, 560, 654.

43 Vgl. *Horst*, ZAP 2018, 597.

44 *Schmidt/Rossow*, DSBerater 2019, 4, 5.

45 Vgl. *Conrad*, DuD 2019, 134, 136.

46 Mehr dazu *Helfrich*, in: *Forgó/Helfrich/Schneider*, Betrieblicher Datenschutz, Teil 5, Kapitel 2, Rn. 31 ff.

47 Vgl. *Wagner*, ZD 2018, 307, 308 f.

48 *Conrad*, DuD 2018, 541, 544.

49 <https://www.heise.de/tp/features/KI-System-zur-praeventiven-Identifizierung-von-moeglichen-Straftaetern-4235898.html> (letzter Abruf: 10.5.2019).

50 Vgl. <https://www.spiegel.de/gesundheit/diagnose/kuenstliche-intelligenz-erkennt-seltene-erbkrankheiten-a-1247042.html> (letzter Abruf: 10.5.2019); <https://www.mdr.de/wissen/mensch-alltag/gesichtserkennung-als-diagnose-hilfe-100.html> (letzter Abruf: 10.5.2019).

51 Vgl. <https://www.golem.de/news/affectiva-ki-erkennt-die-gefuehle-von-autofahrern-1903-140255.html> (letzter Abruf: 10.5.2019).

52 Vgl. Entwurf einer Erschließung des Europäischen Parlaments (Januar 2017), http://www.europarl.europa.eu/doceo/document/A-8-2017-0005_DE.html?redirect (letzter Abruf: 30.6.2019).

36 Dazu mehr unter 3.0.

37 *Schreiber*, ZD 2019, 55, 60.

38 EuGH, Urteil vom 5.6.2018, Az.: C-210/16.

39 Praktisch bei jedem umfangreichen Portal/Webdienst mit Nutzerprofilen und Inhaltssteuerung des Nutzers.

40 *Martini*, in: *Paal/Pauly*, DS-GVO, Art. 26 DS-GVO, Rn. 5 f.

41 *Wagner*, ZD 2018, 307, 312.

de Medikamente bestellt,⁵³ sondern gleich auch die Medikation und weitere Behandlung empfiehlt bzw. dem Nutzer gegenüber ausspricht, sind wir nicht mehr weit von dieser Fiktion entfernt. Dann würde ein neuer Zweck der Datenverarbeitung verfolgt, neue Mittel der Datenverarbeitung gegebenenfalls herangezogen und eine eigene Verantwortlichkeit der KI-Anwendung anzunehmen sein. Nach den skizzierten Abgrenzungskriterien würde also bei „freiwerdender“ KI eine eigene Verantwortlichkeit nahelegend sein, von der sich spätestens bei der Aufklärung und Haftung der Entwickler, Betreiber oder Nutzer distanzieren würde.

Dies hieße aber auch, dass der (neue) Verantwortliche, selbst als Privatbürger, den datenschutzrechtlichen und teils bußgeldbewehrten Pflichten nachzukommen hat, zu welchen unter anderem die Umsetzung der Informationspflichten, Meldung von Datenpannen, Wahrung der Betroffenenrechte und Einhaltung angemessener technisch-organisatorischer Maßnahmen, wie auch die Einhaltung der Rechtmäßigkeit der Datenverarbeitung zählen. Während Verbände, kleinere Unternehmen und Privatpersonen unzumutbar belastet werden, könnten zukünftige Technologien an rechtliche Grenzen stoßen. Die erwähnte elektronische Person zur KI-Anwendung oder der Nutzer von IoT-Geräten als Verantwortlicher im Sinne von Art. 4 Nr. 7 DS-GVO müsste – plakativ formuliert – schließlich die Einwilligung des Nutzers (bzw. Rechtmäßigkeit der Datenverarbeitung) wie auch allgemeine Datenschutzerklärung vorhalten, die Betroffenenrechte umsetzen bzw. dokumentieren und sogar ein Verzeichnis der Verarbeitungstätigkeiten führen (können). Vor allem müsste die KI derartige Anforderungen überhaupt umsetzen können, also folglich innerhalb der Anwendung die technischen und rechtlichen Vorkehrungen implementiert bzw. die KI hierauf programmiert worden sein, andernfalls dürfte die Datenverarbeitung unzulässig sein – mit der Konsequenz, dass der Nutzer (im Falle einer gemeinsamen Verantwortlichkeit) als Adressat in die Pflicht zu nehmen wäre.

Man stelle sich vor, der private Nutzer seiner modernen Endgeräte müsste sich um die Einhaltung der datenschutzrechtlichen Bestimmungen bemühen. Und das Haushaltsprivileg wäre womöglich dann nicht mehr gegeben, wenn der Nachbar oder die Cousine kurzzeitig zu Besuch kommt bzw. im connected Car im Straßenverkehr mitfährt und von den digitalen Assistenten erfasst wird, oder aber die Daten in weitreichend vernetzten Systemen verarbeitet werden, was zunehmend zu beobachten ist.

Das Recht (der Datenschutz-Grundverordnung) strahlt dann in die „Privatsphäre“ des Einzelnen aus, um einen effizienten Schutz der personenbezogenen Daten nach der Datenschutz-Grundverordnung zu gewährleisten, belastet in der Konsequenz jedoch zumindest den Nutzer und mittelbar unter Umständen auch die Anbieter/Hersteller der Produkte. Im Hinblick auf das technologische Zukunftsbild droht sogar das Recht ins Leere zu laufen, wenn die Verantwortungsverteilung bzw. Verantwortlichkeitskette nicht mehr aufzulösen ist und daher mit zunehmenden Adressatenkreis keine effiziente Durchsetzung der Datenschutz-Grundverordnung mehr möglich ist.⁵⁴

4 Lösungsmöglichkeiten

Angesichts der zuletzt genannten Fallbeispiele gilt es neue Modelle im Datenschutzrecht zu entwickeln. Es ist zwingend die Verantwortlichkeit (auch für Folge-Prozesse) festzulegen, um zu verhindern, dass sich Anbieter aus der Haftung / Pflicht zu entziehen versuchen oder aber der Nutzer in die Verantwortlichkeit gedrängt wird. Die rechtsdogmatische Begründung einer (fiktiven) Verantwortlichkeit einer Einheit ohne Vermögen, tatsächlicher Einflussnahme oder sogar außerhalb menschlicher Steuerung ist nicht zielführend und mag höchstens eine juristische Diskussion erfüllen.

Ebenso sind zukünftige Konstellationen zu vermeiden, in welchen Anbieter mittels ihrer Monopolstellung (Kräfteverhältnis) in Folge der EuGH-Rechtsprechung⁵⁵ eine gemeinsame Verantwortlichkeit konstruieren und etwaige Pflichten auf kleinere Unternehmen abwälzen. Würden sogar Privatpersonen als Verantwortlicher eingestuft werden, beispielsweise durch einen umfangreichen Dienst oder Feature bei IoT-Geräten, droht ein unangemessenes Haftungsverhältnis, indem die Haftung und Umsetzung der Pflichten aus der Datenschutz-Grundverordnung ebenso gegenüber der Privatperson gelten würden. Hier sollte eine Freistellung der Haftung bzw. eine Reduzierung der Verantwortlichkeit auf null seitens der Privatperson zulässig sein. Das wird auch grundsätzlich durch Haftungsregelung der Datenschutz-Grundverordnung (Art. 82 Abs. 5 DS-GVO) austariert werden können, wenn angesichts der gesamtschuldnerischen Haftung der gemeinsam Verantwortlichen im Innenverhältnis ein Ausgleich zwischen den Verantwortlichen nach „ihrem Anteil an der Verantwortung für den Schaden“ erfolgen kann, der sich in der getroffenen Vereinbarungen und der hierin definierten Aufgaben/Rollenverteilung festlegen lässt.⁵⁶ Dennoch drängt sich eine Anpassung der Definition des Verantwortlichen auf, um dessen Reichweite zu beschränken und eine Ausweitung der Vorschriften der Datenschutz-Grundverordnung auf Privatpersonen oder kleinere Akteure zu verhindern. Das könnte unter Umständen auch durch eine maßvolle Privilegierung (wie das Haushaltsprivileg⁵⁷) erreicht werden.

Und auch ein weiteres Zukunftsszenario sollte zu denken geben. So ist im Fall der „Künstlichen Intelligenz“ zu überdenken, ob die Konstruktion der Verantwortlichkeit der KI als solche (als elektronische Rechtsfigur) sinnvoll erscheint. Die KI als Programm kann angehalten sein, technische Anfragen automatisch zu beantworten oder umzusetzen, wie z. B. die Mitteilung von Informationen oder Umsetzung des Widerrufs oder einer Löschung der Daten, jedoch wird ein fiktiver Computer/Roboter schwerlich mit „Bußgeldern“ oder „Strafen“ beeinflusst werden können, sofern die Figur nicht über Vermögen und Vernunft verfügt. Daher sollten die Entwickler oder Betreiber als Person oder als Gesellschaft in die Verantwortung bzw. Haftung einbezogen werden.

Die Hambacher Erklärung zur Künstlichen Intelligenz vom 3. April 2019⁵⁸ im Rahmen der Entschließung der 97. Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und

⁵³ So z. B. EuGH, Urteil vom 5.6.2018, Az.: C-210/16.

⁵⁶ Vgl. Martini, in: Paal/Pauly, DS-GVO, Art. 26 DS-GVO, Rn. 5 f.; Bergt, in: Kühling/Buchner, Art. 82 DS-GVO, Rn. 60.

⁵⁷ Siehe oben, 2.3 unterer Absatz.

⁵⁸ https://www.datenschutz.rlp.de/fileadmin/lfdi/Konferenzdokumente/Datenschutz/DSK/Entschliessungen/097_Hambacher_Erklaerung.pdf (letzter Abruf am 15.5.2019).

⁵³ Vgl. dazu: <https://www.datenschutz-notizen.de/alexa-hoert-dich-husten-bevor-du-ueberhaupt-erkaeltet-bist-4021452/> (letzter Abruf: 10.5.2019).

⁵⁴ Vgl. Schreiber, ZD 2019, 55, 60.

Highlight



T. Hess

Digitale Transformation strategisch steuern

Vom Zufallstreffer zum systematischen Vorgehen

2019, XII, 216 S. 37 Abb., 1 Abb.

in Farbe. Book + eBook. Geb.

€ (D) 24,99 | € (A) 25,58 | *sFr 27,00

ISBN 978-3-658-24474-3

€ 19,99 | *sFr 21,50

ISBN 978-3-658-24475-0 (eBook)

- Ein Leitfaden für Unternehmen zum richtigen Umgang mit der digitalen Transformation
- Enger Bezug zu neusten wissenschaftlichen Erkenntnissen

Ihre Vorteile in unserem Online Shop:

Über 280.000 Titel aus allen Fachgebieten | eBooks sind auf allen Endgeräten nutzbar | Kostenloser Versand für Printbücher weltweit

€ (D) sind gebundene Ladenpreise in Deutschland und enthalten 7 % für Printprodukte bzw. 19 % MwSt. für elektronische Produkte. € (A) sind gebundene Ladenpreise in Österreich und enthalten 10 % für Printprodukte bzw. 20 % MwSt. für elektronische Produkte. Die mit * gekennzeichneten Preise sind unverbindliche Preisempfehlungen und enthalten die landesübliche MwSt. Preisänderungen und Irrtümer vorbehalten.

Part of **SPRINGER NATURE**

[springer.com/dts](https://www.springer.com/dts)

A70439

der Länder (DSK) mit sieben aufgestellten Regeln zum Datenschutz macht auf diesen Umstand aufmerksam. Hierin wird gefordert, dass bei komplexen, undurchdringlichen Sachverhalten weiterhin eine Verantwortlichkeit bei einem Menschen oder einem involvierten Unternehmen zu bestimmen ist.⁵⁹ In dem fiktiven Schauspiel der Datenverarbeitung soll demnach also eine Figur als Moderator bestimmt werden. Andernfalls entstehen denkbare Regelungslücken oder Wertungswidersprüche.

Es wäre zu überlegen, ob nicht – ähnlich wie im Urheberrecht – hier von Gesetzes wegen eine „Rolle“ als Verantwortlicher für einen angestoßenen Prozess zu begründen wäre. Selbst vertragliche Regelungen dürfen dies nicht abbedingen.

5 Fazit

Das derzeitige Modell des Datenschutzrechts bietet im Hinblick auf die Verantwortlichkeiten und den daraus erwachsenen Folgen/Ansprüchen für den Handelnden nicht ausreichend Rechtssicherheit. Die weit gefasste Definition erschafft einen großen Adressatenkreis bzw. viele datenschutzrechtlich Verantwortliche, was den Betroffenen die Umsetzung seiner ihm durch die Datenschutz-Grundverordnung gegebenen Instrumente erleichtern und insgesamt in seinen Rechten schützen soll, jedoch in der Konsequenz für die Unternehmen und sogar einzelnen Personen jenseits der „Haushaltsprivilegierung“ erhebliche Belastungen bedeuten kann. Fehlt es an konkreten Vereinbarungen gem. Art. 26 DS-GVO, drohen den handelnden Akteuren (und Privatpersonen?) nicht nur Bußgelder, sondern darüber hinaus sogar, dass die Regelungen der Verordnung ins Leere laufen.

Denn je mehr Möglichkeiten der Einflussnahme in den modernen Systemen der Datenverarbeitung auf Seiten des Nutzers vorliegen, desto eher wird der Nutzer in die Situation der gemeinsamen Verantwortlichkeit gedrängt und der Haftung ausgesetzt werden können. Dieses dürfte langfristig den Nutzer vom Kauf solcher Produkte abschrecken. Insgesamt droht eine unklare Aufgabenverteilung mit unbilliger Verschiebung der Haftung, was in letzter Konsequenz die effiziente Durchführung der Datenschutz-Grundverordnung einschränkt.

Im Kontext der zukünftig erdenklichen Szenarien der KI-Anwendungen muss gesondert klargestellt werden, dass die Verantwortlichkeit nicht beim Nutzer selbst oder gar beim KI-System (Roboter als elektronische Person) liegen darf, was Wertungswidersprüche und Nachteile hervorruft und auch die Entwickler bzw. Betreiber aus der Haftung nehmen würde.

⁵⁹ Vgl. kritisch dazu <https://www.datenschutz-notizen.de/die-sieben-neuen-ki-regeln-der-datenschutzkonferenz-0722439/> (letzter Abruf am 15.5.2019).