Das Bundesdatenschutzgesetz im Vergleich mit der Datenschutz-Grundverordnung

Marcel Kapfer

Zusammenfassung–Ende Mai 2018 tritt die neue EU-weite Datenschutz-Grundverordnung in Kraft. Diese soll nicht nur die noch gültige Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum Datenverkehr ablösen, sondern auch das aktuelle Bundesdatenschutzgesetz ersetzten, wobei es eine neue Fassung von diesem gibt, welche zeitgleich mit der Datenschutz-Grundverordnung in Kraft treten wird. Es stellt sich allerdings die Frage, inwiefern sich der Datenschutz durch die Gesetzesnovellen verändert. Dies wird im Folgenden anhand einiger Aspekte genauer betrachtet wird.

1 Einleitung

Die europäische Datenschutz-Grundverordnung (im Folgenden als DSGVO bezeichnet) wird am 25. 05. 2018 gültig und somit EU-weit für einen neuen Datenschutzstandard sorgen. Im Rahmen der In-Kraft-Tretung wird die noch geltende europäische Richtlinie 95/46/EG zum Schutz von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten und zum Datenverkehr abgelöst [2]. Dabei ist es auch nötig, dass das deutsche Gesetz zum Datenschutz, das Bundesdatenschutzgesetz (hier als BDSG bezeichnet, wobei damit die alte, noch gültige Version gemeint ist) überarbeitet wird. Dies ist durch das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU) geregelt.

In den Gesetzen wird generell zwischen zwei Personen unterschieden. Dem Verantwortlichen, also dem Anbieter eines Services, welcher Daten speichert, verarbeitet und/oder nutzt und dem Betroffenem, welcher personenbezogene Daten von sich (im folgenden der Einfachheit halber nur als „Daten“ bezeichnet) dem Verantwortlichem direkt oder indirekt zur Verfügung stellt oder gestellt hat. Diese Begriffe werden auch im Folgenden verwendet.

2 Unterschiede Bundesdatenschutzgesetz – Datenschutz-Grundverordnung

Aufgrund der Gesetzesänderungen stellt sich die Frage, welche Neuerungen es tatsächlich gibt und wie stark sich diese auswirken. Im Folgenden wird dabei auf einige Gesichtspunkte der Gesetzte eingegangen und diese miteinander verglichen.

Der offensichtlichste Unterschied zwischen den Gesetzen ist die Aufteilung. Das BDSG unterscheidet in weiten Teilen die Datenverarbeitung an öffentlichen Stellen und die an nicht-öffentlichen und öffentlich-rechtlichen Wettbewerbsunternehmen. In der DSGVO hingegen wird nicht nach Organen, sonder rein nach Thematik unterschieden.

2.1 Rechte der Betroffenen

2.1.1 Recht auf Auskunft

Eines der am ausführlichsten behandelten Themen in den Gesetzen sind die Rechte der Betroffenen. Darunter befindet sich vor allem das Recht des Betroffenen, seine gespeicherten Daten bei dem Verantwortlichen zu erfragen. Im BDSG ist dies in §6 festgesetzt und in §§19,34 näher ausgeführt. §19 gilt dabei für öffentliche Stellen, während §34 für nicht-öffentliche und öffentlich-rechtliche Wettbewerbsunternehmen gilt [1].

Sowohl §19, als auch §34, sichern die unentgeltliche Auskunft, allerdings wird in §34 Unternehmen erlaubt, ein Entgelt zu verrechnen, wenn der Betroffene mehr als eine Auskunft pro Kalenderjahr erfragt und die gewonnenen Daten gegenüber Dritten wirtschaftlich nutzen kann. Dieses Entgelt darf allerdings nicht die tatsächlichen Bearbeitungskosten übersteigen. Bei einer Anfrage muss der Verantwortliche dem Betroffenen folgende Daten schriftlich übermitteln: die gespeicherten Daten, sowie deren Herkunft, die Empfänger (oder Empfängerkategorien) der Daten (bei Übertragung) und der Zweck der Speicherung. Bei Anfragen soll der Betroffene näher beschreiben, welche Art von Daten er möchte. Eine öffentliche Stelle kann eine Anfrage unter Angabe der rechtlichen Vorschriften ablehnen, wobei diese darauf hinweisen muss, dass sich der Betroffene an den Bundesbeauftragten für Datenschutz und Informationsfreiheit wenden kann. Die Auskunft kann abgewiesen werden, wenn diese die Erfüllung die Aufgaben der verantwortlichen Behörde beeinträchtigen würde, die Auskunft die öffentliche Sicherheit und Ordnung gefährden könnte, dem Wohl des Landes / Bundes Nachteile bringen würde oder die Daten (oder ihre Existenz) durch ihr Wesen oder durch Recht geheim bleiben müssen. Auch können öffentliche Stellen die Anfrage ablehnen, wenn die entsprechenden Daten nicht automatisiert sind, der Betroffene keine genauen Angaben zum Auffinden der Daten macht und der nötige Aufwand nicht im Verhältnis zum Informationsinteresse des Betroffenen steht. Nicht-öffentliche Stellen und öffentliche-rechtliche

Wettbewerbsunternehmen können eine Anfrage ablehnen, wenn dadurch ein Geschäftsgeheimnis gefährdet werden könnte. Die Daten, die bei der Anfrage selbst dem Verantwortlichen übermittelt werden, dürfen von diesem nur für die Bearbeitung der Anfrage verwendet werden.

In der DSGVO wird auf das Recht auf Auskunft in den Artikeln 12, 15, 19 und 23 eingegangen. Laut Art. 15 hat der Betroffene das Recht, von einem Verantwortlichen eine Bestätigung zu verlangen, ob Daten von ihm von diesem verarbeitet werden. Falls dies der Fall ist, so muss ihm der Verantwortliche den Zweck der Verarbeitung, die Kategorie der Daten, den Empfänger (oder Empfängerkategorien), die geplante Dauer der Speicherung (falls möglich), das Recht auf Auskunft, Löschung, Einschränkung und Widerspruch gegen Verarbeitung, das Beschwerderecht bei der Aufsichtsbehörde, die Herkunft der Daten und das Bestehen einer automatischen Entscheidungsfindung nebst den Daten selbst mitteilen. Wenn Daten an internationale Organisationen oder ein Drittland (in diesem Fall ein Land außerhalb der EU) übermittelt werden, so sind dem Betroffenen auch die Garantien der verantwortlichen Stelle mit der Stelle des Empfängers mitzuteilen. In der DSGVO wird an dieser Stelle auch explizit darauf hingewiesen, dass die Daten elektronisch in einem gängigen Format herausgegeben werden sollen, wenn der Betroffene den Antrag elektronisch stellt und nichts anderes wünscht. Im Gegensatz zum BDSG findet sich hier auch die Anmerkung, dass die Herausgabe der Datenkategorien nicht die Rechte und Freiheiten anderer Personen beeinträchtigen darf. Die Herausgabe der Daten muss, wie auch im BDSG, entgeltlos erfolgen. Dabei gibt es in der DSGVO Ausnahmen, die den Verantwortlichen stärker schützen. Wenn der Betroffene unbegründete und/oder exzessive Anträge (z.B. häufige Anfragen) stellt, so kann der Verantwortliche ein Entgelt für die nötigen Verwaltungskosten verlangen oder die Auskunft verweigern. Ähnlich wie das BDSG Beschränkungen vorgibt, gibt die DSGVO Möglichkeiten für Beschränkungen in Art. 23 vor, die durch die Union oder ihre Mitgliedstaaten umgesetzt werden können. Diese sollen die Grundgesetze und Grundfreiheiten achten und eine notwendige, sowie verhältnismäßige Maßnahme darstellen. Dafür sollen die nationale und öffentliche Sicherheit, die Verhütung, Aufdeckung und Verfolgung von Straftaten, der Schutz weitere öffentlicher Interessen, der Schutz der Unabhängigkeit der Justiz, der Schutz des Betroffenen, die Rechte und Freiheiten anderer Personen und die Durchsetzung zivilrechtlicher Ansprüche berücksichtigt werden. Dabei muss in solchen Vorschriften gegebenenfalls auf folgende Aspekte eingegangen werden: die Verarbeitungszwecke, die Kategorien der Daten, der Umfang der Beschränkungen, Garantien gegen Missbrauch und unrechtmäßigen Zugang oder Übermittlungen, Angaben zum Verantwortlichen, die Speicherfristen, die Risiken für Rechte und Freiheiten und das Recht auf Unterrichtung der Betroffenen (solang dem Zweck nicht abträglich).

In Art. 12 der DSGVO werden dem Verantwortlichem auch Fristen für eine Reaktion auf Anträge auferlegt. So muss dieser innerhalb eines Monats auf eine Anfrage antworten. Falls diese komplex ist, kann der Verantwortliche die Beantwortung der Anfrage an sich um bis zu zwei Monate verschieben. Falls der Verantwortliche die Anfrage nicht antworten kann, so muss er auch dies dem Betroffenen binnen eines Monats kundtun und ihn darauf hinweisen, dass dieser die Möglichkeit hat, die zuständige Aufsichtsbehörde anzurufen.

2.1.2 Berichtigung, Löschung und Sperrung von Daten

Neben der Einsicht in die Daten sichern die Gesetze dem Betroffenen auch die Berichtigung, Sperrung und Löschung der Daten zu. Im BDSG wird dies zuerst in §6 festgeschrieben. Dort wird festgelegt, dass diese Rechte, sowie das in 2.1.1 diskutierte Recht auf Auskunft, nicht durch andere Rechtsgeschäfte einschränkbar oder ausschließbar sind. Auch Daten von diesbezüglichen Anträgen dürfen lediglich zur Erfüllung dieser selbst verwendet werden.

In §20 Abs. 1 ist die Berichtigung bei öffentlichen Stellen genauer beschrieben: falsche Daten müssen korrigiert werden, außer diese Daten sind nicht automatisiert oder der Betroffene widerspricht der Korrektur. In diesem Fall ist die Berichtigung bzw. der Widerspruch festzuhalten und die Daten sind zu sperren, also von weiteren Verarbeitungen oder Übermittlungen auszuschließen. Werden Daten berichtigt und wurden die fehlerhaften Daten anderen Stellen weitergegeben, sind diese Stellen über die Berichtigung zu benachrichtigen.

Öffentliche Stellen müssen Daten löschen, wenn die Speicherung dieser unzulässig (geworden) ist oder die Daten nicht mehr benötigt werden. Alternativ dürfen die Daten gesperrt werden, wenn die Daten vertraglich oder rechtlich aufbewahrt werden müssen oder die Löschung zu großen Aufwand verursacht.

§35 bildet die rechtliche Grundlage für nichtöffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen. Wie auch bei öffentlichen Stellen sind die Daten zu berichtigen, wenn sie falsch sind. Werden Daten geschätzt, so sind diese eindeutig zu kennzeichnen.

Auch hier müssen Daten gelöscht werden, wenn sich herausstellt, dass die Speicherung unzulässig (geworden) ist, die Daten nicht mehr benötigt werden oder falls streng-vertrauliche Daten vorliegen, deren Richtigkeit nicht bewiesen werden kann. Eine alternative Sperrung ist dann notwendig, wenn eine Löschung gegen Aufbewahrungsfristen verstößt oder wenn es Gründe gibt, dass die Löschung besondere schutzwürdige Interessen des Betroffenen beeinträchtigen würde. Auch wenn die Löschung nicht verhältnismäßig wäre (durch besondere Speicherung), können die Daten alternativ gesperrt werden. Auch müssen Daten gesperrt werden, wenn der Betroffene widerspricht, dass die Daten richtig sind und

das Gegenteil nicht bewiesen werden kann. Eine derartige Sperrung darf allerdings nicht übermittelt werden.

Wenn bei Daten die Richtigkeit angezweifelt wird, dürfen diese trotzdem unverändert übermittelt werden, wenn die Daten aus öffentlichen Quellen kommen oder Dokumentation der Zweck ist. Verlangt der Betroffene eine Gegendarstellung, so muss diese allerdings mit übermittelt werden.

In beiden Arten von Stellen gilt, dass der Betroffene einer automatisierten Erfassung und Verarbeitung widersprechen darf, falls die Interessen des Verantwortlichen der Schutzwürdigkeit (durch eine besondere Situation) des Betroffenen unterliegen.

Gesperrte Daten dürfen nur dann ohne Einwilligung des Betroffenen genutzt oder übermittelt werden, wenn diese für wissenschaftliche Zwecke gebraucht werden, für die Behebung einer Beweisnot benötigt werden oder die Gründe des Verantwortlichem oder eines Dritten unerlässlich sind. Die Voraussetzung hierfür ist allerdings, dass die Übermittlung oder Nutzung der Daten erlaubt gewesen wäre, wenn diese nicht gesperrt wären.

Die DSGVO geht im Aspekt der Datenberichtigung in Art. 16 einen Schritt weiter. Es müssen nicht nur falsche Daten berichtigt werden, sondern auch weitere Daten zu unvollständigen Datensätzen (im Hinblick auf den Verarbeitungszweck) hinzugefügt werden.

Laut Art. 17 („Recht auf Vergessenwerden“) kann der Betroffene eine Antrag an den Verantwortlichen stellen, seine Daten zu Löschen. Der Verantwortliche wiederum hat die Pflicht die Daten unter ebendiesen Gründen zu Löschen. Genauso wie im BDSG müssen die Daten gelöscht werden, wenn diese nicht mehr benötigt werden oder unrechtmäßig verarbeitet werden. Die Daten sind auch zu Löschen, wenn der Betroffene seine Einwilligung widerruft oder der Verarbeitung, aus besonderen Gründen oder weil diese für Direktwerbung genutzt werden, widerspricht. Vor allem der letzte Aspekt ist im BDSG nicht enthalten. Wenn die Daten vom Verantwortlichen veröffentlicht wurden, muss er alle Empfänger auch über die Löschung informieren, soweit dies technisch machbar ist. Der Verantwortliche kann sich einer Löschung widersetzen, wenn die Daten für freie Meinungsäußerung und Informationen verwendet werden, die Daten für rechtliche Verpflichtungen benötigt werden, für die öffentliche Gesundheit wichtig sind oder für öffentliche Archive, wissenschaftliche und historische Forschung oder Statistik unverzichtbar sind. Die Daten dürfen auch dann nicht gelöscht werden, wenn sie noch für Rechtsansprüche benötigt werden.

Bei Berichtigungen oder Löschung von Daten muss der Verantwortliche laut Art. 19 alle Empfänger (falls dies möglich und verhältnismäßig ist) darüber benachrichtigen. Dem Betroffenem muss dieser eine Liste dieser Empfänger geben, wenn dieser das wünscht.

Der Betroffene darf laut Art. 18 die Daten für die Dauer einer Überprüfung sperren lassen, wenn die Korrektheit dieser von ihm angezweifelt wird oder er Widerspruch gegen die Datenverarbeitung eingelegt hat. Weitere Gründe für eine Einschränkung der Daten sind zum einen, dass zwar die Verarbeitung unrechtmäßig ist, allerdings der Betroffene eine Löschung ablehnt, und zum anderen, dass die Daten unnötig sind, allerdings der Betroffene diese unter Umständen für Rechtsansprüche benötigt. Eingeschränkte Daten dürfen nur nach Einwilligung des Betroffenen verarbeitet werden oder falls sie für Rechtsansprüche benötigt werden. Wenn die Sperrung aufgehoben werden soll, ist der Betroffene davon zu benachrichtigen.

Der Betroffene kann, aus besonderen Gründen oder da die Daten für Direktwerbung verwendet werden, einer Datenverarbeitung widersprechen. Dies wird in Art. 21 geregelt. Der Verantwortliche kann die Daten weiterverarbeiten, falls dieser schutzwürdige Gründe nachweisen kann oder die Daten für Rechtsansprüche benötigt werden. Es wird hier explizit erlaubt, dass der Widerspruch bei digitalen Diensten auch durch ein automatisiertes Verfahren eingereicht werden kann. Der Betroffene kann auch ausdrücklich gegen eine Datenverarbeitung für wissenschaftliche, historische oder statistische Zwecke widersprechen, außer ebendiese Datenverarbeitung ist unerlässlich für die Erfüllung von Aufgaben im öffentlichen Interesse.

2.1.3 Benachrichtigung des Betroffenen

Neben der Recht auf Auskunft (2.1.1) des Betroffenen hat der Verantwortliche auch die Pflicht den Betroffenen eigenständig über gewisse Vorkommnisse zu Benachrichtigen.

Für öffentliche Stellen gilt in diesem Fall §19a. Hier wird festgeschrieben, dass der Betroffene zu benachrichtigen ist, wenn Daten über ihn ohne dessen Kenntnis erworben wurden, wobei hier auch der Grund des Datenerwerbs mit aufzuführen ist. Werden Daten an weitere Stellen übermittelt und konnte das der Betroffene nicht wissen, so ist er auch darüber zu informieren, wer der Empfänger (oder die Empfängerkategorie) ist. Der Betroffene muss nicht benachrichtigt werden, wenn er über andere Wege über die Speicherung oder Übermittlung erfahren hat, wenn der Aufwand für die Benachrichtigung unverhältnismäßig ist oder wenn die Speicherung oder Übertragung rechtlich vorgesehen ist.

Bei nicht-öffentlichen Stellen und öffentlich-rechtlichen Wettbewerbsunternehmen gilt für die Benachrichtigung §33. Bei einer erstmaligen Speicherung ist der Betroffene zu benachrichtigen, wobei darin der Zweck der Speicherung, die Art der Daten und die Identität des Verantwortlichen mitgeteilt werden müssen. Folgt die Speicherung zur Übermittlung der Daten, so ist der Betroffene vor der ersten Übermittlung über die Kategorie der Empfänger zu benachrichtigen. Die Benachrichtigung entfällt, wenn der Betroffene aus einer anderen Quelle Kenntnis erlangt hat, Gesetze, Satzungen oder Verträge dies erlauben, die Daten durch Gesetze oder ihr Wesen geheim gehalten werden müssen oder eine öffentliche Stelle feststellt, dass das Bekanntwerden der Daten

das Allgemeinwohl schädigen könnte. Wenn die Daten aus öffentlichen Quellen kommen und eine Benachrichtigung unverhältnismäßig wäre, darf diese ebenfalls entfallen. Der Verantwortliche muss dabei schriftlich festlegen, wann die Benachrichtigung entfällt.

In der DSGVO wird die Benachrichtigung des Betroffenen durch Art. 13 und 14 geregelt. Wenn eine Erhebung von Daten stattfindet, so muss der Verantwortliche dem Betroffenen seinen Namen sowie seine Kontaktdaten und gegebenenfalls auch die Kontaktdaten des Datenschutzbeauftragten, den Zweck und die Rechtsgrundlage, gegebenenfalls die Empfänger, gegebenenfalls die Absicht die Daten an Drittländer und/oder internationale Organisationen zu übermitteln, falls möglich auch die Dauer der Speicherung und eventuell das Bestehen einer automatischen Entscheidungsfindung mitteilen. Zusätzlich muss der Betroffene auch auf sein Recht auf Auskunft, Berichtigung, Löschung und Sperrung sowie auf sein Widerspruchsrecht hingewiesen werden. Auch ist es notwendig zu erläutern, ob die Datenerhebung gesetzlich oder vertraglich vorgeschrieben ist oder für einen Vertragsabschluss benötigt wird und ob der Betroffene verpflichtet ist, die Daten bereitzustellen und was passiert, wenn dieser sich dagegen weigert. Wenn der Verantwortlich den Zweck der Daten ändert, muss der Betroffene ebenfalls darauf hingewiesen werden. Die Pflichten hat auch ein Verantwortlicher, welcher die Daten indirekt und nicht direkt von dem Betroffenen erhalten hat. Die Benachrichtigung muss dann binnen eines Monats erfolgen oder, wenn die Daten zur Kommunikation mit dem Betroffenen verwendet werden, mit der ersten Mitteilung.

Die Benachrichtigungspflicht entfällt, genauso wie im BDSG, wenn der Betroffene darüber bereits Kenntnis erlangt hat. Weitere Gründe, den Betroffenen nicht zu informieren, sind unverhältnismäßig hoher Aufwand zur Benachrichtigung, eine Erlangung der Daten per Gesetz oder die Geheimhaltung per Gesetz.

2.2 Datenspeicherung, -veränderung und -nutzung

Ein weiteres großes Thema in den Gesetzestexten ist die Nutzung, Speicherung, Veränderung und Erhebung von Daten. Im BDSG werden die Grundlagen der Datenerhebung, -verarbeitung und -nutzung in §4 festgelegt. Wie schon in 2.1 erwähnt findet sich auch hier die Aufteilung zwischen öffentlichen Stellen (§14) und nicht-öffentlichen und öffentlich-rechtlichen Wettbewerbsunternehmen (§§28-28b und §§30a-32). In §§39-41 werden darüber hinaus noch einige Sondervorschriften festgelegt. In der DSGVO wird auf diese Thematik vor allem in den Artikeln 5 und 6 sowie 9 und 11 eingegangen. Darüber hinaus werden in den Artikeln 18 und 32 weitere Aspekte geregelt.

2.2.1 Grundlegende Regelungen

Allgemein gilt im BDSG laut §4, dass Daten nur mit einer Einwilligung des Betroffenen oder mit einer rechtlichen Grundlage verarbeitet, erhoben oder genutzt werden dürfen. Dabei sind die Daten in der Regel beim Betroffenen selbst zu erheben. Ausnahmen für dies sind Rechtsvorschriften oder wenn eine Erhebung der Daten bei oder durch Dritte durch den Zweck der Datenverarbeitung erforderlich ist. Es lässt sich auch von dieser Verpflichtung absehen, wenn der Aufwand einer direkten Erhebung unverhältnismäßig groß ist. Bei einer Erhebung ist der Betroffene darüber zu informieren, welche Stelle die Daten erhebt und zu welchen Zwecken. Möchte die Stelle die Daten an Dritte weitergeben, so ist der Betroffene auch über die Kategorie dieser Empfänger zu informieren. Diese Informationspflicht gilt allerdings nicht, wenn der Betroffene schon auf eine andere Art und Weise darüber erfahren hat. Des weiteren muss der Verantwortliche den Betroffenen darauf hinweisen, ob die Datenerhebung auf freiwilliger Basis (für den Betroffenen) stattfindet, oder ob diese durch eine Rechtsvorschrift festgelegt ist. Wenn der Betroffene es wünscht oder es auf sonst eine Art und Weise erforderlich ist, so ist er auch darüber mitzuteilen, was die Folgen einer Verweigerung sind.

Für öffentliche Stellen gilt laut §14, dass die Speicherung, Nutzung und Veränderung von Daten nur zulässig ist, wenn dies für die Erfüllung der Aufgabe der Behörden erforderlich ist und die Daten auch für diesen Zweck erhoben wurden. Darüber hinaus dürfen die Daten auch verwendet werden, wenn dies durch eine Rechtsvorschrift gestattet ist, zur Verfolgung und Vollstreckung von Straftaten und auch zum Schutz des Allgemeinwohls oder zur Abwehr einer Beeinträchtigung einer anderen Person. Auch kann der Zweck erweitert werden, wenn der Betroffene diesem explizit zustimmt, es im Interesse des Betroffenen liegt oder Angaben des Betroffenen überprüft werden müssen. Weiterhin gilt die Einschränkung auch nicht, wenn die Daten öffentlich zugänglich sind oder die Behörde diese öffentlich zugänglich machen dürfte und ebenso nicht, wenn die Daten für wissenschaftliche Forschung erforderlich sind.

Die Auflagen die für nicht-öffentliche Stellen und öffentlich-rechtliche Wettbewerbsunternehmen gelten, sind hier deutlich umfassender. §28 ist dabei das Analogon zu §14, in den folgenden Paragraphen werden dann noch weitere Fälle festgelegt. Die Datenerhebung, -speicherung, -veränderung und -übermittlung ist für Geschäftszwecke zulässig, sowie für berechtigte Interessen des Verantwortlichen. Ähnlich zu §14 ist das Verwenden von öffentlichen Daten oder Daten, die die verantwortliche Stelle öffentlich machen dürfte, genehmigt. Bei der Erhebung von Daten müssen die Zwecke der Verarbeitung festgelegt werden. Die Erweiterung des Zwecks ist für die gerade genannten Gründe erlaubt und ebenso, falls die Daten für die Wahrung der öffentlichen Sicherheit, zur Verfolgung von Straftaten oder für wissenschaftliche Zwecke erforderlich sind. Die Verarbeitung der Daten für einen Adresshandel oder zu Werbezwecken ist nur zulässig, falls der Betroffenen diesem

zugestimmt hat oder wenn es sich bei den verwendeten Daten um eine listenartige Aufstellung handelt. In einer solchen Liste darf über den Betroffenen nur Name, Titel, akademischer Grad, Anschrift und Geburtsjahr enthalten sein. Dabei darf die damit verbreitete Werbung nur für eigene Produkte, im Hinblick auf den Beruf des Betroffenen und für steuerbegünstigte Spenden sein. Die Daten dürfen zwar für Werbezwecke an Dritte weitergegeben werden, allerdings muss die Quelle der Daten in der Werbung sichtbar sein. Daten, die für Werbezwecke übermittelt werden, dürfen vom Empfänger ausschließlich für diese Zwecke verwendet werden. Der Betroffene kann der Verwendung von Daten für Werbezwecke und für die Verwendung dieser für Markt- und Meinungsforschung widersprechen. Auf dieses Widerspruchsrecht ist er Betroffene vom Verantwortlichem hinzuweisen. Ein Dritter darf die übermittelten Daten nur die Zwecke nutzen, für die sie übermittelt wurden. Hierbei gelten dieselben Ausnahmen wie für die ursprüngliche Stelle.

In der DSGVO werden die grundlegenden Regelungen in Artikeln 5 und 6 sowie 9 bis 10 festgelegt. In Art. 5 wird zuerst vorgeschrieben, dass Daten auf rechtmäßige und nachvollziehbare Weise, aber auch nach „Treu und Glauben“ verarbeitet werden müssen. Des weiteren müssen die Daten für eindeutige Zwecke erhoben werden und dürfen auch nur für diese verwendet werden. Archivzwecke im öffentlichen Interesse, wissenschaftliche und historische Forschung sowie statistische Zwecke sind von der Zweckbindung befreit. Auch hat die Verarbeitung der Daten auf das notwendige Maß beschränkt zu sein und mit einer angemessenen Sicherheit zu geschehen. Die gespeicherten Daten müssen sachlich richtig sowie aktuell sein (soweit dies nötig ist) und möglichst anonymisiert werden, sobald eine Identifizierung des Betroffenen mit den Daten nicht mehr erforderlich ist, wobei auch hier die selben Ausnahmen gelten, wie bei der Zweckbindung. Abschließend ist auch der Verantwortliche für die Erfüllung dieser Bedingungen verantwortlich und auch diesbezüglich rechenschaftspflichtig. Diese Grundsätze werden in Art. 5 durch die Begriffe „Rechtmäßigkeit“ „Verarbeitung nach Treu und Glaube“, „Transparenz“, „Zweckbindung“, „Datenminimierung“, „Richtigkeit“, „Speicherbegrenzung“, „Integrität und Vertraulichkeit“ und „Rechenschaftspflicht“ zusammengefasst.

Art. 6 geht auf die Rechtmäßigkeit von Verarbeitungen ein. Diese ist erfüllt, wenn der Betroffene eingewilligt hat, die Verarbeitung für die Erfüllung eines Vertrags oder aus rechtlichen Gründen erforderlich ist, zum Schutz lebenswichtiger Interessen einer natürlichen Person oder wenn die Verarbeitung für berechtigte Interessen des Verantwortlichen, der Öffentlichkeit oder eines Dritten erforderlich ist. Folgt die Verarbeitung einem anderem als dem ursprünglichem Zweck (aufgrund einer Einwilligung oder eines Gesetzes), so hat der Verantwortliche zu berücksichtigen, ob der andere Zweck mit dem ursprünglichen vereinbar ist. Dabei hat er vor allem die Verbindung zwischen dem Zweck durch Einwilligung oder Rechtsvorschrift, den Zusammenhang der Datenerhebung mit dem geplanten Zweck, die Art von Daten und die möglichen Folgen zu betrachten.

2.2.2 Daten besonderer Art

Besondere Regelungen gelten für die sogenannten persönlichen Daten besonderer Art. Dazu zählen laut §3 Abs. 9 BDSG Daten über die rassische und ethische Herkunft, politische Meinungen, religiöse und philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben. Wenn der Betroffene keine Einwilligung laut §4a gegeben hat, kann die verantwortliche Stelle trotzdem solche Daten erheben, verarbeiten und nutzen, wenn der Betroffene die Daten öffentlich gemacht hat oder dies zum Schutz von lebenswichtigen Interessen einer natürlichen Person erforderlich ist und der Betroffenen außerstande ist, seine Einwilligung zu geben. Auch wenn die Daten für rechtliche Ansprüche notwendig sind und keine schutzwürdigen Interessen des Betroffenen annehmbar sind oder wenn die Daten für wissenschaftliche Zwecke unabdingbar sind, so dürfen diese erhoben und genutzt werden. Weitergehend ist das Erheben solcher Daten durch ärztliches Personal oder Personal mit einer entsprechenden Geheimhaltungspflicht ebenso erlaubt, wenn die Daten für medizinische oder gesundheitliche Zwecke benötigt werden. Ähnlich gibt es auch für politische, philosophische, religiöse und gewerkschaftliche Organisationen Ausnahmen. Solche Organisationen dürfen Daten besonderer Art von ihren Mitgliedern und von Personen die in regelmäßigem Kontakt zu der Organisationen stehen, erheben, verarbeiten und nutzen, wenn dies für die Tätigkeit dieser von Nöten ist.

In der DSGVO geht Art. 9 auf die Verarbeitung von Daten besonderer Art ein. Laut DSGVO zählen nicht nur Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Einstellungen, eine eventuelle Gewerkschaftszugehörigkeit und Daten zum Sexualleben, sondern auch biometrische Daten, Gesundheitsdaten oder Angaben zur sexuellen Orientierung dazu. Die Verarbeitung solcher Daten ist dabei grundsätzlich untersagt und nur für die folgenden Fälle genehmigt. Die Daten dürfen verarbeitet werden, wenn der Betroffene zugesagt oder die Daten selbst veröffentlicht hat, wenn dies zum Schutz von lebenswichtigen Interessen einer natürlichen Person unerlässlich ist oder wenn die Daten für Rechtsansprüche erforderlich sind. Unter Berücksichtigung des Berufsgeheimnisses ist die Verarbeitung dieser Daten auch im Gesundheits- und Medizinbereich gestattet.

2.2.3 Sicherheit der Datenverarbeitung

Im §9 BDSG werden die verantwortlichen Stellen zu technischen und organisatorischen Maßnahmen aufgefordert. Die geforderten Maßnahmen sind vor allem, dass die gesetzlichen Vorschriften eingehalten werden. Darüber hinaus werden in der Anlage zu §9 weitere Maßnahmen definiert, die eingehalten werden sol-

len, wenn dies angemessen bezüglich des Schutzes ist. Laut dieser Anlage soll die verantwortliche Stelle gewährleisten, dass nur berechtigte Personen, auf die Daten Zugriff haben sowie diese Verarbeiten, Eingeben, Löschen oder Ändern können. Weitergehend ist auch dafür zu sorgen, dass nachträglich überprüft werden kann, wer welche Daten auf welche Art und Weise hinzugefügt, verändert oder entfernt hat. Auch soll dafür gesorgt werden, dass die Daten gegen Verlust geschützt sind. Abschließend soll die verantwortliche Stelle auch dafür sorgen, dass Daten für verschiedene Zwecke getrennt verarbeitet werden können.

In der DSGVO wird dazu in Art. 25 näher eingegangen. Der Verantwortlich hat, soweit dies verhältnismäßig ist, die Datenschutzgrundsätze sowohl bei der Festlegung der Daten, als auch bei der Verarbeitung dieser selbst, weit möglichst zu erfüllen. Die Datenschutzgrundsätze sind die in Art. 5 festgelegten (hier auch in 2.2.1 „Grundlegende Regelungen“ zusammengefasst), wobei die Datenminimierung in Art. 25 explizit genannt wird. In Absatz 2 dieses Artikels wird der Verantwortliche dazu verpflichtet, dass durch Voreinstellungen nur die Daten verarbeitet werden, die für den Zweck notwendig sind. Dies gilt für die Menge, Speicherfrist und Zugänglichkeit der Daten sowie den Umfang der Verarbeitungen. Des weiteren muss dafür gesorgt werden, dass nur durch explizites Erlauben des Betroffenen, eine unbestimmte Zahl an Dritten die Daten einsehen können. In Art. 32 werden weitere Grundlagen zur Sicherheit der Datenverarbeitung festgelegt. So sollen Daten im Hinblick auf die Umstände und den Verarbeitungszweck pseudonymisiert und verschlüsselt werden. Auch soll ein Augenmerk darauf gelegt werden, dass die Vertraulichkeit, Integrität und Belastbarkeit über Dauer hinweg vorhanden ist und die Verfügbarkeit bei einem Zwischenfall zügig wiederhergestellt wird. Auch soll der Verantwortliche ein Verfahren zur Überprüfung und Bewertung der Sicherheit in Betracht ziehen.

2.2.4 Automatisierte Entscheidungen im Einzelfall

In §6a BDSG werden automatisierte Entscheidungen, welche rechtliche Konsequenzen für den Betroffenen haben können oder ihn auf eine andere Weise stark beeinträchtigen könnten, untersagt. Davon kann abgesehen werden, wenn dieses Verfahren zu Gunsten des Betroffenen entscheidet oder wenn die Interessen des Betroffenen gewahrt werden und die Stelle den Betroffenen über diese automatisierte Entscheidung informiert. Auf Verlangen des Betroffenen hat die verantwortliche Stelle ihm die Entscheidung zu begründen.

In der DSGVO wird auf automatisierte Einzelfallentscheidungen in Art. 22 eingegangen. Diese verbietet, genauso wie das BDSG, diese Art der Entscheidungsfindung, wenn der Betroffene unter rechtlichen Konsequenzen leiden könnten oder dadurch stark beeinträchtigt werden könnte. Dieses Verbot gilt nicht, wenn eine solche Entscheidung für einen Vertrag notwendig ist oder der Betroffene einer solchen Entscheidung ausdrücklich zugestimmt hat. Der Verantwortliche hat dafür zu sorgen, dass der Betroffene die Entscheidung anfechten kann, seine eigene Position darlegen kann und fordern kann, das eine Person der verantwortlichen Stelle die Entscheidung überprüft. Des weiteren darf eine solche Entscheidung auch keine Daten besonderer Art verwenden, es sei denn der Betroffene stimmt dem zu oder eine Verarbeitung ist für die Öffentlichkeit unabdingbar.

FAZIT

Abschließend betrachtet lässt sich sagen, dass die DSGVO verständlicher ist und nicht so viel juristische Ausdrucksweisen verwendet, wie das BDSG. Des weiteren ist die Aufteilung der DSGVO besser strukturiert, als das BDSG, vor allem durch die Trennung in öffentlichen Stellen sowie nicht-öffentlichen und öffentliche-rechtliche Wettbewerbsunternehmen werden die einzelnen Unterabschnitte größtenteils doppelt betrachtet, wobei sich auch etliche Redundanzen ergeben. Dabei muss man allerdings auch beachten, dass die DSGVO häufig den Mitgliedsländern der Europäischen Union die Möglichkeit (und teilweise auch die Pflicht) gibt, weitere Ausnahmen oder Regelungen zu definieren, was durch nicht falsch ist. Schließlich wäre es ohne solche Ausgestaltungen auf nationaler Ebene den Mitgliedsländern nicht möglich, die Grundverordnung an die nationalen Gesetze (wie z.B. die Grund- oder Strafgesetze) anzupassen. Inwiefern die DSGVO durch die einzelnen Staaten erweitert werden darf, wird im DSGVO an den Stellen, wo diese Möglichkeit gegeben wird, genauer erläutert (siehe z.B. Art. 9 Absatz 2 Buchstabe g).

Durch einige Artikel der DSGVO wird auch ersichtlich, dass diese deutlich jünger ist als das BDSG und mehr auf die digitalisierte Welt ausgerichtet ist. Dies geht unter anderem sehr deutlich aus Art. 20 „Recht auf Datenübertragbarkeit“ hervor. Generell bietet die DSGVO dem Betroffenen, aber auch dem Verantwortlichem, mehr Schutz. Besonders hervorzuheben ist dabei Art. 8 Absatz 1, in welchem die Eltern der Verarbeitung von Daten ihres Kindes zustimmen müssen, wenn dieses das 16. Lebensjahr noch nicht vollendet hat.

LITERATUR

[1] Bundesrepublik Deutschland. Bundesdatenschutzgesetz - dejure.org. dejure.org Rechtsinformationssysteme GmbH. Abgerufen: 17. 12. 2017. [Online]. Available: https://dejure.org/gesetze/BDSG

[2] Europäische Union. Datenschutz-Grundverordnung - dejure.org. dejure.org Rechtsinformationssysteme GmbH. Abgerufen: 17. 12. 2017. [Online]. Available: https://dejure.org/gesetze/DSGVO