

# Perspektiven der Auftragsverarbeitung

## Wegfall der Privilegierung mit der DS-GVO?

Systemwartung  
IT-Services  
Dienstleister  
Beauftragung  
Haftung

■ In unserer arbeitsteilig organisierten und immer stärker digitalisierten Wirtschaft ist die Einschaltung von Dienstleistern für die Verarbeitung personenbezogener Daten oder zur Systemwartung sowie das Outsourcing ganzer Arbeitsprozesse gelebte Realität und faktische Notwendigkeit. Aus dem BDSG ergeben sich detaillierte Anforderungen für die Auswahl und Beauftragung von Dienstleistern. Diese werden mit der DS-GVO fortgeschrieben und teilweise verschärft. Besonders brisant für deutsche Verantwortliche ist, dass die Privilegierung der Auftrags(daten)verarbeitung scheinbar entfällt. Lösungen für diese und weitere Herausforderungen der Einschaltung von Dienstleistern unter der DS-GVO werden im Folgenden dargestellt.

Lesedauer: 16 Minuten

■ In our economy, which is based on the division of labor and is increasingly digitalized, the inclusion of service providers to process personal data or for system maintenance, as well as outsourcing entire business processes is lived reality and factual necessity. The German Federal Data Protection Act (BDSG) sets forth detailed requirements for the selection and instruction of service providers. These are continued in the DS-GVO and, in part, intensified. It is critical, in particular for German persons in charge, that the granting privilege regarding commissioned (data) processing apparently no longer applies. Solutions for these and other challenges for the inclusion of service providers under the DS-GVO will be detailed below.

## I. Privilegierung der Auftragsverarbeitung nach BDSG und Änderungen durch DS-GVO

Das BDSG privilegiert die Einschaltung von Dienstleistern innerhalb des Europäischen Wirtschaftsraums (EWR). Gem. § 3 Abs. 8 Satz 3 BDSG sind diese Dienstleister keine Dritten – sie gehören also aus Sicht des materiellen Datenschutzrechts zur verantwortlichen Stelle. Die Weitergabe personenbezogener Daten an solche Dienstleister ist keine Übermittlung i.S.d. § 3 Abs. 3 BDSG, sondern wird rechtlich wie eine Weitergabe innerhalb der Organisation des Verantwortlichen behandelt. Da per Definition keine Übermittlung und mithin kein Fall der Verarbeitung vorliegt, bedarf diese Weitergabe keiner Rechtfertigung. Diese Tatsache ist in Deutschland als „Privilegierung der Auftragsdatenverarbeitung“ bekannt geworden. Diese in den Begriffsbestimmungen des BDSG angelegte Privilegierung greift jedoch nach dem Wortlaut von § 3 Abs. 8 Satz 3 BDSG nur innerhalb des EWR. Die Datenweitergabe an Dienstleister in Drittstaaten ist hingegen nach verbreiteter Ansicht eine rechtfertigungsbedürftige Übermittlung.<sup>1</sup>

Betrachtet man aus diesem deutschen Rechtsverständnis die DS-GVO, scheint die Privilegierung der (EWR-)Auftragsdatenverarbeitung ersatzlos zu entfallen. Denn anders als im BDSG ist die Privilegierung in den Definitionen des Art. 4 DS-GVO nicht konsequent zum Ausdruck gebracht worden. Zwar gelten Auftragsverarbeiter nach Art. 4 Nr. 10 DS-GVO weiterhin nicht als Dritte im Verhältnis zum Verantwortlichen; nun auch wenn sie sich außerhalb des EWR befinden.<sup>2</sup> Der entscheidende Vorgang der Weitergabe personenbezogener Daten an Auftragsverarbeiter wird jedoch anders als nach § 3 Abs. 3 BDSG nicht vom Verarbeitungsbegriff und damit nicht vom Anwendungsbereich des materiellen Datenschutzrechts ausgenommen.<sup>3</sup> Es handelt sich vielmehr um eine Verarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO, die grundsätzlich einer datenschutzrechtlichen Rechtfertigung bedarf.

Von akademischer Relevanz ist, welche Form der Verarbeitung die Einschaltung von Dienstleistern nach der DS-GVO ist. Einschlägig dürfte die Offenlegung sein, welche sich in die Unterfälle der „Übermittlung“, „Verbreitung“ und „andere Form[en] der Bereitstellung“ gliedert. Vom Begriffsverständnis ausgehend, ergibt es Sinn, die Übermittlung auf die Bereitstellung für

Dritte zu beschränken und so von einer „andere[n] Form der Bereitstellung“ abzugrenzen. Da ein Auftragsverarbeiter nach Art. 4 Nr. 10 DS-GVO kein Dritter ist, läge also bei der Einschaltung von Dienstleistern eine „andere Form der Bereitstellung“ vor. I.E. ist es aber unerheblich, um welche Form der Offenlegung (oder sonstige Form der Verarbeitung) es sich handelt, da die DS-GVO an sämtliche Unterfälle der Verarbeitung dieselben Rechtsfolgen knüpft. Entscheidend ist, dass eine Verarbeitung und damit ein datenschutzrelevanter Vorgang vorliegt, der grundsätzlich ein Rechtfertigungsbedürfnis auslöst.

Tatsächlich wird aus dem Vorstehenden zum Teil der Schluss gezogen, die Privilegierung der (EWR-)Auftragsverarbeitung würde nunmehr entfallen, und jede Datenüberlassung an Auftragsverarbeiter sei zukünftig nach den allgemeinen Regeln der Art. 6 und 9 DS-GVO zu rechtfertigen. Gerade die Auftragsverarbeitung besonderer Kategorien personenbezogener Daten – etwa Gesundheitsdaten – wäre dann nach Art. 9 Abs. 2 DS-GVO nur unter sehr engen Voraussetzungen zulässig. Dieses Problem stellt sich unter dem BDSG derzeit nur für die Einschaltung von Dienstleistern außerhalb des EWR, für die es unter dem BDSG keine Privilegierung gibt. Die Befürchtung ist nun, dass mit Inkrafttreten der DS-GVO dieses Problem auch auf die Einschaltung von Dienstleistern innerhalb des EWR erstreckt wird.

## II. Rechtfertigung der Auftragsverarbeitung nach DS-GVO

Die Diskussion um die Rechtfertigung der Einschaltung von Dienstleistern unter der DS-GVO hat gerade erst begonnen. Offizielle Stellungnahmen der Art. 29-Datenschutzgruppe oder der Aufsichtsbehörden gibt es noch nicht. In der Literatur deutet sich ein Streit an, ob die Einschaltung von Dienstleistern stets nach Art. 6 Abs. 1 DS-GVO – bzw. für besondere Kategorien personenbezogener Daten nach Art. 9 Abs. 2 DS-GVO – ge-

<sup>1</sup> Diese Einschaltung von Dienstleistern in Nicht-EWR-Staaten wird auch als „unechte Auftragsdatenverarbeitung“ bezeichnet.

<sup>2</sup> Schreiber, in: Plath, BDSG DSGVO, 1. Aufl. 2016, Art. 4 Rdnr. 33.

<sup>3</sup> Laue/Nink/Kremer, Das neue Datenschutzrecht in der betrieblichen Praxis, 1. Aufl. 2016, S. 163; Robnagel/Kroschwald, ZD 2014, 495, 497; a.A. Albrecht/Jotzo, Das neue Datenschutzrecht der EU, 1. Aufl. 2016, S. 97.

rechtfertigt werden muss (Theorie der Rechtfertigungsbedürftigkeit)<sup>4</sup> oder ob das Rechtfertigungserfordernis für die Beauftragung von Dienstleistern nicht gilt, die Privilegierung also unter der DS-GVO fortbesteht (bzw. sogar auf Nicht-EWR-Verarbeiter ausgeweitet wird) und die Bereitstellung von Daten an einen Auftragsverarbeiter auf Basis eines Auftragsverarbeitungsvertrags und den weiteren Voraussetzungen gem. Art. 28 DS-GVO keiner (weiteren) Rechtfertigung bedarf (Privilegierungstheorie).<sup>5</sup>

## 1. Theorie der Rechtfertigungsbedürftigkeit

Die Theorie der Rechtfertigungsbedürftigkeit<sup>6</sup> zieht aus dem vermeintlichen Wegfall der Privilegierung der Auftragsverarbeitung den Schluss, die Einschaltung eines Dienstleisters müsse wie jeder andere Datenumgang in jedem Einzelfall nach den allgemeinen Rechtfertigungstatbeständen legitimiert werden. Diese Haltung erscheint – von der aktuellen Rechtslage nach dem BDSG ausgehend – auf den ersten Blick konsequent.

Die Theorie der Rechtfertigungsbedürftigkeit führt bei der Auftragsverarbeitung „normaler“ personenbezogener Daten auch zu sachgerechten Ergebnissen. Die Einschaltung eines Dienstleisters wird nämlich in der Regel im berechtigten Interesse des Verantwortlichen gem. Art. 6 Abs. 1 lit. f DS-GVO stehen; soweit die Voraussetzungen gem. Art. 28 DS-GVO gewahrt sind, werden die Betroffeneninteressen dem auch regelmäßig nicht entgegenstehen.

Für die Auftragsverarbeitung besonderer Kategorien personenbezogener Daten ergeben sich im Hinblick auf den Schutzzweck des Datenschutzrechts jedoch nicht angemessene Hindernisse. Man müsste die Auftragsverarbeitung dann nämlich an den hohen Anforderungen des Art. 9 Abs. 2 DS-GVO messen. Die Einschaltung von Dienstleistern wäre dann für die Verarbeitung besonderer Kategorien personenbezogener Daten weitgehend ausgeschlossen und Verantwortliche müssten entsprechende Verfahren ausschließlich intern ausführen. Daneben sprechen weitere zwingende Gründe gegen die Theorie der Rechtfertigungsbedürftigkeit, die im Folgenden dargestellt werden.

<sup>4</sup> Laue/Nink/Kremer (o. FuBn. 3), S. 165; Koós/Englisch, ZD 2014, 276, 284; Piltz, abrufbar unter: <https://www.delegedata.de/2016/05/datenschutz-grundverordnung-kaum-beachtet-deutsche-privilegierung-der-auftragsdatenverarbeitung-entfaellt/>; Roßnagel, Europäische Datenschutzgrundverordnung, 1. Aufl. 2016, S. 180; Roßnagel/Kroschwald, ZD 2014, 495, 498.

<sup>5</sup> Albrecht/Jotzo (o. FuBn. 3); Bogendorfer, in: Knyrim, Datenschutzgrundverordnung, 1. Aufl. 2016, S. 172 f.; Härting, ITRB 2016, 137, 139; Hullen, in: v.d. Bussche/Voigt, Konzerndatenschutz, 1. Aufl. 2014, Teil 8, Rdnr. 84; Plath, in: Plath (o. FuBn. 2), Art. 28 DS-GVO Rdnr. 3.

<sup>6</sup> Laue/Nink/Kremer (o. FuBn. 3), S. 165; Koós/Englisch, ZD 2014, 276, 284; Piltz (o. FuBn. 4); Roßnagel (o. FuBn. 4); Roßnagel/Kroschwald, ZD 2014, 495, 498.

<sup>7</sup> Albrecht/Jotzo (o. FuBn. 3); Bogendorfer (o. FuBn. 5); Härting, ITRB 2016, 137 (139); Hullen (o. FuBn. 5); Plath (o. FuBn. 5); Stellungnahme des BayLDA zur DS-GVO, Auftragsverarbeitung nach der DS-GVO, Stand: 26.10.2016, abrufbar unter: [https://www.lida.bayern.de/media/baylda\\_ds-gvo\\_10\\_processor.pdf](https://www.lida.bayern.de/media/baylda_ds-gvo_10_processor.pdf).

<sup>8</sup> Bogendorfer (o. FuBn. 5).

<sup>9</sup> Albrecht/Jotzo (o. FuBn. 3); Härting, ITRB 2016, 137, 139; Hullen (o. FuBn. 5).

<sup>10</sup> Vgl. auch schon Art. 18 Abs. 3 DS-RL.

<sup>11</sup> Vgl. Art. 28 Abs. 3 DS-GVO: „Processing by a processor shall be governed by a contract ...“ (englische Fassung); „Le traitement par un sous-traitant est régi par un contrat ...“ (französische Fassung); „databehandlers behandling skal være reguleret af en kontrakt eller et andet retligt dokument i henhold til EU-retten“ (dänische Fassung).

<sup>12</sup> Härting, ITRB 2016, 137, 139.

<sup>13</sup> So zur DS-RL Spoerr, in: Wolff/Brink, BDSG, 1. Aufl. 2013, § 11 Rdnr. 31 f.

<sup>14</sup> Vgl. Art. 2 lit. b DS-RL versus Art. 4 Nr. 2 DS-GVO; die Erweiterung der Definition durch die DS-GVO ist in diesem Zusammenhang ohne Belang.

<sup>15</sup> Vgl. Art. 2 lit. f DS-RL versus Art. 4 Nr. 10 DS-GVO.

<sup>16</sup> Vgl. Art. 2 lit. f DS-RL versus Art. 4 Nr. 8 DS-GVO; sowie Art. 17 Abs. 2 und Abs. 3 DS-RL versus Art. 28 Abs. 3 lit. a DS-GVO.

<sup>17</sup> So zu Recht Drewes/Monreal, PinG 2014, 143, 145.

## 2. Privilegierungstheorie

Nach der Privilegierungstheorie<sup>7</sup> ist die Auftragsverarbeitung ein datenschutzrechtlicher Sonderfall, für den andere Rechtfertigungsmaßstäbe heranzuziehen sind als für die Verarbeitung personenbezogener Daten durch den Verantwortlichen selbst; nämlich die Anforderungen gem. Art. 28 DS-GVO. Sind diese Anforderungen erfüllt, ist die Einschaltung eines Dienstleisters gerechtfertigt<sup>8</sup> oder nicht (gesondert) rechtfertigungsbedürftig.<sup>9</sup> Die Privilegierungstheorie ist aus den im Folgenden dargestellten Gründen zutreffend.

### a) Wortlaut

Der Wortlaut des Art. 28 Abs. 3 DS-GVO stützt die Privilegierungstheorie. Danach erfolgt „die Verarbeitung durch einen Auftragsverarbeiter ... auf der Grundlage eines Vertrags oder eines anderen Regelungsinstruments nach dem Unionsrecht oder dem Recht der Mitgliedstaaten ...“. <sup>10</sup> Es liegt also nahe, die nach Art. 28 DS-GVO geschlossene Vereinbarung über die Auftragsverarbeitung als Rechtfertigungsgrundlage der Datenüberlassung an den Auftragsverarbeiter anzusehen. Für sich allein kann dieses Argument freilich noch nicht überzeugen, da andere Sprachfassungen der DS-GVO auch so verstanden werden können, dass der Vertrag nicht Verarbeitungsgrundlage ist, sondern die Auftragsverarbeitung lediglich regelt bzw. die Anforderungen an deren (formale) Ausgestaltung.<sup>11</sup>

### b) Systematik

Vertreten wird auch, die Einschaltung eines Dienstleisters sei kein eigener Verarbeitungsschritt, sodass es kein Rechtfertigungserfordernis dafür gäbe.<sup>12</sup> Dieser Argumentationsansatz stützt sich auf das Argument, die Definition der Verarbeitung in Art. 4 Nr. 2 DS-GVO sei nicht „kleinschrittig“ angelegt; die Zulässigkeit einzelner Verarbeitungsvorgänge, wie die Überlassung personenbezogener Daten an einen Dienstleister, müsse daher nicht ergänzend zur Rechtfertigung der Datenverarbeitung durch den Verantwortlichen geprüft werden. Richtig ist jedenfalls, dass weder die Datenschutzrichtlinie (RL 95/46/EG – DS-RL) noch die DS-GVO dem Verständnis entgegensteht, dass es sich bei der Auftragsverarbeitung um einen einheitlichen Verarbeitungsvorgang des Auftraggebers handelt.<sup>13</sup> Mangels entsprechend klarer Ausprägung im Wortlaut ist dieses Argument alleine aber wohl ebenfalls nicht hinreichend, um die Privilegierungstheorie zu stützen.

### c) Historische Auslegung

Entscheidend für die Privilegierungstheorie streitet letztlich die historische Auslegung. Dabei darf der Fehler der Theorie der Rechtfertigungsbedürftigkeit nicht wiederholt werden, welche die DS-GVO als Nachfolgeregelung zum BDSG interpretiert anstatt – wie es einzig richtig ist – als Nachfolgeregelung der DS-RL. Bei der gebotenen autonomen Auslegung der DS-GVO vor dem Hintergrund der DS-RL wird zunächst klar, dass die DS-GVO bei der Legitimierung der Auftragsdatenverarbeitung keineswegs von der DS-RL abweichen, also insoweit keine neue Rechtslage schaffen will. Vielmehr übernimmt sie die in diesem Zusammenhang entscheidenden Definitionen – „Verarbeitung“, <sup>14</sup> „Dritter“, <sup>15</sup> „Auftrags(daten)verarbeitung“<sup>16</sup> – weitgehend wortgleich. Ein relevanter Unterschied ergibt sich insoweit nur zu den Definitionen des BDSG, nicht aber zur DS-RL.

Damit entpuppt sich der vermeintliche „Wegfall der Privilegierung“ als Fehleinschätzung. Denn die Privilegierung der Auftragsdatenverarbeitung war keine Erfindung des BDSG-Gesetzgebers, sondern war bereits in der DS-RL vorgesehen.<sup>17</sup> Das Recht, einen Auftragsverarbeiter einzuschalten und Daten an diesen zu übermitteln, ist zwar in die DS-RL nicht ausdrücklich aufgenommen worden, es ist aber in der Entscheidungsbefug-

nis des Verantwortlichen, der per Definition über die „Zwecke und Mittel der Verarbeitung“ entscheidet, enthalten.<sup>18</sup> Auch dies hat die DS-GVO übernommen.<sup>19</sup>

Ferner ist die Privilegierung in der Regelung des Art. 16 DS-RL und nunmehr in Art. 29 DS-GVO vorausgesetzt, wonach der Auftragsverarbeiter die Daten ausschließlich auf Weisung verarbeiten darf. Diese Vorschrift will die Datenverarbeitung einerseits beschränken (auf den Rahmen der Weisungen), umgekehrt aber auch die weisungsgerechte Verarbeitung erlauben. Sie legitimiert damit als notwendige Vorstufe dieser Verarbeitung auch die Datenüberlassung an den ordnungsgemäß verpflichteten Auftragsverarbeiter.

Das in der Richtlinie implizierte Privileg ist in den mitgliedstaatlichen Umsetzungsvorschriften zum Teil explizit zum Ausdruck gekommen. Zu nennen ist zum einen das BDSG selbst (welches die Privilegierung allerdings auf EWR-Auftragsverarbeiter beschränkt). Ein weiteres Beispiel ist das österreichische Datenschutzgesetz (DSG 2000), welches in wünschenswerter Klarheit unter der Überschrift „Zulässigkeit der Überlassung von Daten zur Erbringung von Dienstleistungen“ in § 10 Abs. 1 Satz 1 DSG festhält: „Auftraggeber dürfen bei ihren Datenanwendungen Dienstleister in Anspruch nehmen, wenn diese ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten.“

Auch in anderen Umsetzungsgesetzen ist die Rechtsmacht des Verantwortlichen zur Bestimmung eines Auftragsverarbeiters zum Ausdruck gekommen, etwa im italienischen Datenschutzgesetz<sup>20</sup> oder im – ebenfalls auf der DS-RL beruhenden – Datenschutzgesetz der Schweiz.<sup>21</sup> Voraussetzung ist stets, dass der Auftragsverarbeiter ordnungsgemäß verpflichtet wird; eine weitere Rechtfertigungsprüfung findet dann nicht statt.

Diese in der DS-RL angelegte Privilegierung hat der deutsche Gesetzgeber – womöglich richtlinienwidrig – verkürzt, indem er sie auf Auftragsverarbeiter innerhalb des EWR eingeschränkt hat. Mit der DS-GVO wird dagegen das weite Privileg aus der DS-RL fortgeschrieben. Im Vergleich des BDSG mit der DS-GVO entfällt damit i.E. nicht die Privilegierung, sondern vielmehr deren Verkürzung durch das BDSG. I.E. handelt es sich bei der Auftragsverarbeitung nach der Konzeption der DS-GVO (wie schon der DS-RL) um einen datenschutzrechtlichen Sonderfall, der keiner weiteren Rechtfertigung bedarf, soweit der Auftragsverarbeiter ordnungsgemäß ausgewählt und verpflichtet wurde.

#### d) Teleologische Auslegung

Aus der Theorie der Rechtfertigungsbedürftigkeit ergeben sich Einschränkungen des IT-Outsourcing, die in einem krassen Gegensatz zur gelebten Praxis der zunehmenden Auslagerung von Datenverarbeitungen stehen und die nicht dazu beitragen, den Schutz der Betroffenen zu verbessern. Es ist nämlich keinesfalls anzunehmen, dass Verantwortliche, deren Kernkompetenz nicht in der Verarbeitung personenbezogener Daten liegt, diese besser schützen könnten als darauf spezialisierte Dienstleister. Soweit Dienstleister sorgfältig ausgewählt werden und sichergestellt ist, dass sie angemessene technisch-organisatorische Maßnahmen für den Schutz personenbezogener Daten getroffen haben, kann durch die Auftragsverarbeitung dann nämlich ein gleich hohes – meistens sogar ein höheres – Datenschutzniveau geschaffen werden.

Die materiellen Sondervorgaben für die Einschaltung von Dienstleistern in Art. 28 DS-GVO<sup>22</sup> stellen nämlich sicher, dass der Auftragsverarbeiter nur als „verlängerter Arm“ oder „Alter Ego“ des Verantwortlichen tätig und angemessen kontrolliert wird. Der Schutz der Betroffenen erfordert daher nicht, dass die Weitergabe der Daten zusätzlich gerechtfertigt wird. Das Ergebnis schafft vielmehr einen Ausgleich mit dem weiteren Zweck der DS-GVO, den freien Datenverkehr zu fördern (Art. 1 Abs. 3 DS-GVO).

Teilweise wird sogar vertreten, dass Art. 6 DS-GVO und Art. 9 DS-GVO teleologisch zu reduzieren und nicht auf die Auftragsverarbeitung anzuwenden seien.<sup>23</sup> Dem ist jedenfalls i.E. zuzustimmen. Ob es dieser teleologischen Reduktion zur Begründung der Privilegierungstheorie bedarf, kann aber letztlich dahinstehen. Es ergibt keinen Unterschied, wenn man die Privilegierung – wie es die historische Auslegung nahelegt – stattdessen auf eine implizite Auslagerungsbefugnis des Verantwortlichen stützt (die durch Art. 28 DS-GVO ausgestaltet ist) oder Art. 28 DS-GVO selbst als Rechtfertigungsnorm ansieht.

Vor allem steht die Privilegierung auch nicht im Widerspruch zum Schutzzweck des Art. 9 DS-GVO, hohen Schutz für die Verarbeitung besonderer Kategorien personenbezogener Daten zu gewährleisten. Dieser lässt sich nämlich auch bei einer Rechtfertigung gem. Art. 28 DS-GVO umsetzen. So sind diese hohen Schutzanforderungen nämlich durch den Auftragsverarbeiter insbesondere bei der Gestaltung technisch-organisatorischer Maßnahmen für die Verarbeitung zu berücksichtigen. Deren Konzeption und Einhaltung ist durch den Verantwortlichen zu kontrollieren.

#### e) Ergebnis

Die Auftragsverarbeitung ist nach hier vertretener Ansicht künftig zulässig, wenn der Verantwortliche und der Auftragsverarbeiter gem. Art. 28 Abs. 3 DS-GVO einen Vertrag über die Auftragsverarbeitung schließen und die übrigen Voraussetzungen gem. Art. 28 DS-GVO erfüllt sind. Einer darüberhinausgehenden Rechtfertigung nach allgemeinen datenschutzrechtlichen Rechtfertigungstatbeständen bedarf es dann nicht mehr. Im Unterschied zum BDSG entfällt nicht die Privilegierung, sondern es entfällt vielmehr die Diskriminierung der Nicht-EWR-Auftragsverarbeitung. Diese ist zukünftig zulässig, wenn die Voraussetzungen der Auftragsverarbeitung (Art. 28 DS-GVO) und zusätzlich die Voraussetzungen der Übermittlungen in Drittländer (Art. 44 ff. DS-GVO) erfüllt sind.

### III. Systemwartung

Nach § 11 Abs. 5 BDSG gelten für die Prüfung oder Wartung von Verfahren oder Datenverarbeitungsanlagen (also insbesondere Hard- und Softwarewartung, im Folgenden: Systemwartung) die Regelungen für die Auftragsverarbeitung gem. § 11 Abs. 1-4 BDSG entsprechend. Eine vergleichbare Regelung oder Sonderregelungen für die Systemwartung fehlen in der DS-GVO. Fraglich ist damit, unter welchen Voraussetzungen die Systemwartung künftig datenschutzrechtlich zulässig sein soll.

Mit dem Wegfall der Regelung in § 11 Abs. 5 BDSG wird damit der längst erledigt geglaubte Streit um die Rechtsnatur der Systemwartung scheinbar wieder relevant,<sup>24</sup> den der Bundesgesetzgeber 2001 mit der Regelung in § 11 Abs. 5 BDSG beendet hatte. Als Lösung wird vorgeschlagen, die Regelungen über die Auftragsverarbeitung analog auf die Systemwartung anzuwenden<sup>25</sup> oder die Systemwartung künftig nicht mehr als daten-

<sup>18</sup> Art. 2 lit. d DS-RL.

<sup>19</sup> Art. 4 Nr. 7 DS-GVO.

<sup>20</sup> S. das italienische Datenschutzgesetz (Decreto legislativo 30 giugno 2003, n. 196), Art. 29 Abs. 1: „Il responsabile è designato dal titolare facoltativamente“.

<sup>21</sup> S. das Schweizer Bundesgesetz über den Datenschutz, Art. 10a Abs. 1: „Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz Dritten übertragen werden, wenn ...“.

<sup>22</sup> Bogendorfer (o. Fußn. 5); s. hierzu auch Lissner, in: Taeger, Smart World – Smart Law, 1. Aufl. 2016, S. 406 f.

<sup>23</sup> Bogendorfer (o. Fußn. 5), S. 173.

<sup>24</sup> Dazu Büermann, RDV 1994, 202; Gabel, in: Taeger/Gabel, BDSG, 2. Aufl. 2013, § 11 Rdnr. 65; Wedde, in: Däubler/Klebe/Wedde/Weichert, BDSG, 4. Aufl. 2014, § 11 Rdnr. 73.

<sup>25</sup> Mithlein, RDV 2016, 74, 83.

schutzrechtlich relevanten Vorgang anzusehen.<sup>26</sup> Als weitere Möglichkeit kommt in Betracht, Systemwartung künftig als datenschutzrechtlich rechtfertigungsbedürftigen Vorgang gem. Art. 6 Abs. 1 DS-GVO bzw. Art. 9 Abs. 2 DS-GVO anzusehen.

Nach hier vertretener Ansicht ist jedoch auch der „Wegfall“ des § 11 Abs. 5 BDSG und die Einordnung der Systemwartung in das datenschutzrechtliche System der DS-GVO ein Scheinproblem. Die Regelungen des Art. 28 DS-GVO sind nämlich direkt auf die Systemwartung anzuwenden. Bei der Systemwartung erhält der Dienstleister in der Regel die Möglichkeit, auf personenbezogene Daten zuzugreifen. Es handelt sich dabei um eine Verarbeitung i.S.d. Art. 4 Nr. 2 DS-GVO. Ob Systemwartung dabei eine Offenlegung „durch Übermittlung“, „Verbreitung“ oder „eine andere Form der Bereitstellung“ ist, kann als akademische Frage offenbleiben (naheliegender wäre die Einordnung als andere Form der Bereitstellung).

All dies sind nach Art. 4 Nr. 2 DS-GVO aber nur Beispiele für die eigentliche Definition der Verarbeitung als „Vorgang ... im Zusammenhang mit personenbezogenen Daten“. Diese Definition erfüllt die Wartung eines IT-Systems in jedem Fall. Auch nach dem gesetzlichen Schutzzweck kann ein solcher Vorgang nicht dem Anwendungsbereich der DS-GVO entzogen werden, sofern er mit einer Zugriffsmöglichkeit auf die personenbezogenen Daten und damit mit einer Gefahr für das informationelle Selbstbestimmungsrecht der Betroffenen verbunden ist.

Diese Verarbeitung erfolgt auch im Auftrag des Verantwortlichen. Es handelt sich damit um einen Fall der Auftragsverarbeitung gem. Art. 28 Abs. 1 DS-GVO, die unter den Voraussetzungen des Art. 28 DS-GVO zulässig ist.

#### IV. Pflichten des Verantwortlichen

Anforderungen für die Einschaltung von Auftragsverarbeitern durch den Verantwortlichen ergeben sich insbesondere aus Art. 28 Abs. 1 und Abs. 3 DS-GVO. Hiernach muss der Verantwortliche den Auftragsverarbeiter entsprechend der aktuell anwendbaren Vorschrift des § 11 Abs. 2 BDSG im Hinblick auf seine Zuverlässigkeit sorgfältig auswählen. Die Zuverlässigkeit kann nach Art. 28 Abs. 5 DS-GVO insbesondere auch anhand der Einhaltung von genehmigten Verhaltensregelungen nach Art. 40 DS-GVO oder einer Zertifizierung des Dienstleisters nach Art. 42 DS-GVO beurteilt werden.<sup>27</sup>

Eine Herausforderung dabei ist, dass sich konkret erforderliche technisch-organisatorische Maßnahmen nicht abschließend aus der DS-GVO ergeben. Gem. Art. 32 Abs. 1 DS-GVO ergeben sich nur Mindestanforderungen, wie die Pseudonymisierung, Verschlüsselung und Maßnahmen zur Herstellung von Vertraulichkeit, Integrität und Verfügbarkeit. Diese Maßnahmen sind in der Anlage zu § 9 BDSG weitgehend enthalten, sodass es sich aus der Perspektive deutscher Verantwortlicher und Auftragsverarbeiter anbietet, technisch-organisatorische Datensicherheitskonzepte weiter danach zu konzipieren.<sup>28</sup>

In dieser ausdrücklichen Form neu sind jedoch technisch-organisatorische Maßnahmen zur schnellen Wiederherstellung von Systemen bei technischen Zwischenfällen (Art. 32 Abs. 1 lit. c DS-GVO) und technisch-organisatorische Maßnahmen zur regelmäßigen Evaluierung der Wirksamkeit der technisch-organisatorischen Maßnahmen insgesamt (Art. 32 Abs. 1 lit. d DS-GVO). Auf die Umsetzung dieser Maßnahmen sollte zukünftig ein besonderer Fokus gelegt werden.

<sup>26</sup> Lissner (o. FuBn. 22), S. 414 f.

<sup>27</sup> Hierzu Albrecht/Jotzo (o. FuBn. 3), S. 99.

<sup>28</sup> So auch Laue/Nink/Kremer (o. FuBn. 3), S. 219.

<sup>29</sup> Laue/Nink/Kremer (o. FuBn. 3); Schmitz/Dall'Armi, ZD 2016, 427, 432.

<sup>30</sup> Dazu Gabel (o. FuBn. 24), § 7 Rdnr. 25 ff.

Zusätzlich zur sorgfältigen Auswahl des Dienstleisters müssen Verantwortliche wie bisher mit diesem einen Vertrag über die Auftragsverarbeitung schließen. Die Anforderungen dafür ergeben sich aus Art. 28 Abs. 3 lit. a-h DS-GVO. Anders als aktuell nach § 11 Abs. 2 Satz 2 BDSG ist künftig gem. Art. 28 Abs. 9 DS-GVO neben der Schriftform aber auch die elektronische Form hinreichend. Alternativ zum Abschluss eines Vertrags über die Auftragsverarbeitung kommt nach Art. 28 Abs. 3 DS-GVO zudem in Betracht, den Dienstleister entsprechend einem anderen Rechtsinstrument des Unionsrechts oder des mitgliedstaatlichen Rechts zu verpflichten.

#### V. Pflichten des Auftragsverarbeiters

Anders als nach der Konzeption des § 11 Abs. 1 BDSG liegt die Verantwortung für die Einhaltung des Datenschutzrechts künftig nicht mehr allein bei dem Verantwortlichen, sondern sowohl bei dem Verantwortlichen als auch dem Auftragsverarbeiter, die gemeinsam die Einhaltung des Datenschutzrechts sicherstellen müssen.<sup>29</sup>

Die Pflichten des Auftragsverarbeiters ergeben sich zudem künftig stärker als bisher neben dem Vertrag über die Auftragsverarbeitung direkt aus dem Gesetz. So ist der Auftragsverarbeiter gem. Art. 28 Abs. 2 DS-GVO verpflichtet, vor der Beauftragung von Sub-Dienstleistern eine gesonderte Einwilligung des Verantwortlichen einzuholen oder – im Fall einer allgemeinen schriftlichen Gestattung – den Verantwortlichen zu informieren. Der Verantwortliche hat dann ein Widerspruchsrecht gegen die Einschaltung des Sub-Dienstleisters. Mit dieser Regelung in Art. 28 Abs. 2 DS-GVO könnte ein Dauerbrenner in der Verhandlung von Verträgen mit größeren Dienstleistern nun obsolet werden. Zu erwarten ist, dass diese eine allgemeine schriftliche Gestattung in ihre Verträge aufnehmen. Wie sie mit dem Widerspruchsrecht der Verantwortlichen in der Praxis umgehen werden, bleibt spannend.

Auch die Pflicht zur Mitteilung von Datenschutzverstößen durch Dienstleister ist nur direkt in Art. 28 Abs. 3 Satz 4 DS-GVO und nicht mehr nur in der Vereinbarung mit dem Verantwortlichen enthalten. Das Gleiche gilt für die Verpflichtung von Unterauftragnehmern zur Einhaltung der Datenschutzpflichten aus dem Vertrag mit dem Verantwortlichen in Art. 28 Abs. 4 DS-GVO. Die Pflicht des Dienstleisters zur Befolgung von Weisungen des Auftraggebers ist nun ebenfalls direkt gesetzlich in Art. 29 DS-GVO geregelt.

#### VI. Haftung für Datenschutzverstöße bei Auftragsverarbeitung

Die Haftung für Datenschutzverstöße nach Art. 82 DS-GVO ändert sich im Vergleich zum bisherigen Datenschutz-Schadensersatzrecht grundlegend.

Aktuell haftet gem. § 7 BDSG nur die verantwortliche Stelle gegenüber den Betroffenen für Schäden aus der Verletzung des Datenschutzrechts. Eine Haftung des Auftragsverarbeiters gegenüber den Betroffenen kommt nur in Ausnahmefällen in Betracht, nämlich insbesondere bei schweren Verletzungen des allgemeinen Persönlichkeitsrechts unter den hohen Anforderungen der deliktischen Haftung.<sup>30</sup>

Gem. Art. 82 Abs. 2 DS-GVO haftet künftig auch der Auftragsverarbeiter direkt im Verhältnis zu dem Geschädigten. Besonders brisant sind dabei zwei Aspekte. Erstens erfasst die datenschutzrechtliche Haftung künftig gem. Art. 82 Abs. 1 DS-GVO auch immaterielle Schäden. Damit könnte das bisher selten relevante Datenschutz-Schadensersatzrecht künftig ein weiteres scharfes Schwert bei der Durchsetzung des Datenschutzrechts werden. Zweitens haften Verantwortlicher und Auftragsdaten-

verarbeiter gem. Art. 82 Abs. 4 DS-GVO gesamtschuldnerisch. Der Geschädigte kann sich daher den mutmaßlich solventeren Schuldner oder das bessere Forum wählen, um seinen Anspruch auf Schadensersatz durchzusetzen.

Auch wenn der Auftragsverarbeiter nicht gegen seine auftragsverarbeiterspezifischen Pflichten gem. Art. 82 Abs. 2 DS-GVO verstoßen hat und auch nicht entgegen den Weisungen des Verantwortlichen gehandelt hat – also grundsätzlich nicht haften müsste –, ist er gegenüber dem Geschädigten zum Ersatz des Schadens verpflichtet. Diese Haftungsprivilegierung des Auftragsverarbeiters nach Art. 82 Abs. 2 DS-GVO wird damit im Zweifel nur im Innenausgleich mit dem Verantwortlichen gem. Art. 82 Abs. 5 DS-GVO relevant.

## VII. Fazit

Die DS-GVO entwickelt das Anforderungskonzept für die Einschaltung von Dienstleistern weiter, ohne es zu revolutionieren. So ergeben sich bisher nur vertraglich zu regelnde Pflichten des Auftragsverarbeiters künftig direkt aus dem Gesetz und die Systemwartung wird ein Regelfall der Auftragsverarbeitung. Die größten wirtschaftlichen Folgen könnten sich aus der gemeinsamen Verantwortlichkeit und der verschärften gesamtschuldneri-

schen Haftung von Auftragsverarbeiter und Verantwortlichem ergeben.

Eine juristische Unsicherheit birgt der vermeintliche Wegfall der Privilegierung der Auftragsverarbeitung. Die Diskussion hierüber hat eben erst begonnen. Wie gezeigt wurde, ist bei richtiger Auslegung aber von einer Erweiterung der Privilegierung gegenüber dem BDSG – nämlich auf Nicht-EWR-Verarbeiter – auszugehen. Die Auftragsverarbeitung bleibt danach auch künftig zulässig, sofern der Auftragsverarbeiter ordnungsgemäß ausgewählt und verpflichtet wird.



**Dr. Bernd Schmidt, LL.M. (Auckland),**  
ist Rechtsanwalt und Gründungspartner der Kanzlei  
PLANIT // LEGAL in Hamburg.



**Dr. Bernhard Freund, LL.M. (Wellington), M.Comp.Sc.,**  
ist Rechtsanwalt und Gründungspartner der Kanzlei  
PLANIT // LEGAL in Hamburg.