

von Rechtsanwalt **Phil Salewski**

# Ab 2018: Änderungen für den Online-Handel durch neue EU-Datenschutzgrundverordnung

Nach jahrelangen Diskursen und Verhandlungen ist am 04. Mai 2016 die komplexe europäische Datenschutz-Grundverordnung (DSGVO) im Amtsblatt der Europäischen Union verkündet worden, die Prognosen zufolge das in Deutschland geltende Datenschutzrecht weitgehend auf den Kopf stellen sollte. Tatsächlich bringt das seitenreiche Regelwerk vor allem im Bereich der Verantwortlichenpflichten und Betroffenenrechte wesentliche Neuerungen mit sich, greift auf der anderen Seite aber auch auf bekannte und altbewährte Datenschutzgrundsätze zurück. Die Änderungen und Vorgaben, denen sich insbesondere der Online-Handel künftig gegenübersehen wird und die zwingend eine Berücksichtigung werden erfahren müssen, sollen nachfolgend in einem ersten Überblick mit Bezügen auf das geltende Recht dargestellt werden.

## A. Überblick über Gegenstand und Anwendungsbereich der DSGVO

### I. Anwendung, Zweck und Systematik der EU-Datenschutzgrundverordnung

Unter der Zielsetzung, einerseits den Auswirkungen der rapiden technologischen Entwicklung sowie der Globalisierung auf das Ausmaß der Erhebung und des Austauschs personenbezogener Daten Rechnung zu tragen und andererseits die teilweise stark divergierenden datenschutzrechtlichen Vorgaben der einzelnen Mitgliedsstaaten auf ein homogenes und angemessen hohes Niveau zu heben, ist nach einem ungewöhnlich langwierigen Gesetzgebungsverfahren am 04. Mai 2016 die [„Europäischen Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr“](#) (kurz: [EU-Datenschutzgrundverordnung/DSGVO](#)) im offiziellen Amtsblatt der Europäischen Union verkündet worden.

Nachdem über Jahre hinweg versucht wurde, einen verhältnismäßigen Ausgleich zwischen den eingebrachten Belangen von Datenschutzexperten, Wirtschaftsvertretern, Technologiespezialisten und Beauftragten der einzelnen Mitgliedsstaaten herzustellen, entstand ein selbst für europäische Verhältnisse außerordentlich komplexer Rechtsakt, der mit 173 Erwägungsgründen und 99 Artikeln einen effektiven Rahmen für den angemessenen Schutz personenbezogener Daten einerseits und die möglichst belastungs- und auflagenmoderate Datennutzung und -verarbeitung durch erhebende Stellen andererseits bilden sollte.

Obwohl die EU-Datenschutzgrundverordnung bereits durch die amtliche Verkündung in Kraft trat, gilt sie **unmittelbar erst ab dem dem 25. Mai 2018** und ist hinsichtlich ihrer Regelungen somit erst ab

diesem Zeitpunkt verbindlich. Online-Händlern bleibt insofern eine zweijährige Übergangsfrist, die zwar lang bemessen erscheint, allerdings in Anbetracht der vorzunehmenden informationstechnologischen, vertraglichen und informatorischen Umgestaltungen zur Einhaltung der neuen Vorgaben in vielen Fällen auch notwendig sein dürfte.

Das durch die Verordnung angestrebte einheitlich hohe Schutzniveau in Prozessen der Datenerhebung, -speicherung, -verarbeitung und -übertragung im Einklang mit den Interessen der Verantwortlichen an einer rechtssicheren, rechtmäßigen und weitgehend ungehinderten Nutzung personenbezogener Daten spiegelt sich maßgeblich in der Systematik der Verordnung wieder.

In einem ersten Kapitel werden in den Artikeln 1-4 Anwendungsbereich und Begrifflichkeiten eingegrenzt und erläutert, woraufhin in Kapitel 2 die wesentlichen zu berücksichtigenden datenschutzrechtlichen Grundsätze ebenso postuliert werden wie die Zulässigkeitsvoraussetzungen einer jeglichen Datenverarbeitung. Anders als im derzeit geltenden Bundesdatenschutzgesetz (BDSG), in welchem die einzelnen Erlaubnistatbestände über den Vorschriftenkatalog verstreut sind, werden in der EU-Grundverordnung die verschiedenen Rechtmäßigkeitsvoraussetzungen gesammelt angeführt.

Besondere Berücksichtigung finden hierbei auch die Belange Minderjähriger und die Schutzwürdigkeit sog. sensibler persönlicher Daten wie z.B. die ethnische Herkunft, die religiöse oder weltanschauliche Auffassung und die sexuelle Orientierung.

In einem dritten Kapitel formuliert der europäische Gesetzgeber zunächst allgemeine Transparenzgrundsätze (Art. 12) und geht sodann auf spezifische informatorische Pflichten der Verantwortlichen ein (Art. 13 und 14), denen Rechte der von der Datenverarbeitung betroffenen gegenübergestellt werden (Art. 15 – 22). Auffällig ist, dass zum Zwecke des angestrebten Interessenausgleichs für jede Berechtigung bestimmte Ausnahmekonstellationen angeführt werden, in denen die Betroffenenrechte eingeschränkt oder ausgeschlossen werden können.

In Kapitel 4 legt der Ordnungsgeber sodann die allgemeinen Verantwortlichkeiten der Datenerheber fest und stellt spezifische Anforderungen und Grundsätze für die Konstellationen der gemeinsamen Verantwortlichkeit (Art. 26), der Verantwortlichenvertretung bei Sitz des Verantwortlichen im EU-Ausland (Art. 27) und der Auftragsdatenverarbeitung auf (Art. 28).

Daneben werden bestimmte Dokumentations- und Meldepflichten der Verantwortlichen formuliert (Art. 30, 33, 35) und die Stellung und Pflichten zur Benennung von Datenschutzbeauftragten konkretisiert (Art. 37ff.)

Ein fünftes Kapitel regelt die Grundsätze und rechtlichen Anforderungen der Übermittlung von personenbezogenen Daten an Drittländer und internationale Organisationen (Art. 44 – 50), während in Kapitel 6 und 7 die Stellung und die Funktionsweise sowie die Leitlinien einer Zusammenarbeit der einzurichtenden datenschutzrechtlichen Aufsichtsbehörden niedergeschrieben sind (Art. 51 – 76).

Das achte Kapitel thematisiert die gerichtlichen und außergerichtlichen Rechtsbehelfe und Mittel der Betroffenen bei Verstößen gegen die Datenschutzvorgaben der Verordnung und stellt scharfe Haftungsmaßstäbe (Art. 82) und Sanktionen (Art. 83 und 84) für Verantwortliche auf.

In den drei letzten Kapiteln ergehen schließlich Vorschriften für besondere Verarbeitungssituationen (Informationsfreiheit, Arbeitsverhältnisse, Forschung etc.) und Schlussbestimmungen.

## II. Verhältnis zum BDSG und den §§11 ff. TMG

Bei dem neuen europäischen Datenschutzrechtsakt handelt es sich aufgrund seiner rechtlichen Ausgestaltung als Verordnung um ein in den Mitgliedsstaaten unmittelbar anwendbares Sekundärrecht, das insofern – anders als europäische Richtlinien – keiner nationalen Umsetzung mehr bedarf.

Weil europäische Rechtsbestimmungen in den Mitgliedsstaaten in Anbetracht gleichrangiger nationaler Regelungen grundsätzlich Anwendungsvorrang haben, stellt sich die praktisch bedeutsame Frage, in welchem Verhältnis die neuen europäischen Vorgaben nach Ablauf der Übergangsfrist zu den geltenden deutschen datenschutzrechtlichen Bestimmungen nach §§11 ff. TMG und dem BDSG stehen werden.

### 1.) Auswirkungen auf das geltende BDSG

Bisher regelt das deutsche Bundesdatenschutzgesetz (BDSG) die Rechte und Pflichten der Verantwortlichen bei sowie die Zulässigkeit der Erhebung, Verarbeitung, Nutzung und Speicherung personenbezogener Daten weitgehend abschließend. In bestimmten Bereichen drohen ab dem Zeitpunkt der Anwendbarkeit der neuen Datenschutzgrundverordnung im Jahr 2018 allerdings Rechtskollisionen, die auf gegenläufige oder in ihrem Umfang divergierende Vorgaben und Einschränkungen fußen.

**Zu beachten ist allerdings, dass wesentliche Teile des geltenden BDSG auf einer Umsetzung der europäischen Datenschutzrichtlinie RL 95/46/EG beruhen, welche nach eindeutiger Titelbezeichnung und in Anlehnung an den Erwägungsgrund 171 durch die Grundverordnung aufgehoben werden sollen.**

Insofern ist anzunehmen, dass maßgebliche Abschnitte des BDSG durch die Rechtswirkungen des neuen europäischen Rechtsaktes verdrängt werden und so ihren Geltungsanspruch zugunsten der reformierten Bestimmungen aufgeben müssen. Mithin ist auf dem Gebiet des BDSG in Zukunft grundsätzlich von einer vorrangigen Geltung der neuen Grundverordnung auszugehen, welcher der deutsche Gesetzgeber durch klarstellende Gesetzesänderungen auf dem Gebiet des Datenschutzrechts zukünftig Ausdruck verleihen sollte.

Problematisch und derzeit zu Lasten der Rechtssicherheit noch nicht annähernd eruiert ist allerdings die Frage, inwieweit die Verdrängungswirkung im deutschen Recht tatsächlich Einzug halten wird. Insofern stellen zwar viele Sektionen des BDSG eine Umsetzung von nunmehr aufgehobenen europäischen Richtlinienbestimmungen dar. Allerdings existieren im Regelwerk des BDSG auch Vorgaben, die autonomen nationalgesetzlichen Entscheidungen entspringen und dem Regelungsbereich von Richtlinien bisher nicht zugänglich waren.

Diese Doppelseitigkeit des deutschen Datenschutzrechts und die damit einhergehenden Anwendungsfragen werden durch die neue Grundverordnung noch weiter ausgedehnt.

Der neue Rechtsakt gibt – wie der Name schon impliziert – nämlich nur den gesetzlichen Rahmen für ein harmonisiertes Datenschutzrecht vor, überlässt in vielen Regelungspunkten die Ausrüstung und das gesetzliche „Finetuning“ aber der jeweiligen mitgliedstaatlichen Legislative (z.B. bzgl. des Mindestalters für einwilligungsfähige Minderjährige, Art. 8, oder der Ausgestaltung der Zulässigkeit des „Profiling“, Art. 20.)

Durch die Freigabe nationalgesetzlicher Konkretisierungen wird nicht nur der eigentliche Verordnungszweck der verbindlichen europarechtlichen Harmonisierung des Datenschutzniveaus teilweise unmittelbar konterkariert, sondern zudem ein weitreichender Gesetzgebungsaufwand für die Mitgliedsstaaten begründet, die trotz der direkten Geltung der neuen DSGVO weitere spezialgesetzliche Bestimmungen erlassen müssen.

Derzeit vermag man noch nicht zu sagen, ob autonome nationale Paragraphen des BDSG bereits zulässige Konkretisierungen enthalten oder ob mit Rücksicht auf die Delegation durch die Grundverordnung in Zukunft weitere Änderungen des BDSG bevorstehen.

Sicher ist jedoch bereits, dass das Zusammenspiel von (nicht aufgehobenen) Vorgaben des BDSG und den Bestimmungen der EU-Grundverordnung die Rechtsanwendung zukünftig vor erhebliche Schwierigkeiten stellen dürfte.

## 2.) Auswirkungen auf die §§11 ff. TMG

Die §§11 ff. des Telemediengesetzes statuieren in Deutschland besondere datenschutzrechtliche Grundsätze für Anbieter von Telemedien und sind ob ihrer differenzierten Informations-, Verarbeitungs-, und Schutzpflichten für den Umgang und die Prozessierung personenbezogener Daten vor allem im Online-Bereich spezialgesetzliche Ausprägungen des allgemeinen Datenschutzrechts nach dem BDSG.

In ihrer derzeitigen Fassung liegen die maßgeblichen Bestimmungen einer ausschließlichen Entscheidung des deutschen Gesetzgebers zugrunde und basieren nicht auf europäischem Recht, sodass vieles dafür spricht, dass die Regelungen der DSGVO die §§11 ff. TMG überschreiben werden.

Dies gilt nicht nur hinsichtlich der in §13 TMG vorgesehenen Informationspflichten (meist als Datenschutzerklärung bezeichnet), welche in den Art. 12-14 DSGVO weitreichendere Ausprägungen erfahren, sondern auch bezüglich der allgemeinen Handhabung personenbezogener Daten durch Telediensteanbieter. Festzustellen ist nämlich, dass die DSGVO hinsichtlich der informationstechnologischen Eigenschaften der Verantwortlichen gerade nicht differenziert und somit sämtliche Datenverarbeitungsvorgänge unabhängig von ihrem Wirkungsbereich einheitlichen Zulässigkeitsvoraussetzungen unterwirft.

Für eine Differenzierung zwischen Diensteanbietern einerseits und sonstigen Stellen andererseits dürfte nach Ablauf der Übergangsfrist demgemäß kein Raum mehr bestehen. Gleiches gilt für die Klassifizierung und die dadurch begründete Problematik der Anwendbarkeit des TMG oder des BDSG je nach Vorliegen von Inhalts-, Nutzungs- oder Bestandsdaten.

Eine derartige Einteilung sieht – was der Rechtssicherheit zuträglich ist – die neue DSGVO nicht mehr vor, sondern legt ihren Vorgaben nur personenbezogene Daten im Allgemeinen zugrunde. Besondere Voraussetzungen existieren nunmehr nur noch für sensible personenbezogene Daten nach Art. 9.

**Hinweis:** besonders beachtlich ist im Geltungsbereich der DSGVO, dass eine der in der geschäftlichen Praxis des Online-Handels bedeutsamen Bestimmung des §15 Abs. 3 TMG vergleichbare Regelung in der DSGVO fehlt. Die Erlaubnis zur pseudonymisierten Erstellung von Nutzungsprofilen zu Marktforschungszwecken ohne vorangegangene Einwilligung entfällt nach den neuen Bestimmungen ausdrücklich. Vielmehr wird derartiges „Profiling“ – ob mit oder ohne Pseudonym – nunmehr gemäß Erwägungsgrund 71 als klassische Verarbeitungsform eingestuft, die den allgemeinen Rechtmäßigkeitsanforderungen unterliegt.

### III. Geltungsbereich der DSGVO

Um die Auswirkungen des neuen Datenschutzrechtsakts auf den Online-Handel zielgerichtet und sinnhaft bestimmen zu können, ist die Berücksichtigung des Anwendungsbereichs der DSGVO unumgänglich.

Auch wenn die maßgeblichen Grenzziehungen (Geltungsausschluss für familiäre Zwecke, für behördliche präventive und repressive Zwecke etc.) die Anwendung der Verordnung für den Online-Handel unberührt lassen, ergibt sich eine wesentliche Einschränkung aus Erwägungsgrund 14. Dieser beschränkt das Pflichtprogramm der DSGVO nämlich ausschließlich auf Fälle der Erhebung, Verarbeitung und Nutzung personenbezogener **Daten von natürlichen Personen**.

Personenbezogene Daten von juristischen Personen und von als juristische Personen gegründeten Unternehmen unterliegen den neuen datenschutzrechtlichen Vorgaben gerade nicht. Online-Händler, die ausschließlich im B2B-Bereich tätig sind und sich bei ihren Handelstätigkeiten nur Personengesellschaften gegenübersehen, haben die neuartigen Pflichten also nicht zu beachten.

In räumlicher Hinsicht hält die DSGVO dahingegen aber eine Erweiterung bereit. Unbeachtlich für ihre Anwendung soll es nunmehr nämlich sein, dass die Datenverarbeitung außerhalb der Union erfolgt, solange nur der Verantwortliche oder ein Auftragsverarbeiter seine Niederlassung in der EU hat, Art. 3 Abs. 1.

Gleichsam findet die DSGVO in allen Fällen Anwendung auch für außereuropäische Verarbeiter (im Einzugsgebiet souveräner Drittstaaten), sofern sie Daten von EU-Bürgern erheben oder verarbeiten und die Verarbeitung – wie im E-Commerce regelmäßig – im Zusammenhang mit dem Absatz von Waren oder Dienstleistungen steht, Art. 3 Abs. 2 lit. a.

Damit wird erstmals auch Verantwortlichen aus Drittländern unmittelbar die Beachtung der europäischen Vorgaben aufgezwängt, sofern sie zu Zwecken des Produktabsatzes an EU-Bürger herantreten und vom Ausland aus deren persönliche Daten erheben.

## B. Gleichbleibendes und relevante Änderungen

### I. Unveränderte Datenschutzgrundsätze

Die DSGVO stellt in Artikel 5 allgemeine Grundsätze für den Umgang mit erhobenen personenbezogenen Daten auf, die weitestgehend an die in Deutschland bereits vorherrschenden Richtlinien für die Datenverarbeitung angelehnt sind und somit keine bedeutenden Änderungen mit sich bringen, im Online-Handel aber dennoch uneingeschränkte Beachtung finden müssen.

#### 1.) Verarbeitungsverbot mit Erlaubnisvorbehalt

Dem geltenden deutschen Datenschutzrecht liegt ebenso wie der DSGVO die Maxime des Erlaubnisvorbehalts zugrunde, nach welchem sämtliche Datenerhebungs- und Verarbeitungsvorgänge verboten und nur ausnahmsweise dann zulässig sind, wenn der Betroffene dies ausdrücklich gestattet oder eine gesetzliche Legitimation zugunsten des Verantwortlichen eingreift.

Erfolgt eine Prozessierung personenbezogener Daten ohne privatautonome oder gesetzliche Berechtigung, gestaltet sich der Vorgang nach deutschem und europäischen Leitbild gleichermaßen als rechtswidrig (vgl. §4 Abs. 1 BDSG, 6 DSGVO).

#### 2.) Datensparsamkeit und enge Zweckbindung

Die nach §§ 3 und 4 BDSG maßgeblichen Prinzipien der Datensparsamkeit und zweckgebundenen Verarbeitung spiegeln sich in Art. 5 Abs. 1 lit. b und c wieder. Danach muss die Datenerhebung zum einen auf das für die Erfüllung ihres Zwecks erforderliche Maß derart begrenzt sein, dass nicht mehr Daten erhoben werden dürfen als zwingend benötigt.

Dies ist, soweit mit dem Erhebungszweck vereinbar und zumutbar, gemäß Erwägungsgrund 78 durch eine bestmögliche Pseudonymisierung zu erreichen.

Dem Grundsatz der Datensparsamkeit dient auch das in Art. 5 Abs. 1 lit. e formulierte Prinzip der Speicherbegrenzung, welches dem Verantwortlichen die Einhaltung einer am Verarbeitungszweck bemessenen Speicherdauer abverlangt und ihn zur Löschung verpflichtet, sofern der Zweck erreicht ist (so momentan auch §20 Abs. 2 Nr. 2 BDSG).

Das Prinzip der Speicherbegrenzung ist im Online-Handel vor allem bei der Datennutzung zur Abwicklung von Verträgen zu berücksichtigen und verpflichtet zur Löschung nach gegenseitiger Erfüllung und Ablauf der Widerrufsfrist.

Gleichzeitig ergeht aus der genannten Bestimmung der Grundsatz, dass Daten nur für festgelegte und mithin genau eingegrenzte, legitime und eindeutige Zwecke erhoben werden dürfen. Eine Weiterverarbeitung über den vereinbarten Zweck hinaus sowie eine einseitige Umwidmung des Erhebungs- und Nutzungszwecks mit dem Ziel, die Daten auch anderweitig zu verwenden, sind grundsätzlich untersagt.

### 3.) Datensicherheit

Anders als im BDSG ist in der DSGVO das Prinzip der Datensicherheit als allgemeiner Grundsatz normiert. Geht er in den einschlägigen nationalen Regelungen implizit aus spezifischen Anforderungen hervor, fordert Art. 5 Abs. 1 lit. f (i.V.m. Art 32) ausdrücklich zur Gewährleistung dessen auf, dass unter Berücksichtigung der technischen und organisatorischen Möglichkeiten, der Kosten und der zweckbedingten Umstände der Verarbeitung erhobene Daten angemessen geschützt und dem Zugriff unbefugter Dritter entzogen werden. Gleichzeitig soll die Verhinderung unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung sichergestellt werden.

Das Sicherheitsniveau muss dabei dem jeweiligen Gefahrenpotenzial angemessen angepasst sein.

Auch die Datensicherheit kann zur bestmöglichen zweckwahrenden Anonymisierung und Pseudonymisierung verpflichten, hält aber auch zur Wartung und Überprüfung der Integrität der verwendeten Systeme an.

### 4.) Datenrichtigkeit

Ebenfalls als datenschutzrechtlicher Grundsatz ist in Art. 5 Abs. 1 lit. d DSGVO auch das in §20 Abs. 1 BDSG zum Ausdruck kommende Richtigkeitsgebot formuliert, das den Verantwortlichen verpflichtet, für die sachliche und inhaltliche Tatsächlichkeit der erhobenen Daten und für ihre Aktualität Sorge zu tragen.

Gleichsam fordert das allgemeine Prinzip dazu auf, alle technischen und organisatorischen Maßnahmen dafür zu treffen, dass im Falle der Unrichtigkeit oder Rückständigkeit der verwendeten Daten eine unverzügliche Berichtigung oder Löschung erfolgen kann.

Damit geht die genannte Vorschrift weiter als §20 Abs. 1 BDSG, der nur eine Berichtigung, aber keine Löschung als ultima ratio vorsieht.

### 5.) Neuartig: Rechenschaftspflicht

Als gegenüber den bewährten Datenschutzgrundsätzen relevante Änderung erweist sich die in Art. 5 Abs. 2 DSGVO erstmalig eingeführte Pflicht, auf Anforderung die Einhaltung aller Datenschutzprinzipien nachweisen zu können.

Mit der so begründeten Rechenschaftspflicht wollte der europäische Gesetzgeber der Umsetzung der datenschutzrechtlichen Grundpflichten Nachdruck verleihen und zur unbedingten Befolgen anhalten.

Inwiefern sich aus der neuartigen Verbindlichkeit Eingriffsbefugnisse der Aufsichtsbehörden herleiten lassen, vermag noch nicht abschließend beurteilt zu werden. Allerdings können bei einem belegbaren Verstoß gegen die Basisprinzipien nach Art. 83 Abs. 5 DSGVO äußerst empfindliche Geldbußen bis zu einer Höhe von 20 000 000€ oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt werden.

Empfehlenswert ist es für Online-Händler deshalb, durch eine geeignete Protokollierung ihrer Verarbeitungssysteme und Nutzungsumfänge im Zweifel beweisen zu können, dass eine kontinuierliche

und gewissenhafte autonome Ausrichtung nach den geltenden Leitlinien erfolgt ist und weiterhin erfolgt.

## II. Änderungen der Voraussetzungen für rechtmäßige Datenverarbeitungen

Ebenso wie das bisherige deutsche Datenschutzrecht geht auch die europäische DSGVO von einem grundsätzlichen Datenverarbeitungsverbot mit Erlaubnisvorbehalt aus. Während jedoch die Tatbestände einer rechtmäßigen Erhebung und Nutzung von personenbezogenen Daten im BDSG über das Gesetz hinweg verstreut aufzufinden sind, kodifiziert der europäische Gesetzgeber diese gesammelt in Art. 6 DSGVO. Zwar wird auch hier eine Differenzierung zwischen der durch eine Einwilligung des Betroffenen gerechtfertigten Datennutzung und gesetzlichen Gestattungstatbeständen vorgenommen. Dabei entfallen allerdings bisher nach dem BDSG ausdrücklich vorgesehene Rechtmäßigkeitsgrundlagen.

### 1.) Die datenschutzrechtliche Einwilligung

Wie auch das deutsche Recht macht der europäische Gesetzgeber die Rechtmäßigkeit einer Datenverarbeitung maßgeblich von der Einwilligung des Betroffenen abhängig, Art. 6 Abs. 1 lit. a DSGVO.

#### a) Ausdrücklichkeits- und Bestimmtheiterfordernis

Dabei ist, ähnlich der derzeitigen Kodifizierung in §4a BDSG, zwingend darauf zu achten, dass die Einwilligung des Nutzers auf dessen autonomer und ausdrücklich selbstbestimmter Entscheidung zur Preisgabe der relevanten Daten beruht. Sie ist insofern streng zweckgebunden einzuholen und muss, wie sich aus dem Umkehrschluss der Formulierung „Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben“ ergibt, stets die mit der Einwilligung zu rechtfertigenden Verarbeitungszwecke anführen.

**Ebenso wie im geltenden deutschen Recht entfällt damit die Möglichkeit einer Generaleinwilligung in eine unbeschränkte Verarbeitung und Nutzung der personenbezogenen Daten.**

Auch der europäische Gesetzgeber sieht die Möglichkeit einer elektronischen Einwilligung (derzeit geregelt in §13 Abs. 2 TMG) vor, regelt deren Anforderungen aber nicht spezifisch, sondern ordnet sie ausweislich des Erwägungsgrundes 32 als einen Unterfall der „schriftlichen Erklärung“ ein.

Hinweis: möglich ist auch die Einholung einer mündlichen Erklärung sowie die informationstechnologische Ausgestaltung eines Einwilligungsprozesses, bei dem hinreichend eindeutige Verhaltensweisen des Nutzers als Rechtfertigung gelten können.

Wird die Einwilligungserklärung – wie im Online-Handel üblich – elektronisch eingeholt, so soll dies nach Erwägungsgrund 32 beispielsweise durch das aktive Anklicken eines Kontrollkästchens möglich sein.

Erstmalig normiert wird im unmittelbaren Zusammenhang auch die – in Deutschland vor allem durch die Rechtsprechung geprägte – Kasuistik der vorangekreuzten Einwilligungsfelder.

Nach Erwägungsgrund 32 sollen Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit der betroffenen Person keine wirksame Einwilligung darstellen.

### b) Beweisbarkeits- und Transparenzgebot

Aus Art. 7 DSGVO, welcher die Anforderungen an die rechtfertigende datenschutzrechtliche Einwilligung konkretisiert, geht hervor, dass eine eingeholte Einwilligung zwingend zu dokumentieren und zu speichern ist. Online-Händler haben insofern durch informationstechnologische Systeme sicherzustellen, dass sie eine erteilte Nutzereinstimmung im Zweifel beweisen können.

Weil die elektronische Einwilligungserklärung als Form der schriftlichen gewertet wird, ist für ihr Wirksamwerden das neue spezialgesetzlich normierte Transparenzgebot des Art. 7 Abs. 2 DSGVO zu beachten. Danach muss die Einwilligung in klarer und verständlicher Sprache erfolgen und insbesondere dann, wenn der Einwilligungstext noch andere Sachverhalte betrifft, die datenschutzrechtliche Relevanz gesondert hervorheben.

### c) Freiwilligkeit

Ist die Einwilligung nur rechtfertigend, wenn sie Ausdruck einer selbstbestimmten und ungezwungenen Entscheidung ist, so muss sie zwingend freiwillig erteilt werden (Erwägungsgrund 32). Jegliche forcierenden Handlungen des Verarbeitenden sowie die Ausübung von Druck lassen ihre Wirksamkeit entfallen.

**In diesem Zusammenhang neu ist die Regelung des Art. 7 Abs. 4 DSGVO, welche die Freiwilligkeit auch davon abhängig macht, ob die Einwilligung in Datenverarbeitungsprozesse als zwingende Bedingung für die Durchführung eines Vertrages formuliert ist, obwohl der Verarbeiter die Daten dafür eigentlich nicht benötigt.**

Anzunehmen ist insofern, dass die Freiwilligkeit und mithin die Wirksamkeit der Einwilligung fortan entfallen soll, wenn an ihre Erteilung das „Ob“ der Durchführung eines Kausalgeschäfts gekoppelt wird, das mit der konkreten Datennutzung oder dem Umfang der erhobenen Daten in keinem sachlichen Zusammenhang steht.

Auswirkungen ergeben sich hier **vor allem für Online-Gewinnspiele**, bei denen eine Teilnahme nicht selten von der Einwilligung des Nutzers in die Verarbeitung von Daten zu Werbezwecken abhängig gemacht wird, die für die konkrete Gewinnaktion nicht zwangsweise erforderlich sind. Ebenso wird die Zulässigkeit des Erfordernisses einer Newsletter-Anmeldung zur möglichen Inanspruchnahme eines Gewinns in Zukunft vor neue Hürden gestellt werden.

#### d) **Widerruflichkeit**

Wie im deutschen Datenschutzrecht muss auch nach der DSGVO der Betroffene eine einmal erteilte Einwilligung jederzeit mit Wirkung für die Zukunft widerrufen können, Art. 7 Abs. 3.

**Neu** ist hierbei allerdings die Pflicht des Verarbeiters zur Einhaltung eines **Simplizitätsgebots: der Widerruf der Einwilligung muss in Zukunft genau so einfach sein wie ihre Erteilung.**

Dies erscheint insbesondere im Falle elektronisch eingeholter Einwilligungen durch die schlichte Betätigung einer Checkbox problematisch, weil es – ohne registriertes Kundenkonto – meist an der Möglichkeit fehlen wird, das Checkbox-Häkchen nachträglich wieder zu entfernen. Zwar wird ausdrücklich nicht gefordert, dass das Widerrufsverfahren demjenigen der Erteilung 1:1 entspricht. Fraglich bleibt aber dennoch, ob ein Widerruf per Mail oder Telefonanruf in seiner Unkompliziertheit dem bloßen Setzen eines Häkchens nebst einer Einwilligungserklärung wird entsprechend können.

Immerhin für die wegen ihrer Marketingwirksamkeit besonders bedeutsamen Fälle der Newsletter-Werbung wird auch dem neuen Simplizitätsgebot wohl hinreichend dadurch Rechnung getragen, dass jeder Mail am Ende ein eigener „Unsubscribe-Link“ beigestellt wird, dessen bloße Betätigung der Datenverarbeitung Einhalt gebietet.

#### e) **Wichtig: Fortgeltung für vor 2018 eingeholte Einwilligungen**

Weil mit Auslaufen der Übergangsfristen zum 25.08.2016 die besonderen Einwilligungsbestimmungen der DSGVO an die Stelle der bis dato geltenden nationalen Vorschriften treten werden, war fraglich, wie die bis zu diesem Zeitpunkt unter Geltung der alten Rechtslage in den Mitgliedsstaaten wirksam eingeholten Einwilligungen umgegangen werden sollte.

Zugunsten der Verarbeiter hat sich der europäische Gesetzgeber hier für eine Fortgeltung der bereits eingeholten datenschutzrechtlichen Einwilligungen entschieden.

Nach Erwägungsgrund 171 bleiben insofern auf Grundlage des geltenden BDSG und TMG wirksam eingeholte Einwilligungen in Verarbeitungsprozesse auch unter Geltung der neuen DSGVO bestehen, sofern die Art der erteilten Einwilligung auch den Bedingungen der DSGVO entspricht. Da die maßgeblichen Einwilligungserfordernisse nach geltendem und neuem Recht in Deutschland sich weitgehend überschneiden, entfällt im Online-Handel in der Regel die Notwendigkeit, zum 25.05.2018 von jedem Nutzer, dessen Daten bereits mit Einwilligung verarbeitet werden, eine solche erneut einzuholen.

#### f) Neu: besondere Erfordernisse für die Einwilligung Minderjähriger

Eine neuartige Ausprägung hat die datenschutzrechtliche Einwilligungsdogmatik in der Normierung spezieller Wirksamkeitsanforderungen für die datenschutzrechtliche Verarbeitungserlaubnis Minderjähriger erhalten, welche die Tragweite und Reichweite von erteilten Rechtfertigungen weniger sicher und umfassend abzuschätzen wissen als Erwachsene.

Während nach geltendem deutschen Recht die Wirksamkeit von Einwilligungen Minderjähriger individuell nach deren geistiger Reife und konkreter Einsichtsfähigkeit bemessen wird, wird es nach Art. 8 DSGVO zukünftig starre Altersgrenzen geben.

Gemäß Art. 8 Abs. 1 DSGVO wird die Einwilligung eines Minderjährigen in die Verarbeitung von diesen betreffenden personenbezogenen Daten in Kommunikationsmedien grundsätzlich nur wirksam, wenn dieser das 16. Lebensjahr vollendet hat.

Kinder und Jugendliche unter 16 Jahren sollen demgegenüber autonom keine wirksamen Erlaubnisse erteilen können. Vielmehr bedarf es für die rechtmäßige Nutzung der Daten von unter 16-jährigen in Zukunft der ausdrücklichen Genehmigung des gesetzlichen Vertreters.

Die maßgebliche Altersgrenze bei 16 Jahren ist allerdings nur ein Richtwert, von welchem die Mitgliedsstaaten gemäß Art. 8 Abs. 1 Unterabsatz 2 DSGVO abweichen dürfen. **Dabei darf in Anbetracht der Wirksamkeit von Minderjährigeneinwilligungen allerdings nicht die absolute Untergrenze von 13 Lebensjahren unterschritten werden.**

Inwiefern der deutsche Gesetzgeber bei der nationalen Ausgestaltung der speziellen Anforderungen an der vorgegebenen Altersgrenze von 16 Jahren festhalten oder diese über- oder unterbieten wird, kann bisher noch nicht gesagt werden.

Fest steht aber jetzt schon, dass Online-Händler **künftig geeignete Altersverifikationssysteme** in ihre elektronischen Einwilligungsprozesse integrieren müssen, um sich nicht der Gefahr unrechtmäßiger Datenverarbeitungen auszusetzen und mithin die Wirksamkeit aller eingeholten Einwilligungen garantieren zu können. Gleichsam wird die **Einrichtung neuer informationstechnologische Mechanismen** erforderlich werden, mit denen ein gesetzlicher Vertreter als solcher identifiziert und zur Abgabe einer eigenständigen Einwilligung für den Schutzbefohlenen veranlasst werden kann.

Dies gilt insbesondere deshalb, weil Art. 8 Abs. 2 DSGVO den Verantwortlichen abverlangt, „angemessene Anstrengungen zu unternehmen“, um die Einhaltung der altersgerechten Differenzierung zu gewährleisten und im Zweifel die Einschaltung der elterlichen Vertreter sicherzustellen.

## 2.) Gesetzliche Erlaubnistatbestände

Neben der ausdrücklichen und autonomen Einwilligung des Betroffenen, die als primäres datenschutzrechtliches Institut für die Rechtmäßigkeit jeglicher Verarbeitung von Nöten ist, kodifiziert die DSGVO zusätzliche Konstellationen zulässiger Datennutzungsprozesse, bei denen eine vorherige Einwilligung entbehrlich sein soll.

Gleichzeitig entfallen aber auch gesetzliche Erlaubnisse für bisher nach dem BDSG und TMG zulässige Verarbeitungsprozesse.

### a) Rechtmäßige Verarbeitungen ohne Einwilligungserfordernis

Erlaubt ist nach Art. 6 Abs. 1 lit. b-f die einwilligungslose Datenverarbeitung, die

- für die Erfüllung eines Vertrages, dessen Vertragspartei die betroffene Person ist (vgl. die gleichlautende Regelung des §28 Abs. 1 Nr. 1 BDSG), oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Antrag der betroffenen Person erfolgen
- zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist, der der Verantwortliche unterliegt
- erforderlich ist, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;
- im öffentlichen Interesse oder zur Erfüllung hoheitlicher Aufgaben erforderlich ist
- die Wahrung berechtigter Interessen des Verantwortlichen oder eines Dritten erforderlich ist und die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person nicht überwiegen (vgl. §28 Abs. 1 Nr. 2 BDSG)

Insbesondere die Datenverarbeitung zur Wahrung berechtigter Interessen wird im Online-Handel große Bedeutung erlangen, da sie im Einzelfall nicht nur Fälle des Direktmarketings, sondern auch nutzungsbasierte Online-Werbung zu rechtfertigen vermag, ohne dass es einer Einwilligung bedürfte.

So ergibt sich aus Erwägungsgrund 47, dass die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden kann.

Voraussetzung bleibt aber in jedem Einzelfall, dass vor allem die persönlichkeitsrechtlichen Belange des Geworbenen die Werbeinteressen nicht überwiegen.

### b) Wegfall anerkannter Erlaubnisgründe

Ein Rückgriff auch die berechtigten Interessen wird in Zukunft vor allem deswegen maßgebliche Bedeutung erlangen, weil für die Praxis des Online-Handels hoch relevante Nutzungsvorgänge, die bisher ohne Einwilligung möglich waren, ab 2018 den generellen Einwilligungserfordernissen unterliegen werden.

So werden die besonderen datenschutzrechtlichen Erlaubnistatbestände der §§28a und 28b BDSG durch die DSGVO vollständig aufgehoben. Eine Datenübermittlung an Auskunftsteien sowie die Evaluation von Nutzerverhaltensmuster im Wege des „Scoring“ werden künftig nur noch dann zulässig sein, wenn Ihnen eine ausdrückliche Einwilligung des Betroffenen im Sinne des Art. 6 Abs. 1 lit. a DSGVO

vorangegangen ist.

Gleiches gilt für die Sondererlaubnis der Datennutzung im Beschäftigungsverhältnis nach dem – zum 25.05.2018 entfallenden – §32 BDSG.

Besonders zu beachten ist gleichsam, dass die gesetzliche Erlaubnis zur pseudonymisierten Erstellung von Nutzungsprofilen zu Marktforschungszwecken ohne vorangegangene Einwilligung entfällt nach §15 Abs. 3 TMG ersatzlos wegfällt. Die Rechtmäßigkeit eines solchen „Profiling“ – ob mit oder ohne Pseudonymisierung – wird sich in Zukunft ausschließlich am Vorliegen einer wirksamen zweckgerichteten Betroffenen einwilligung orientieren.

Zwar ermöglichen die neuen, meist generell gehaltenen Erlaubnistatbestände der DSGVO eine flexiblere Rechtsanwendung. In Ermangelung klarer Abgrenzungskriterien und der Normierung eindeutig zulässiger Datenverarbeitungsprozesse geht dies aber für die Verantwortlichen gleichsam zu Lasten der Rechtssicherheit.

### 3.) Geänderte Zulässigkeitsbedingungen für die Zweckänderung von Verarbeitungen

Die DSGVO statuiert im Verhältnis zur derzeitigen Rechtslage deutlich strengere Anforderungen an die Zulässigkeit von Datenverarbeitungen, die zu einem anderen Zweck erfolgen sollen als zu demjenigen, für den die Betroffenen einwilligung ursprünglich eingeholt wurde.

Konnte die einwilligungslose Zweckänderung, beispielsweise die Verwendung einer für den Empfang von Newslettern erhobenen E-Mail-Adresse zu Zwecken der Marktforschung oder der Liquiditätsprüfung oder der Erstellung eines Nutzerprofils, bisher nach §28 Abs.2 Nr. 1 BDSG durch berechnigte Interessen gerechtfertigt werden, ist nunmehr ausweislich des Art. 6 Abs. 4 DSGVO eine umfangreiche Interessenabwägung der Vereinbarkeit erforderlich, die bei negativem Ausfall die Einholung einer separaten Einwilligung erforderlich machen soll.

Für die Bewertung, ob der intendierte Nutzungszweck mit dem ursprünglichen vereinbar ist, sind zukünftig insbesondere folgende Gesichtspunkte zu berücksichtigen:

- jede Verbindung zwischen den Zwecken, für die die personenbezogenen Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung
- der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere hinsichtlich des Verhältnisses zwischen den betroffenen Personen und dem Verantwortlichen
- die Art der personenbezogenen Daten, insbesondere ob besondere Kategorien personenbezogener Daten (sensible Daten nach Art. 9 DSGVO) verarbeitet werden oder ob personenbezogene Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 verarbeitet werden
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen
- das Vorhandensein geeigneter Garantien, wozu Verschlüsselung oder Pseudonymisierung gehören kann

Ergibt die stets im Einzelfall durchzuführende Prüfung eine Unvereinbarkeit, ist die Zweckänderung nur bei expliziter Einwilligung zulässig.

Weil der Verantwortliche das positive Abwägungsergebnis und seine Grundlagen im Zweifelsfall aber beweisen muss und die genannten Kriterien in Ermangelung konkreter Bewertungsmaßstäbe kaum geeignet sind, dem Laien eine interessengerechte Entscheidung zu ermöglichen, wird sich die Änderung der Zulässigkeitsanforderungen faktisch wie eine Sperre der einwilligungslos erlaubten Zweckänderungen auswirken.

Zu hoch sind nämlich die Gefahren einer fehlerhaften Beurteilung und zu gering ist die Rechtssicherheit, sodass zu empfehlen ist, im Interesse einer Risikominimierung künftig jeder Zweckänderung eine erneute Einwilligungserteilung vorangehen zu lassen.

### III. Erweiterung der Betroffenenrechte und Handlungspflichten der Verantwortlichen

Die neue DSGVO geht mit einer erheblichen Stärkung der Betroffenenrechte einher, die auch im Online-Handel zwingend Berücksichtigung finden müssen und weitreichende Handlungspflichten begründen können. Teilweise wurden den deutschen Datenschutzgesetzen bereits bekannte Rechte um neue Inhalte und Ausprägungen erweitert, teilweise wurden gänzlich neue Berechtigungen von Betroffenen formuliert.

#### 1.) Auskunftsrecht, Art. 15 DSGVO

Ebenso wie der derzeit geltende §34 BDSG sieht auch die DSGVO in Art. 15 ein Auskunftsrecht des Betroffenen vor, nach welchem dieser auf Verlangen über die Art, den Inhalt und die Zwecke der von ihm erhobenen Daten zu informieren ist.

Zukünftig wird der Umfang der mit dem Auskunftsrecht korrespondierenden Auskunftspflicht des Verantwortlichen aber das derzeit geltende Maß bei weitem überschreiten und so den Betroffenen zur Einholung eines ganzen Katalogs an Informationen berechtigen.

Auf Antrag sind dem Betroffenen, dessen Daten erwiesenermaßen erhoben wurden, insofern fortan Auskünfte über folgende Umstände zu erteilen:

- die Verarbeitungszwecke
- die Kategorien personenbezogener Daten, die verarbeitet werden
- die Empfänger oder Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, insbesondere bei Empfängern in Drittländern oder bei internationalen Organisationen
- falls möglich die geplante Dauer, für die die personenbezogenen Daten gespeichert werden, oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- das Bestehen eines Rechts auf Berichtigung oder Löschung der sie betreffenden personenbezogenen Daten oder auf Einschränkung der Verarbeitung durch den Verantwortlichen oder eines Widerspruchsrechts gegen diese Verarbeitung
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, alle verfügbaren Informationen über die Herkunft der Daten

- ggf. das Bestehen einer automatisierten Entscheidungsfindung einschließlich „Profiling“ gemäß Artikel 22 Absatz 1 und 4 DSGVO und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person

Gleichzeitig wird der Verantwortliche im Falle des Auskunftsverlangens gemäß Art. 15 Abs. 3 DSGVO künftig verpflichtet sein, den Informationen eine Kopie sämtlicher personenbezogener Daten, die Gegenstand der Verarbeitung sind, beizustellen, und so die von der Auskunftspflicht umfassten Datenkategorien zu konkretisieren.

Online-Händler werden demnach gehalten sein, digitale Verzeichnisse anzulegen, in denen für jeden Betroffenen die individuell erhobenen Daten hinterlegt sind, damit diese im Falle der Geltendmachung von Auskunftsrechten zielgerichtet übermittelt werden können.

Erfolgt der Antrag – wie im Online-Handel regelmäßig – elektronisch, so sind die Informationen ebenfalls in einem gängigen elektronischen Format (bspw. per Mail) bereitzustellen.

## 2.) Berichtigungs- und Löschungsrecht, Art. 16 und 17 DSGVO

Ebenso wie bereits nach geltendem deutschem Recht (§35 BDSG) wird der Betroffene auch unter Geltung der DSGVO mit Berichtigungs- und Löschungsansprüchen ausgestattet. Allerdings wurden deren Voraussetzungen und die Grundlagen für eine Berechtigung reformiert.

Während eine Berichtigung, zu der ausdrücklich auch die Vervollständigung gezählt wird, nach Art. 16 DSGVO dann verlangt werden kann, wenn die erhobenen Daten unrichtig sind, muss der Verantwortliche dem Anspruch auf Löschung dann Rechnung tragen, wenn

- der Zweck der Datenverarbeitung erreicht wurde und die personenbezogenen Daten insofern nicht mehr erforderlich sind
- der Betroffene seine Einwilligung widerrufen hat und keine anderweitige (gesetzliche) Rechtsgrundlage für die Verarbeitung im Sinne von Art. 6 Abs. 1 lit. b-f DSGVO eingreift
- der Betroffene gegen die Verarbeitung Widerspruch im Sinne des Art. 21 DSGVO eingelegt hat
- die personenbezogenen Daten unrechtmäßig, also nicht von Art. 6 DSGVO gedeckt, erhoben, verarbeitet oder genutzt wurden
- der Betroffene seine Einwilligung als Minderjähriger gemäß Art. 8 DSGVO abgegeben hat und die Löschung verlangt (\*Achtung:\* dieses Recht steht dem Betroffenen auch zu, wenn er inzwischen nicht mehr Minderjährig ist, Erwägungsgrund 65)

**Wichtig:** außer in den Fällen, in denen die Einwilligung durch einen (ehemals) Minderjährigen oder dessen gesetzlichen Vertreter erteilt wurde, ist die Löschung durch den Verantwortlichen auch ohne eine vorherige Geltendmachung des Betroffenen, also eigenständig und von sich aus, zu bewirken!

Hat der Verantwortliche die zu löschenden Daten an Dritte weitergegeben oder gar öffentlich gemacht, hat er bei Vorliegen eines Löschungsgrundes alle Dritten über die Löschung zu informieren, damit diese ihrerseits Löschungsverfahren einleiten können. Diese Pflicht greift nur insoweit, wie die Unterrichtung

möglich und dem Verantwortlichen nicht unzumutbar ist.

Verlangt der Betroffene eine Auskunft über die Personen der Dritten, so ist diese unverzüglich zu erteilen (Art. 17 Abs. 2 i.V.m. Art. 19 DSGVO).

Eine Löschung kann trotz Vorliegen eines oben angeführten Lösungsgrundes rechtmäßig abgelehnt werden, wenn der Verantwortliche ein berechtigtes Interesse an der Weiternutzung der Daten hat (Art. 17 Abs. 3 DSGVO). Im Online-Handel kann dies insbesondere der Fall sein, wenn die Verarbeitung oder Speicherung **zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich** ist.

### 3.) Neu: Recht auf Einschränkung der Verarbeitung, Art. 18 DSGVO

Mit der Einführung eines Rechts auf Einschränkung der Verarbeitung, welches im weitesten Sinne dem Recht auf Sperrung anstelle der Löschung nach §35 Abs. 3 BDSG entspricht, wollte der europäische Gesetzgeber Konstellationen Rechnung tragen, in denen eine sofortige Löschung entweder schutzwürdige Interessen der Verantwortlichen an der andauernden Speicherung unbillig beschneiden oder aber den Interessen des Betroffenen selbst zuwiderlaufen würde.

Unter Geltendmachung seines Rechts auf Einschränkung der Verarbeitung kann der Betroffene verlangen, dass sämtliche erhobene personenbezogene Daten fortan nur mit individueller Einwilligung (und zur Geltendmachung und Durchsetzung von Rechtsansprüchen) verarbeitet werden dürfen. Die Berechtigung des Verantwortlichen zur Speicherung wird dadurch allerdings nicht berührt. Ist eine Einschränkung erfolgt, soll er die gespeicherten Daten nur nicht wie bisher verwenden können.

Eine Einschränkung der Verarbeitung ist fortan dann vorzunehmen, wenn der Betroffene es verlangt und

- er die Richtigkeit der personenbezogenen Daten bestreitet, wobei die Einschränkung dann für die Dauer zu bewirken ist, die es dem Verantwortlichen ermöglicht, die Richtigkeit der personenbezogenen Daten zu überprüfen **oder**
- die Verarbeitung unrechtmäßig ist und die betroffene Person die Löschung der personenbezogenen Daten ablehnt und stattdessen die Einschränkung der Nutzung der personenbezogenen Daten verlangt **oder**
- der Verantwortliche die personenbezogenen Daten für die Zwecke der Verarbeitung nicht länger benötigt, die betroffene Person sie jedoch zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt **oder**
- Widerspruch gegen die Verarbeitung gemäß Artikel 21 Abs. 1 DSGVO eingelegt hat, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen der betroffenen Person überwiegen

**Achtung:** erwirkt der Betroffene die Einschränkung der Verarbeitung, begründet dies für den Verantwortlichen **die Informationspflicht, den Betroffenen vor der Aufhebung der Einschränkung über diese zu unterrichten.**

Auch im Falle der Einschränkung ist der Verantwortliche gemäß Art. 19 DSGVO zusätzlich verpflichtet, Dritte, an welche die Daten übermittelt wurden, zu informieren, damit diese ihre Verarbeitungsprozesse

selbst einschränken können. Diese Pflicht greift nur insoweit, wie die Unterrichtung möglich und dem Verantwortlichen nicht unzumutbar ist.

Verlangt der Betroffene eine Auskunft über die Personen der Dritten, so ist diese unverzüglich zu erteilen.

#### 4.) Neu: Recht auf Datenübertragbarkeit, Art. 20 DSGVO

Im Vergleich zum geltenden deutschen Datenschutzrecht neuartig ist auch die Berechtigung des Betroffenen, vom jeweiligen Verantwortlichen die ungehinderte und uneingeschränkte Übermittlung erhobener personenbezogener Daten an einen Dritten zu verlangen. Diese dient dem Ziel, eine bessere persönliche Überwachung und Kontrolle vor allem bei automatisierten Verarbeitungsvorgängen zu gewähren und die Prozessierung von einmal erhobenen Daten auf einen Dritten zu vereinfachen, ohne dass es einer erneuten Eingabe durch den Betroffenen bedürfte.

Der Betroffene kann insofern entweder nach Art. 20 Abs.1 DSGVO die vom Verantwortlichen die Herausgabe der erhobenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format verlangen und diese – ohne dass der Verantwortliche dies behindern darf – eigenständig einem anderen übermitteln.

Alternativ kann der Betroffene aber auch direkt vom Verantwortlichen verlangen, die Übermittlung ohne seine eigene Zwischenschaltung unmittelbar an den bestimmungsgemäßen Empfänger zu veranlassen, Art. 20 Abs. 2 DSGVO.

Allerdings ist – um schützenswerte Interessen des herausgabepflichtigen Verantwortlichen zu wahren – die zulässige Ausübung des Rechts auf Datenübertragbarkeit durch den Betroffenen auf die Fälle begrenzt, in denen

- entweder seine Einwilligung in die originäre Verarbeitung erforderlich war oder aber die Daten ohne Einwilligung zur Durchführung eines Vertragsverhältnisses rechtmäßig genutzt werden durften **oder**
- (wie im Online-Handel regelmäßig) die Datenverarbeitung mithilfe automatisierter Verfahren erfolgt ist

Online-Händler, die personenbezogene Daten erheben und verarbeiten, werden sich in Ansehung des neuen Betroffenenrechts zukünftig Nutzerbegehren fügen müssen, in welchen die Übermittlung von erhobenen Daten an einen Dritten verlangt wird.

Gleichzeitig werden sie in der mehr als zweijährigen Übergangsfrist gehalten sein, interoperable Formate zu entwickeln und einzurichten, welche eine reibungslose Datenübertragbarkeit ermöglichen (vgl. auch Erwägungsgrund 68).

## 5.) Neu: Widerspruchsrecht bei einwilligungsloser Verarbeitung zur Wahrung berechtigter Interessen, Art. 21 DSGVO.

Erfolgt eine Datenverarbeitung durch den Verantwortlichen ohne Einwilligung aufgrund der gesetzesmäßigen Wahrnehmung berechtigter Interessen, so steht dem Betroffenen fortan das Recht zu, dieser Verarbeitung zu widersprechen.

Im Online-Handel dürfte das neue Widerspruchsrecht vor allem dann Bedeutung entfalten, wenn eine Datennutzung zu (berechtigten) Direktmarketingzwecken erfolgt, ohne dass der Betroffene eingewilligt hätte, und der Betroffene unter Verarbeitung seiner Daten mithin mit Werbemaßnahmen konfrontiert wird.

Grundsätzlich ist einem Widerspruch nur stattzugeben, wenn dieser unter Darlegung persönlicher Versagungsgründe erfolgt, welche die berechtigten Interessen des Verantwortlichen überwiegen.

Im Falle der Direktwerbung jedoch ist einem Widerspruch in die werbetechnische Datenverarbeitung auch ohne Angabe von Gründen und ohne Interessenabwägung stets Folge zu leisten, Art. 21 Abs. 2 und 3 DSGVO. Der Widerspruch erstreckt sich in diesem Falle auch auf sämtliche Maßnahmen zur Erstellung von Nutzerprofilen, die mit der Werbung in Zusammenhang stehen.

Legt der Betroffene gegen die Datenverarbeitung zu Werbezwecken Widerspruch ein, so hat der Verantwortliche unverzüglich sicherzustellen, dass eine diesbezügliche Nutzung der personenbezogenen Daten fortan unterbleibt.

Wie die Widerspruchsoption insbesondere bei automatisierten Datenerhebungsprozessen im Internet technologisch ausgestaltet werden muss, gibt die DSGVO nicht vor, sondern überlässt die Einrichtung von Widerspruchssystemen mithin dem jeweiligen Verantwortlichen.

Zu erwarten ist aber, dass Online-Händler, die von der Möglichkeit einwilligungsloser Datenverarbeitungen zu Werbezwecken Gebrauch machen, künftig gehalten sein werden, entweder elektronische Widerspruchsmechanismen mit eindeutiger Identifizierbarkeit des jeweiligen Betroffenen vorzuhalten oder aber den Widerspruch über gängige Kommunikationsmittel entgegenzunehmen.

In jedem Fall besteht bei der einwilligungslosen Datenverarbeitung zu Werbezwecken eine **spezielle Informationspflicht, den Betroffenen auf sein Widerspruchsrecht und die Modalitäten für dessen Ausübung spätestens zu Beginn der ersten Kommunikation hinzuweisen, Art. 21 Abs. 4 DSGVO.**

## 6.) Neu: Recht auf Unbetroffenheit von rechtsverbindlichen Entscheidungen mit Grundlage in automatisierten Datenprozessen, Art. 22 DSGVO

Ein zuvor nicht dagewesenes Betroffenenrecht, das insbesondere im Zusammenhang mit der Erstellung von Nutzerprofilen und der Zusammenarbeit mit Auskunftgebern zukünftig eine bedeutende Rolle spielen wird, normiert Art. 22 Abs. 1 DSGVO. Die Vorschrift verbietet es, ausschließlich automatisierte Verarbeitungsprozesse zur Entscheidungsgrundlage für die Begründung oder Ablehnung rechtlicher Beziehungen mit Betroffenen zu machen, und gewährt diesen insofern das Recht, von derartigen Entscheidungen unberührt zu bleiben.

Erfolgt eine Entscheidung, die auf automatisch erhobenen Daten beruht, dennoch, soll dem Betroffenen ein Anfechtungsrecht zustehen.

Mit der Kodifizierung dieses zugegeben abstrakten Rechts sollten Prozesse unterbunden werden, in denen Verantwortliche in Zusammenarbeit mit anderen datenverarbeitenden Institutionen automatisch Informationen über konkrete Betroffene einholen, um auf Basis dieser Informationen sodann über den zukünftigen Umgang mit dem Betroffenen zu entscheiden.

Als praxisrelevantestes Beispiel kann hier etwa die Anfrage von Bonitätsnachweisen bei Kreditinstituten oder Auskunfteien wie der Schufa angeführt werden, von deren Ausfall sodann die Begründung schuldrechtlicher Verbindlichkeiten automatisch abhängig gemacht wird.

Zu beachten ist allerdings, dass dieses neuartige Recht die Möglichkeiten von Online-Händlern, Vertragsverhältnisse unter Vorbehalt erfolgreicher Bonitäts- oder Liquiditätsprüfungen für bestimmte Zahlungsarten (etwa Lastschrift, Kreditkarte etc.) zu begründen, weitgehend unberührt lassen wird.

Insofern kann sich der Betroffene auf das oben angeführte Recht gemäß Art.22 Abs. 2 lit. a DSGVO nämlich gerade **nicht berufen, sofern die Entscheidung für die Erfüllung eines Vertrages erforderlich ist**. Im Bereich der Schufa-Anfragen und Bonitätskontrollen wird man die Erforderlichkeit stets mit Blick auf das Interesse des Händlers an der Vermeidung von Zahlungsausfällen und der Abwendung des vertragspartnerlichen Insolvenzrisikos bejahen können.

Liegt die Notwendigkeit der datenbasierten Entscheidung nicht in der Durchführung eines Vertrages begründet, so kann das Anfechtungsrecht des Betroffenen grundsätzlich nur dadurch abgewendet werden, dass der jeweilige Verantwortliche diesen zuvor in die Datenanfrage und die sich daraus ergebende intendierte Rechtsverbindlichkeit einwilligen lässt, Art. 22 Abs. 2 lit. c DSGVO.

## 7.) Achtung: neuartige Bearbeitungs- und Reaktionsfristen, Art. 12 Abs. 3 DSGVO

Während der Verantwortliche auf Basis der geltenden Rechtslage für die Umsetzung von Ansprüchen der Betroffenen und für das Folgeleisten etwaiger Rechte noch an keine zeitlichen Grenzen gebunden ist, führt die DSGVO mit Art. 12 Abs. 3 starre Fristen ein, binnen derer der Verantwortliche zwingend reagieren muss.

Ergreift der Betroffene Maßnahmen zur Durchsetzung seiner oben aufgeführten Rechte aus den Art. 15-22 DSGVO, so hat der Verantwortliche künftig unverzüglich, **spätestens aber innerhalb eines Monats nach Eingang des Antrags des Betroffenen, zur beantragten Maßnahme verpflichtend Stellung zu nehmen**. Insofern muss spätestens zum Ablauf einer einmonatigen Frist der Antrag so bearbeitet worden sein, dass der Verantwortliche dem Betroffenen

- im Falle der Abhilfe gemäß Art. 12 Abs. 3 DSGVO eine Information über die auf Antrag ergriffenen Maßnahmen (Berichtigung, Löschung, Beschränkung etc.) oder
- im Falle der Nichtabhilfe gemäß Art. 12 Abs. 4 DSGVO eine Unterrichtung über deren Gründe und die Möglichkeit einer Beschwerde bei der Aufsichtsbehörde und der Einlegung eines gerichtlichen Rechtsbehelfs

bereitstellen kann.

Grundsätzlich wird dem Verantwortlichen also eine Handlungsfrist gesetzt, binnen derer er sich mit der geltend gemachten Rechtsverfolgung des Betroffenen auseinandersetzen und dieser entweder nachkommen oder diese begründet ablehnen muss. Stellt die betroffene Person den Antrag elektronisch, so soll nach Möglichkeit auch die Unterrichtung elektronisch erfolgen.

Online-Händler werden, um dem neuartigen Fristerfordernis Rechnung tragen zu können, in Zukunft nicht nur eine lückenlose Dokumentation jedes individualisierten Datenverarbeitungsvorgangs zur Überprüfung der Begründetheit von Anträgen und zur schnellen Sammlung der für die Maßnahmen erforderlichen Informationen gewährleisten, sondern zudem mithilfe technischer Mittel Verfahren einrichten müssen, mit welchen eine Bearbeitung von Anträgen weitgehend automatisch erfolgen kann. Anders ließen sich – gerade im Angesicht einer Vielzahl von Anträgen – die kurz bemessenen Reaktionsfristen, die für jeden Antrag individuell laufen, wohl kaum einhalten.

**Allerdings besteht die Möglichkeit, in Härtefällen eine Fristverlängerung um 2 weitere Monate durchzusetzen, sofern dies unter Berücksichtigung der Komplexität und vor allem der Anzahl von Anträgen erforderlich ist. Will der Verantwortliche von dieser Verlängerungsmöglichkeit Gebrauch machen, hat er den Betroffenen innerhalb von einem Monat nach Eingang des Antrags (bei elektronischem Antrag in elektronischer Form) darüber zu informieren, dass die Bearbeitung mehr Zeit in Anspruch nimmt. Dabei sind der abschätzbare Zeitraum der Verzögerung sowie die Gründe für diese anzugeben, Art. 12 Abs. 3 Satz 3 DSGVO.**

## IV. Umfänglichere Datenschutzerklärung

Die Änderungen des europäischen Datenschutzrechts durch die DSGVO gehen nicht nur mit einer Stärkung und Ausweitung der Betroffenenrechte einher, sondern führen gleichzeitig auch neue und im Vergleich zur geltenden Rechtslage gesteigerte Informationspflichten für Verantwortliche ein.

Diese werden sich im Online-Handel vor allem in Form einer weitreichenden Novellierung der notwendigen Datenschutzerklärungen niederschlagen.

### 1. Verarbeitungsbezogene Pflichtangaben oder Hinweise in Datenschutzerklärung?

Im Geltungsbereich der neuen DSGVO gibt die Regelung des Art. 13 den Verantwortlichen eine Reihe von Informationspflichten auf, welche nicht nur eine einfache Identifizierung der Personen ermöglichen sollen, die mit den erhobenen Daten in Berührung kommen sollen, sondern vor allem die konkreten Verarbeitungsprozesse fair und für den Betroffenen transparent machen sollen.

Problematisch scheint hierbei zunächst, dass gemäß Art. 13 Abs.1 DSGVO die Bereitstellung der zwingenden Pflichtangaben **zum jeweiligen Erhebungszeitpunkt** verlangt und die Verantwortlichen im Online-Handel somit grundsätzlich dazu anhält, informationstechnische Lösungen einzurichten, die mit Hilfe von Pop-Ups oder anderen elektronischen Informationsmechanismen unmittelbar vor der Datenübermittlung über die Begleitumstände der konkreten Erhebung und Verarbeitung unterrichten.

Statuiert wird in anderen Worten eine betroffenenabhängige, individuelle Pflicht zur verarbeitungs-basierten Belehrung.

Allerdings hat der europäische Gesetzgeber berücksichtigt, dass eine derartige situationsbezogene Unterrichts-obliegenheit vor allem in Bereichen des elektronischen Geschäftsverkehrs mit einem unverhältnismäßigen Umstellungsaufwand für die Verantwortlichen einhergehen kann, der die Betroffeneninteressen an Fairness und Transparenz übersteigt.

Den Belangen der Händler wird hier durch Art. 13 Abs. 4 DSGVO Rechnung getragen, der die Pflicht zur situationsbedingten Belehrung vor jeglicher Datenverarbeitung dann entfallen lässt, wenn der jeweils Betroffene über alle maßgeblichen Informationen bereits verfügt.

Ermöglicht werden sollte durch diese Einschränkung insbesondere, alle relevanten Angaben an einer geeigneten Stelle des für die Datenverarbeitung grundlegenden Kommunikationssystems so zum Abruf bereit zu halten, dass der Betroffene leicht und zu jeder Zeit auf diese zugreifen kann und mithin einer konkreten Unterrichtung vor Beginn der Verarbeitungsprozesse nicht mehr bedarf.

Vor allem in Bereich der Telemediendienste – so auch im Online-Handel – wird es den Verantwortlichen also auch zukünftig erlaubt sein, anstelle einer verarbeitungsabhängigen Information von einer generellen Datenschutzerklärung Gebrauch zu machen, die an zentraler Stelle jederzeit eingesehen werden kann und über alle datenschutzrelevanten Umstände aufklärt.

**Hält der Verantwortliche also eine verordnungskonforme Datenschutzerklärung vor, ist er nicht mehr verpflichtet, jeder einzelnen Erhebung personenbezogener Daten eine Belehrung mit allen nach Art. 13 DSGVO maßgeblichen Angaben vorangehen zu lassen.**

Zu beachten ist hierbei, dass die Datenschutzerklärung ausweislich des Art. 12 Abs. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache anzuführen ist.

Bezüglich der Formerfordernisse ergeben sich im Vergleich zur derzeitigen Rechtslage keine neuen Voraussetzungen. Auch künftig wird es demnach im Online-Handel ausreichen, die Datenschutzerklärung auf einer Unterseite so einzurichten, dass sie mittels eines sprechenden Links von jeder Stelle der Web-Präsenz erreicht werden kann.

## 2.) Erweiterung der Pflichtinhalte

Nach der derzeit geltenden Rechtslage ergibt sich die Pflicht, sich über die konkreten Datenverarbeitungsprozesse im Online-Handel zu erklären, aus §13 Abs. 1 TMG. Diese Vorschrift gibt allerdings nur allgemein auf, über Art, Umfang und Zwecke der Erhebung und Verwendung personenbezogener Daten zu unterrichten und hat über die Jahre eine stetige Konkretisierung durch die Rechtsprechung erfahren.

Nach Ablauf der Übergangsfristen zum 25.05.2018 wird der Geltungsbereich des derzeitigen §13 Abs. 1 TMG durch den Katalog an Pflichtinformationen nach Art. 13 Abs. 1 DSGVO ersetzt werden, welcher den **Umfang an zwingend bereitzustellenden Angaben bedeutsam erweitert.**

Zukünftig sind Verantwortliche, die von der Möglichkeit einer Datenschutzerklärung im Sinne des Art. 13

Abs. 4 DSGVO Gebrauch machen wollen, gehalten, diese mit Informationen über alle der nachstehenden Punkte anzureichen:

- den Namen und die Kontaktdaten (Anschrift, E-Mail-Adresse, ggf. Telefon und Fax) des Verantwortlichen (sowie bei nicht in der Union niedergelassenen Verantwortlichen diejenigen des Vertreters)
- sofern verpflichtend zu bestellen, die Kontaktdaten des Datenschutzbeauftragten
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung
- wenn die Verarbeitung auf Artikel 6 Absatz 1 Buchstabe f DSGVO beruht, die berechtigten Interessen, die von dem Verantwortlichen oder einem Dritten verfolgt werden
- gegebenenfalls die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten (bei Weitergabe) und
- gegebenenfalls die Absicht des Verantwortlichen, die personenbezogenen Daten an ein Drittland oder eine internationale Organisation zu übermitteln, sowie das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von Übermittlungen gemäß Artikel 46 oder Artikel 47 oder Artikel 49 Absatz 1 Unterabsatz 2 einen Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, wie eine Kopie von ihnen zu erhalten ist, oder wo sie verfügbar sind.
- die Dauer, für die die personenbezogenen Daten gespeichert werden oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer
- das Bestehen eines Rechts auf Auskunft seitens des Verantwortlichen über die betreffenden personenbezogenen Daten (Art. 15 DSGVO) sowie auf Berichtigung oder Löschung (Art. 16 u. 17 DSGVO) oder auf Einschränkung der Verarbeitung (Art. 18 DSGVO) oder eines Widerspruchsrechts gegen die Verarbeitung (Art. 21 DSGVO) sowie des Rechts auf Datenübertragbarkeit (Art. 20 DSGVO)
- wenn die Verarbeitung auf einer wirksamen Einwilligung beruht, das Bestehen eines Rechts, die Einwilligung jederzeit zu widerrufen, ohne dass die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung berührt wird
- das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde
- ob die Bereitstellung der personenbezogenen Daten gesetzlich oder vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die personenbezogenen Daten bereitzustellen, und welche mögliche Folgen die Nichtbereitstellung hätte und
- ggf. das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling gemäß Artikel 22 Absätze 1 und 4 und – zumindest in diesen Fällen – aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person

**Hinweis:** werden die Daten nicht beim Betroffenen erhoben, also z.B. bei einer Auskunft angefragt, ist für die maßgeblichen informationspflichtigen Inhalte nicht auf den Art. 13, sondern auf den noch strengeren Art. 14 DSGVO abzustellen.

Zu beachten ist, dass im Einzelfall in Ansehung der verschiedenen Betroffenenrechte weitere Informationspflichten hinzukommen können, falls diese Rechte ausgeübt werden. Insofern existieren eine generelle Reaktionspflicht (s. unter B.III. 7.) und rechtsspezifische Auskunftspflichten. Für deren rechtskonforme Umsetzung bleibt es bei dem Erfordernis einer individuellen Kontaktaufnahme mit dem jeweils Betroffenen – auf die Datenschutzerklärung darf insofern gerade nicht zurückgegriffen werden.

## V. <sup>10</sup> Neue Dokumentationspflicht, Art. 30 DSGVO

Eine zusätzliche Erweiterung des Pflichtprogramm für datenschutzrechtliche Verantwortliche stellt Art. 30 DSGVO auf, der erstmalig zur Dokumentation sämtlicher Datenverarbeitungsprozesse anhält.

### 1.) Verpflichtende Verzeichnisse

Ab 2018 werden Verantwortliche somit grundsätzlich gehalten sein, **schriftlich oder elektronisch** (Abs. 3) Verzeichnisse zu anzulegen und zu führen, in welchen sämtliche der nachstehenden Angaben aufgeführt werden:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten
- die Zwecke der Verarbeitung
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

## 2.) Ausnahme: weniger als 250 Mitarbeiter und keine Verarbeitung sensibler Daten

Zu beachten ist aber, dass im Angesicht des erheblichen technischen und organisatorischen Aufwandes, welchen die Anlegung und stetige Aktualisierung der Verzeichnisse mit sich bringen wird, ein gesetzlicher Befreiungstatbestand etabliert wurde.

Nach Art. 30 Abs. 5 DSGVO entfalten die Dokumentationspflichten gegenüber Unternehmen keine Wirkung, die weniger als 250 Mitarbeiter beschäftigen und nicht mit der Erhebung und Verarbeitung besonders sensibler Daten im Sinne des Art. 9 DSGVO (etwa über die sexuelle Orientierung, ethnische Herkunft, Religion oder Weltanschauung etc.) befasst sind.

Weil im Online-Handel personenbezogene Daten regelmäßig nur erhoben werden, um die Durchführung von Kausalgeschäften und personen- und interessenbasierte Werbemaßnahmen zu ermöglichen, ohne dass den Betroffenen die Angabe besonders sensibler Daten abverlangt würde, wird der Großteil der kleinen und mittleren Marktakteure im elektronischen Geschäftsverkehr zur Dokumentation von Verarbeitungsvorgängen auch zukünftig nicht verpflichtet sein.

Anders verhält sich dies freilich bei Großunternehmen, welche die maßgebliche Grenze der Beschäftigtenzahl überschreiten.

## VI. Gelockerte Pflicht zur Bestellung von Datenschutzbeauftragten

Eine weitere maßgebliche Änderung wird das Datenschutzrecht zum 25.05.2018 durch eine Anhebung der Voraussetzungen für die verpflichtende Bestellung eines Datenschutzbeauftragten erfahren, in deren Zuge viele Verantwortliche im Online-Handel nicht mehr zwingend gehalten sein werden, einen solchen zur Überwachung der Einhaltung der gesetzlichen Datenschutzvorgaben einzuschalten.

Während nach dem geltenden §4f Abs. 1 Satz 1 und 4 BDSG ein Datenschutzbeauftragter bei einer nicht-öffentlichen, also vor allem gewerblichen Stelle schon immer dann zu bestellen ist, wenn mehr als neun Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind, wird diese Pflicht durch Art. 37 DSGVO entscheidend gelockert.

Nunmehr ist die Bestellung eines Datenschutzbeauftragten für nicht-öffentliche und vor allem gewerbliche Verantwortliche nur noch zwingend, wenn

- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonders sensibler Daten gemäß Artikel 9 DSGVO besteht

Insbesondere wird die personenmäßige Zahl der in einem Unternehmen mit Datenvorgängen Beschäftigten als pflichtauslösende Voraussetzung künftig entfallen.

Inwiefern der Online-Handel nach den neuen Anforderungen zukünftig als Tätigkeit eingestuft werden kann, die ob ihrer Art oder aufgrund des Umfangs von Datenverarbeitungsprozessen eine regelmäßige Überprüfung durch einen Beauftragten erforderlich macht, kann zu diesem Zeitpunkt zwar noch nicht abschließend gesagt werden.

Allerdings scheint vieles dafür zu sprechen, den E-Commerce, in welchem die Erhebung von personenbezogenen Daten primär zur Abwicklung von Kausalgeschäften und sekundär zu Werbezwecken erfolgt, ohne dass aber vollumfängliche oder besonders sensible personenbezogene Daten verarbeitet würden, von der Bestellungspflicht im Allgemeinen auszunehmen.

Freilich können aber die Masse und der Umfang der etablierten Datenverarbeitungsprozesse im konkreten Einzelfall auch den Online-Händler, der personenbezogene Daten über das übliche Maß hinaus nutzt, zur Bestellung eines Datenschutzbeauftragten nach Art. 37 DSGVO anhalten.

Abzuwarten bleibt insofern, dass der europäische Gesetzgeber die Kriterien, welche zur Ermittlung der art- und umfangsbasierten Überwachungsbedürftigkeit heranzuziehen und abzuwägen sind, in der Folgezeit noch konkretisiert.

Liegen die verschärften Voraussetzungen für die verpflichtende Bestellung nicht vor, soll es gemäß Art. 37 Abs. 4 DSGVO auch zukünftig jedem Verantwortlichen zur Disposition stehen, freiwillig einen Datenschutzbeauftragten zur Überwachung der Datenverarbeitungsprozesse einzuschalten.

## VII. Verschärfte Sanktionen bei Verstößen

Um der besonderen Bedeutung effektiver Datenschutzmaßnahmen zur Wahrung der legitimen Betroffeneninteressen zu mehr Geltung zu verhelfen und eine lückenlose Umsetzung der neuen Vorgaben mit Mitteln der Abschreckung zu garantieren, hebt die DSGVO den Bußgeldrahmen für Verstöße gegen die Ordnungsbestimmungen im Vergleich zur geltenden Rechtslage erheblich an und überschreitet hierbei erstmalig die Millionengrenze.

Während nach dem geltenden §43 Abs. 3 BDSG bisher Bußgelder in Höhe von die 300.000€ die (relative) Höchstgrenze bildeten, ergeht aus Art.83 DSGVO in Zukunft folgender Rahmen:

- Verstößt ein Verantwortlicher oder Auftragsverarbeiter gegen die Anforderungen der Prüfung und Absicherung von Minderjährigeneinwilligungen gemäß Art. 8 DSGVO, verletzt die Dokumentationspflicht des Art. 30 DSGVO oder handelt sonstigen organisatorischen und technischen Maßnahmen des 4. Kapitels zuwider, können Geldbußen bis zu **10 000 000 € oder in Höhe von 2% des Jahresumsatzes** des vorangegangenen Geschäftsjahres erhoben werden – und zwar je nach dem, welcher Betrag der höhere ist.
- Strafgelder bis zu **20 000 000€ oder 4% des Umsatzes** des letzten Geschäftsjahres können demgegenüber gefordert werden, wenn die Grundsätze für die Rechtmäßigkeit der Verarbeitung, einschließlich der Bedingungen für die Einwilligung gemäß den Art. 5, 6, 7 und 9 DSGVO verletzt werden oder ein Verantwortlicher oder sein Auftragsverarbeiter gegen die Regelungen über die Betroffenenrechte in Art. 12-22 DSGVO verstößt, also insbesondere seine Informations- und Handlungspflichten nicht umsetzt oder rechtswidrig die Abhilfe verweigert.

Daneben werden die Mitgliedsstaaten zudem nach Art. 84 DSGVO ermächtigt, Verstöße gegen weitere Tatbestände der DSGVO mit Bußgeldern zu belegen.

**Achtung:** Unabhängig von Bußgeldverfahren werden Verstöße gegen die DSGVO in Deutschland zukünftig auch über das in §2 Abs. 2 Nr. 11 UKlaG neu eingeführte Verbandsklagerecht von Verbraucherschutzverbänden, Wettbewerbszentralen und anderen. Stellen im Sinne des §3 UKlaG abgemahnt und verfolgt werden können.

## VIII. Fazit

Auch wenn die neue Datenschutzgrundverordnung (DSGVO), die zum 25.05.2018 in allen Mitgliedsstaaten verbindlich wird, in ihren Grundzügen und den maßgeblichen Datenschutzprinzipien mit dem in Deutschland bereits geltenden Recht übereinstimmt, führt sie speziell für den Online-Handel eine Reihe von maßgeblichen Veränderungen herbei, die sich vor allem in einer Ausweitung des datenschutzrechtlichen Pflichtprogramms und einer Stärkung der Betroffenenrechte niederschlagen.

Die Formulierungen neuer Berechtigungen wie derjenigen auf Datenübertragung, auf Unbetroffenheit von automatischen datenbasierten Entscheidungen und auf Widerspruch werden ebenso zur Anpassung der informationstechnologischen Systeme und Datenverarbeitungsstrukturen zwingen wie der Wegfall spezifischer Erlaubnistatbestände und die diesbezügliche Wiedereinführung eines Einwilligungserfordernisses.

Gleichzeitig ist eine vollständige Überholung und Neufassung der Datenschutzerklärung von Nöten, welche erstmalig auch über die Dauer der Datenspeicherung und ein Beschwerderecht bei der Aufsichtsbehörde aufklären muss.

Nachdruck wird dem Anpassungs- und Implementierungsbedarf hier vor allem durch stark verschärfte Bußgeldvorschriften verliehen, welche erstmals auch die Abschöpfung von Millionenbeträgen vorsehen.

Letztlich machen die einzelnen Novellierungen, welche in diesem Beitrag rechtsvergleichend und ausführlich dargestellt werden, plastisch, dass die Übergangsfristen auf den ersten Blick zwar lang bemessen erscheinen mögen, tatsächlich aber zwingend notwendig sind, um den Verantwortlichen eine rechtssichere und umfängliche Umstellung auf die reformierten Datenschutzvorgaben zu ermöglichen.

Bei weiteren Fragen zur neuen Datenschutzgrundverordnung und zur rechtskonformen Umsetzung der geänderten datenschutzrechtlichen Anforderungen steht Ihnen die IT-Recht Kanzlei gerne persönlich zur Verfügung.

Autor:

**RA Phil Salewski**

Rechtsanwalt