IN DIESEM KAPITEL

- erfahren Sie, wie Monster gemacht werden
- welche Art von Monster die DSGVO ist
- werden Sie erstaunt sein, wen das Monster alles beißen kann

Kapitel 1
Ein Monster namens DSGVO

Bereits im Dezember 2011 tauchte erstmals wie ein scheues Rehkitz ein geleakter Entwurf für eine Neuregelung des europäischen Datenschutzes in Form einer *Verordnung* im Internet auf. Bis dahin und noch einige Zeit länger galt in der EU die *Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr*, die im Jahr 1995 von der Europäischen Gemeinschaft (*EG*) erlassen worden war und die von den Mitgliedstaaten in nationale Gesetze umgesetzt werden musste.

Das geschah in den Mitgliedstaaten mit mehr oder weniger großer Begeisterung und einer beeindruckenden Vielfältigkeit, was das jeweils erreichte Datenschutzniveau anbelangt. Internationale Konzerne ließen sich deshalb einfach dort nieder, wo das Datenschutzniveau unterirdisch war. Die teils lächerlichen Geldbußen bei Datenschutzverstößen wurden als marginales, operationelles Risiko betrachtet. Besonders Staaten wie Irland und Luxemburg taten sich als Oasen eines nahezu unkontrollierten und grenzenlosen Verkehrs personenbezogener Daten hervor und zogen so Unternehmen aus aller Welt an. Erfahrungen hatten sie ja bereits als Steueroasen ausreichend gesammelt. Gewusst wie, konnten Datenschutzvorgaben so in ruhigen Gewässern und großer Gelassenheit umsegelt werden.

Das sollte sich aber ändern. Im Januar 2012 erfolgte offiziell die Vorstellung eines ersten Entwurfs eines neuen europäischen Datenschutzrechts durch die EU-Kommission. Der Entwurf wurde im Juni 2013 von den Innen- und Justizministern der Mitgliedstaaten der EU empört abgelehnt. Es dauerte bis zum Oktober 2013, bis im *Ausschuss für bürgerliche Freiheiten, Justiz und Inneres* (*LIBE*) des Europäischen Parlaments ein Kompromiss gefunden werden konnte über den wesentlichen Inhalt einer europäischen Datenschutzreform. Bis dahin hatte sich das scheue Rehkitz allerdings bereits zu einem ausgewachsenen Reh entwickelt und wurde zunehmend weniger scheu. Eine erste Lesung des neuen zweiten Entwurfs für eine Datenschutzgrundverordnung (*DSGVO*) erfolgte dann im März 2014 im Europäischen Parlament und wurde am Folgetag durch das Europäische Parlament veröffentlicht. Nach weiteren und langwierigen Verhandlungen kam es schließlich zu einem dritten

Entwurf. Dieser wurde im Juni 2015 durch den EU-Ministerrat veröffentlicht. Es wurde schnell klar, dass man es offenbar nicht mit einem Reh, sondern eher mit einem Elch zu tun bekommen würde. Gerüchte über ein *Recht auf Vergessenwerden*, *neue Löschpflichten*, umfassende *Betroffenenrechte* sowie *drakonische Sanktionen* bei Verstößen gegen die beabsichtigten neuen Vorschriften geisterten durch die Medien.

Schließlich begannen die ersten Trilog-Treffen, und im letzten davon, an einem 15. Dezember im Jahr 2015, konnte man sich auf einen finalen Stand einer DSGVO einigen. Am 25. Mai 2016 trat die DSGVO dann als *Verordnung (EU) 2016/679* in Kraft. Von Rehen oder Elchen wollte aber plötzlich niemand mehr reden. Stattdessen war von einem *Monster* die Rede, das Einzug in Behörden und Unternehmen in den Mitgliedstaaten halten würde.

Aber nicht nur in der EU begann man zu realisieren, dass es zu einem Paradigmen-Wechsel im europäischen Datenschutz gekommen war. Auch im außereuropäischen Ausland registrierte man bestürzt, dass die EU es mit dem Datenschutz nun offenbar wirklich ernst meinen würde. Denn auch Unternehmen, die keinen Sitz in einem europäischen Mitgliedstaat hatten, wurden durch die Vorschriften der DSGVO nun erbarmungslos mit Sanktionen bedroht, sollten Sie es – wie bisher – wagen, den europäischen Datenschutz weiterhin zu unterlaufen. Gnädig wurde allen noch eine zweijährige Frist bis zum 25. Mai 2018 gewährt, um die neuen Datenschutzvorgaben in die Praxis umzusetzen. Und seit diesem Zeitpunkt müssen alle *Adressaten*, sei es mit oder ohne Sitz in der EU, die Vorschriften der DSGVO einhalten. Willkommen in der *Monster AG*!

Wer alles *Adressat* der Vorschriften der DSGVO ist, erfahren Sie übrigens gleich weiter unten unter der Überschrift *Adressaten*.

Rechtliche Einordnung

Wenn *supranationale Einrichtungen* wie die *Vereinten Nationen* (*UNO*) oder die *Europäische Union* (*EU*) Vorschriften erlassen, handelt es sich – sie ahnen es sicher schon – um *supranationales Recht*. Staaten übertragen bestimmte Regelungsbefugnisse auf solche supranationalen Einrichtungen, geben ihre ursprünglich eigene Verfügungsgewalt damit auf und sind dann an die Entscheidungen der supranationalen Einrichtungen gebunden. Solche Entscheidungen können in einigen Fällen durch Beschlüsse dieser Organisationen gefasst werden. Es gibt aber auch Gesetzeswerke, die von solchen Einrichtungen erlassen werden und an die sich Mitgliedstaaten dann halten müssen. So ist es auch in der EU. Die Gesetzgebung der EU findet dabei einerseits statt durch *Richtlinien* und andererseits durch *Verordnungen*.

Richtlinien

Richtlinien tragen dem Umstand Rechnung, dass es sich bei den jeweiligen Mitgliedstaaten in der EU um teils völlig unterschiedlich strukturierte Staatsgebilde handelt. Allen gemein ist, dass es allesamt *Demokratien* sind. Demokratien können unterschiedlich ausgestaltet sein und sind es in Europa auch. In Frankreich existiert zum Beispiel eine *präsidiale Demokratie*, in Deutschland eine *parlamentarische Demokratie*. Deshalb ist das erste Mittel der Wahl des europäischen Gesetzgebers die Richtlinie. In einer Richtlinie werden erst einmal

nur bestimmte gesetzgeberische Ziele festgelegt, die die Mitgliedstaaten dann durch eigene Landesgesetze in anwendbares Recht umsetzen sollen.

Je nach Ausgestaltung der landestypischen Gesetzgebungsverfahren und Besonderheiten der Landesverfassungen sind die Mitgliedstaaten dabei entsprechend frei in der Umsetzung der gesetzten Zielvorgaben. Setzen Mitgliedstaaten die Vorgaben von Richtlinien nicht oder inhaltlich nur unzureichend um, kann die EU-Kommission ein sogenanntes *Vertragsverletzungsverfahren* nach Art. 258 des *Vertrags über die Arbeitsweise der Europäischen Union* (*AEUV*) einleiten. Das Verfahren ermöglicht der Kommission, den *Europäischen Gerichtshof* (*EuGH*) anzurufen, wenn sie der Meinung ist, dass ein Mitgliedstaat gegen eine Verpflichtung aus den Verträgen verstoßen hat (Art. 260 Abs. 1 AEUV). Ist das der Fall, endet das meist mit hohen Bußgeldern für die betroffenen Staaten.

Verordnungen

Da es aber immer wieder passiert, dass Mitgliedstaaten Richtlinien nur sehr zögerlich umsetzen oder listig Schlupflöcher finden, um die eigentlichen Ziele der Richtlinie zu unterwandern, sieht das europäische Datenschutzrecht auch *Verordnungen* vor. Verordnungen zeichnen sich dadurch aus, dass sie nicht mehr erst durch Gesetze der Mitgliedstaaten umgesetzt werden müssen, sondern nach ihrem Erlass und einer meist gewährten Übergangsfrist unmittelbar anzuwendendes Recht in jedem Mitgliedstaat der EU werden. Der Erlass von Umsetzungsgesetzen ist dann obsolet. Die Verordnung ersetzt dann entgegenstehende Gesetze vollständig. Wobei *vollständig* nicht ganz richtig ist. Verordnungen, wie auch die DSGVO, beinhalten oft sogenannte *Öffnungsklauseln*. Das sind Rechtsvorschriften, in denen es den Mitgliedstaaten erlaubt wird, bestimmte Regelungsinhalte noch zu *konkretisieren* durch eigene ergänzende Gesetze. Konkretisieren meint in diesem Zusammenhang, dass die Mitgliedstaaten zwar ergänzende Regelungen treffen dürfen. Sie dürfen dabei aber nur solche Regeln erlassen, die mit den Vorschriften der Verordnung harmonieren und diese nicht etwa durch die Hintertür heimlich aufweichen. Erlaubt sind nur noch schärfere Regelungen oder aber landestypische Spezifizierungen, aber keine Regelungen, mit denen Vorgaben einer Verordnung umgangen werden. Sollte das ein Mitgliedstaat trotzdem versuchen, droht auch hier ein *Vertragsverletzungsverfahren*.

In der DSGVO existieren *69 Öffnungsklauseln*, die es Mitgliedstaaten ermöglichen, *konkretisierende Gesetze* zu erlassen. Deutschland hat mit dem Erlass des *Bundesdatenschutzgesetzes* (*BDSG*) als einer der ersten Mitgliedstaaten ein entsprechendes Ergänzungsgesetz erlassen. Aber wer wissen will, wie Deutschland bestimmte Datenschutzthemen ergänzend regelt, der muss zusätzlich einen Blick in das BDSG werfen. Dasselbe gilt für die meisten Mitgliedstaaten der EU, die inzwischen entsprechende ergänzende Gesetze erlassen haben. In Deutschland wird zum Beispiel der *Beschäftigtendatenschutz*, die Anforderungen an die Benennung von *Datenschutzbeauftragten* oder die *Videoüberwachung* zusätzlichen Regelungen unterworfen. Je nachdem in welchem Mitgliedstaat Sie sich also befinden, sollten Sie nicht versäumen, einen Blick in die vorhandenen *nationalen Gesetze* zum Datenschutz zu werfen.

Zu Verordnungen greift die EU also, wenn sie konsequent bestimmte Vorgaben umsetzen will, ohne dies Mitgliedstaaten überlassen zu wollen. Wir dürfen Ihnen also hier vorstellen das allseits gefürchtete Monster, die berühmt-berüchtigte **VERORDNUNG (EU) 2016/679** DES EUROPÄISCHEN PARLAMENTS UND DES RATES *vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG,* auch bekannt unter dem Namen:

EU-Datenschutz-Grundverordnung

(im Folgenden kurz: **DSGVO**).

Gründe für die Notwendigkeit einer Datenschutzreform

Monster kommen nicht von ungefähr. Meistens werden sie gerufen. Zumindest wenn es nach dem Roman von *Larry Correia* geht (*Die Monster, die ich rief,* Köln 2017). Bei *Goethes Zauberlehrling* waren es noch Geister, aber mit Geistern erschreckt man heutzutage niemanden mehr. Das Monster DSGVO wurde gerufen durch

- ✔ die bis dato uneinheitliche Umsetzung der *Europäischen Datenschutz-Richtlinie 95/46/EG* in nationales Recht,
- ✔ den Umstand bis dahin national unabhängiger und eigenständiger Datenschutzaufsichtsbehörden,
- ✔ bis dahin nationale Sonderregelungen und ein unterschiedliches Datenschutzniveau in den Mitgliedstaaten und
- ✔ die schwierige Durchsetzbarkeit des europäischen Datenschutzstandards gegenüber Unternehmen mit Sitz in Drittländern.

Uneinheitliche Umsetzung der europäischen Datenschutz-Richtlinie 95/46/EG

Das europäische Datenschutzrecht basierte bis zum Erlass der DSGVO auf der europäischen Datenschutz-Richtlinie 95/46/EG. Wie es Richtlinien der EU so eigen ist, besitzen diese keinen unmittelbaren Charakter. Das bedeutet, dass die EU zwar Ziele vorgibt, die Umsetzung allerdings den Gesetzgebern der Mitgliedstaaten überlässt, wie sie diese umsetzen. Das geschieht dann in der Regel mit mehr oder minder großem Erfolg.

Das hatte zur Folge, dass manche Mitgliedstaaten die gesamte Wirtschaft ihres Lands durch pflichtgemäße Erfüllung der Datenschutzvorgaben in einen Wettbewerbsnachteil gegenüber solchen Unternehmen in solchen Staaten geführt haben, die die Gelegenheit nutzten, durch die nur rudimentäre Umsetzung des Datenschutzes Standortvorteile zu erzielen. Während in Deutschland selbst postalische Werbeschreiben einem pingeligen

Listenprivileg unterworfen waren, haben andere Staaten den dort ansässigen und dort steuerzahlenden Unternehmen gestattet, den Datenschutz nahezu vollständig zu unterwandern. Es ist also kein Wunder, dass Unternehmen wie *Microsoft* oder *Amazon* ihre europäischen Niederlassungen in Irland oder Luxemburg eingerichtet hatten. In einem Staat, der in seiner Hauptstadt am Bahnhof Listen der Passagiere für Züge für alle sichtbar aushängt unter Angabe des Reiseziels und in dem diese Personen dann bei Eintreffen des Zugs auch noch persönlich auffordert werden, einzusteigen, bei dem lässt es sich als Big-Data-Unternehmen fein leben. Mit der Einführung der DSGVO sollen jetzt derartige Abstrusitäten unterbunden und ein einheitliches Datenschutz-Niveau in der gesamten EU sichergestellt werden.

National unabhängige und eigenständige Datenschutzaufsichtsbehörden

Ein grandioses Beispiel für die bis zur Einführung der DSGVO unabgestimmte Vorgehensweise der *Aufsichtsbehörden* untereinander lässt sich einer gemeinsamen Veröffentlichung des Autors mit Harald Bolsinger entnehmen (Bolsinger, Harald/Szidzek, Christian: Datensouveränität und Vertrauen, 2018). Über viele Jahre hinweg hatte Harald versucht, seine über ihn gespeicherten Daten bei Amazon löschen zu lassen. Der Erfolg war mehr als bescheiden. Besonders beeindruckend war dabei aber das Auftreten der bayerischen und luxemburgischen Aufsichtsbehörden, die sich jeweils konsequent für unzuständig erklärten, und das nach damaliger Gesetzeslage noch nicht einmal zu Unrecht. Dass Unternehmen versuchen, sich bestmögliche Bedingungen zu schaffen, ist nachvollziehbar. Oft ist der Geschäftsführer oder Vorstand nicht auch zugleich der Eigentümer des Unternehmens, und Aufgabe von angestellten Geschäftsleitern ist es nun einmal, den Profit zu optimieren. Dass aber Aufsichtsbehörden in dasselbe Horn bliesen, war erstaunlich.

Wenn Sie wissen wollen, wie die Zuständigkeiten der Aufsichtsbehörden nach DSGVO geregelt sind, blättern Sie einfach schon einmal vor zu Kapitel 4 *Die Protagonisten* unter der Überschrift *Die Aufsichtsbehörden*.

Nationale Sonderregelungen – unterschiedliches Datenschutzniveau in den Mitgliedstaaten

Die *Datenschutz-Richtlinie 95/46/EG* hatte zur Folge, dass die Mitgliedstaaten pflichtgemäß Gesetze zu ihrer Umsetzung erließen, einige besonders pfiffige Staaten dabei aber schnell witterten, dass ein besonders abgründiges Datenschutzniveau ihnen den Zulauf internationaler Konzerne ermöglichen würde, wo die eigene Infrastruktur das ansonsten nicht hergegeben hätte. Während also einige Mitgliedstaaten der EU versuchten, die Ziele der Richtlinie bestmöglich umzusetzen, versuchten andere es damit, die Ziele bestmöglich zu unterwandern und sich dadurch einen regionalen Vorteil zu verschaffen. Das gelang auch über viele Jahre hinweg recht gut. Die Folge war, dass Unternehmen, die Geschäfte mit personenbezogenen Daten in der EU machen wollten, sich dort niederließen, wo das Datenschutzniveau am niedrigsten war. Man nennt das *Forum-Shopping*. Dass dies für den europäischen Datenschutz nicht gerade förderlich war, liegt auf der Hand. Und es war seit

Jahren absehbar, dass die Mitgliedstaaten, die versucht hatten, die Datenschutz-Richtlinie effektiv umzusetzen, nicht mehr vorhatten, sich länger auf der Nase herumtanzen zu lassen von den schwarzen Schafen in Ihren Reihen, die ja nicht nur im Datenschutz verhaltensauffällig geworden waren, sondern auch, wenn es um Steuern ging und andere rechtliche Schlupflöcher.

Durchsetzbarkeit des europäischen Datenschutzstandards

Abgesehen vom Problem des *Forum-Shoppings* war es auf Basis der vormaligen *Richtlinie 95/46/EG* auch nicht möglich, Unternehmen datenschutzrechtlich zur Verantwortung zu ziehen, die keinen Sitz in einem Mitgliedstaat der EU hatten, aber dort trotzdem Waren und Dienstleistungen anboten. Das führte dazu, dass solche Unternehmen gegenüber den in der EU ansässigen Unternehmen einen deutlichen Wettbewerbsvorteil verzeichnen konnten, da sie sich um die europäischen Datenschutzvorschriften nicht kümmern mussten. Es galt ausschließlich das sogenannte *Territorialprinzip*. Demzufolge waren Unternehmen mit Sitz in *Drittstaaten* im Wesentlichen vom europäischen Datenschutzsystem ausgenommen. Das hat sich nun mit der DSGVO und der zusätzlichen Einführung des *Marktortprinzips* geändert. Dazu unten gleich mehr.

Welche Länder seit der Einführung der DSGVO als *Drittstaaten* gelten und unter welchen Voraussetzungen Unternehmen, die dort ihren Sitz haben, an die Vorschriften der DSGVO gebunden sind, erfahren Sie weiter unten unter der Überschrift *Räumlicher Anwendungsbereich*.

Ziele der Reform

Wenn es schon die Notwendigkeit gab, das europäische Datenschutzrecht zu reformieren, weshalb dann nicht aus der Not gleich eine Tugend machen? So ungefähr muss sich der europäische Gesetzgeber das gedacht haben und hat deshalb gleich ein paar weitere Ziele mit in den Blick genommen, die mit dem Inkrafttreten der DSGVO erreicht werden sollten. Diese Ziele sind

- ✔ mehr Kontrolle Betroffener über ihre Daten
- ✔ das Setzen globaler Standards für den Datenschutz sowie
- ✔ die Festlegung einheitlicher Datenschutzregeln für den digitalen Binnenmarkt.

Mehr Kontrolle Betroffener über ihre Daten

Betroffene Personen, deren Daten Gegenstand von Verarbeitungen in Unternehmen, Behörden oder sonstigen Einrichtungen – die DSGVO spricht von *Verantwortlichen* (Art. 4 Nr. 7) – sind, sollen durch die DSGVO mehr Kontrolle über das Schicksal ihrer Daten erhalten, als das nach alter Rechtslage noch der Fall war. Aus diesem Grund wurde in die Artikel

12 bis 22 gleich ein ganzer Katalog an neuen Betroffenenrechten aufgenommen. Diese reichen von *Auskunftsansprüchen* über *Berichtigungsrechte* bis hin zu einem *Recht auf Datenlöschung* und *Vergessenwerden*.

Welche Rechte Betroffene im Einzelnen haben und wie Sie diesen gegebenenfalls nachkommen müssen, können Sie in Kapitel 8 *Die Waffen der Betroffenen* ganz ausführlich nachlesen.

Setzen globaler Standards für den Datenschutz

Durch die Einführung des jetzt zusätzlich geltenden *Marktortprinzips* ist es nun möglich, auch solche Unternehmen dem Regime des europäischen Datenschutzes zu unterwerfen, die ihren Sitz außerhalb der EU oder des Europäischen Wirtschaftsraums haben. Dazu gleich mehr unten unter der Überschrift *Räumlicher Anwendungsbereich*. Damit wird das europäische Verständnis von Datenschutz weit über die Territorialgrenzen der EU hinaus transportiert.

Einheitliche Datenschutzregeln für den digitalen Binnenmarkt

Durch die *unmittelbare Anwendbarkeit* der DSGVO in allen Mitgliedstaaten der EU sollten einheitliche Datenschutzregeln für den digitalen europäischen Binnenmarkt geschaffen und Wettbewerbsnachteile, die durch die unterschiedlichen nationalen Datenschutzgesetze bewusst oder unbewusst geschaffen wurden, wieder ausgeglichen werden. Die EU-Kommission schätzt, dass durch die Vereinheitlichung der unterschiedlichen Datenschutzregeln auf Dauer gesehen jährlich Einsparungen in Höhe von rund 2,3 Milliarden Euro möglich sind. Gefühlt waren es für Unternehmen zwar bislang eher zusätzliche Ausgaben als Einsparungen, aber vielleicht ist das ja auch nur zu kurzfristig gedacht. Nach den Folgen der Französischen Revolution gefragt, antwortete etwa der damalige chinesische Premierminister *Tschou En-lai* im Jahr 1972, es sei zu früh, dies zu beurteilen. Es kommt wahrscheinlich darauf an, in welchen Zeiträumen man denkt.

Inhalt

Die DSGVO regelt die Pflichten von Behörden, Unternehmen, sonstigen Einrichtungen, aber auch von privaten Verantwortlichen beim Umgang mit personenbezogenen Daten. Zusätzlich wird ein umfassendes und effizientes Aufsichtswesen etabliert, das einerseits einer konsequenten Umsetzung der Vorgaben der DSGVO verpflichtet ist, zugleich aber auch eine einheitliche Auslegung der Vorschriften auf der gesamten europäischen Ebene sicherstellen soll.

Erwägungsgründe

Wenn Sie die DSGVO das erste Mal aufschlagen, werden Sie überrascht sein. Bevor Sie auch nur den ersten Artikel der DSGVO zu Gesicht bekommen, stehen dort erst einmal

genau 173 sogenannte *Erwägungsgründe*, durch die Sie sich durchquälen können. Aber seien Sie beruhigt, das müssen Sie nicht, wenn Sie wissen wollen, was die DSGVO regelt. Der eigentliche Verordnungstext beginnt nämlich erst bei Art. 1.

Als *Erwägungsgründe* bezeichnet man Erläuterungen, die Gesetzestexten vorangestellt werden, um die Überlegungen nachvollziehbar zu machen, die zum Erlass der sich dann anschließenden und wirklich rechtsverbindlichen Regelungen geführt haben.

Sich die Erwägungsgründe durchzulesen, ist hilfreich, weil sie einen Eindruck vermitteln, warum der Verordnungsgeber welche Regeln erlassen hat. Leider enthalten die Erwägungsgründe der DSGVO aber keine Verweise auf die Vorschriften, auf die sie sich beziehen und umgekehrt. Das macht es nicht gerade leicht.

Wenn Sie mit dem Text der DSGVO arbeiten, suchen Sie sich am besten eine *Edition*, bei der den jeweiligen Artikeln der DSGVO die dazugehörenden *Erwägungsgründe zugeordnet* sind. Im Internet finden Sie verschiedene solcher Editionen über die einschlägigen Suchmaschinen. So wissen Sie immer gleich, was sich der Verordnungsgeber so dachte, als er bestimmte Vorschriften in die Verordnung aufgenommen hat.

Verordnungstext

Die DSGVO besteht aus 99 Artikeln. Wenn wir Ihnen in diesem Dummies-Buch nun den gesamten Text der DSGVO abdruckten, würden Sie sich zu Recht darüber ärgern, dass Sie viel Geld bezahlt haben für einen Verordnungstext, der in sämtliche Sprachen der Mitgliedstaaten übersetzt frei im Internet verfügbar ist. Aus diesem Grund sehen wir mit Ihrem mutmaßlichen Einverständnis an dieser Stelle davon ab. Wenn Sie sich aber näher mit der DSGVO befassen wollen, kommen Sie nicht daran vorbei, sich einen Verordnungstext zuzulegen und dort den einen oder anderen wichtigen Hinweis zu kommentieren.

Sie finden den Volltext auf der EUR-Lex-Seite der EU unter: `https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=celex%3A32016R0679` oder Sie geben einfach die Suchbegriffe *DSGVO*, *Text, EUR-Lex* in eine beliebige Suchmaschine ein und werden auch so fündig.

Unmittelbare Anwendbarkeit

Da es sich bei der DSGVO um eine *Verordnung* der EU handelt, müssen die Vorschriften in jedem Mitgliedstaat genauso angewendet werden, als hätte der Mitgliedstaat das Gesetz selbst erlassen. Das unterscheidet die Verordnung von der *Richtlinie*. Mit Inkrafttreten der DSGVO gab es aber außer der Vereinheitlichung noch einen weiteren *Paradigmenwechsel*: Die DSGVO ist nämlich zusätzlich auch noch *vorrangig* vor *nationalem Recht* anzuwenden. Das war bis zu ihrem Erlass anders. Bis dahin galt das sogenannte *Subsidiaritätsprinzip*. Das damalige Datenschutzrecht war erst dann anzuwenden, wenn es keine anderen Gesetze gab, auf die man sich stützen konnte. Erst wenn es eine Regelungslücke gab, kam das

Datenschutzrecht zur Anwendung. Das *Datenschutzrecht* der DSGVO ist jetzt immer *vorrangig* anzuwenden, und Gesetze von Nationalstaaten, die im Widerspruch zu den Regelungen der DSGVO stehen, dürfen nicht mehr weiter angewendet werden. Das ist auch der Grund, weshalb die Gesetzgeber der Mitgliedstaaten im Jahr 2020 noch immer mit Hochdruck daran arbeiten, Hunderte von nationalstaatlichen Gesetzen anzupassen, die sich mit der DSGVO nicht in Einklang bringen lassen. Nur in Ausnahmefällen und wenn die DSGVO es ausdrücklich erlaubt, können die Mitgliedstaaten speziellere Gesetze erlassen. Da die DSGVO 69 sogenannte *Erfüllungsklauseln* beinhaltet, also Regelungen, bei denen dem nationalen Gesetzgeber der Mitgliedstaaten erlaubt wird, konkretisierende Gesetze zu erlassen, müssen Sie auch immer zugleich noch einen ergänzenden Blick in die Ausführungsgesetze Ihres jeweiligen Mitgliedstaats werfen. Wenn dort ergänzende Gesetze erlassen worden sind, müssen Sie auch diese einhalten.

Und auch das ist noch nicht ganz ausreichend. Es gilt noch die *Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr*, die von den Mitgliedstaaten in vielen Einzelgesetzen in nationales Recht umgesetzt wurde. Sie gilt für Regelungsbereiche, die von der DSGVO nicht abschließend geregelt sind. Das betrifft vor allem Vorschriften über *Telekommunikation* und *Telemedien* sowie den Umgang mit personenbezogenen Daten bei *Diensten der Informationsgesellschaft*. Irgendwann in weiter Ferne wird vielleicht einmal die längst schon für die Vergangenheit angekündigte *E-Privacy-Verordnung* erlassen werden, die sich dieser Themen annehmen soll. Ursprünglich war geplant, die E-Privacy-Verordnung gleichzeitig mit der DSGVO in Kraft treten zu lassen, da sich beide Verordnungen gegenseitig ergänzen sollten. Intensiver Lobby-Arbeit der Big-Data-Branche ist es zu verdanken, dass beide Verordnungen nun erst zeitlich versetzt in Kraft treten können. Wenn die E-Privacy-Verordnung eines Tags einmal in Kraft sein sollte, dann müssen Sie neben der DSGVO also auch diese beachten.

Und dann gibt es da noch Art. 40, der es erlaubt, rechtsverbindliche *Verhaltensregeln* für kleinere oder mittelständische Unternehmen zu erlassen, und es sogar Verbänden ermöglicht, solche Verhaltensregeln selbst auszuarbeiten. Um rechtsverbindlich zu werden, müssen die Verhaltensregeln jedoch zuvor von den Aufsichtsbehörden genehmigt werden. Aktuell hat sich hier allerdings noch nichts Nennenswertes getan. Beobachten sollten Sie das aber schon.

Sie sehen also, die DSGVO ist die Herrin des europäischen Datenschutzrechts, aber in der Praxis müssen Sie sich zusätzlich leider auch noch durch viele ergänzende und weitere konkretisierende Vorschriften quälen.

Am besten gehen Sie die Vorschriften in der folgenden Reihenfolge durch, wenn Sie nichts übersehen wollen.

- ✔ Vorschriften der E-Privacy-VO als Spezialregelung (nach Inkrafttreten)
- ✔ Vorschriften der DSGVO
- ✔ Nationales Umsetzungsgesetz zur Richtlinie 2000/31/EG über den elektronischen Geschäftsverkehr
- ✔ Ergänzende Gesetze Ihres Mitgliedstaats, die aufgrund von Öffnungsklauseln der DSGVO erlassen worden sind

- ✔ Verhaltensregeln nach Art. 40 (soweit vorhanden)
- ✔ Vertragliche Verpflichtungen im Rahmen einer Auftragsverarbeitung (siehe dazu Näheres in Kapitel 7 *Zusammenarbeit von Unternehmen* unter der Überschrift *Die Auftragsverarbeitung*

Adressaten

Adressaten von Vorschriften sind immer diejenigen, an die sich eine Vorschrift richtet. Wenn Sie Jude sind, braucht Sie das Neue Testament nicht zu interessieren, als Christ wäre das allerdings zu empfehlen, wenn Sie nicht in die Hölle kommen wollen. Das Fegefeuer soll ja inzwischen abgeschafft sein. Ebenso wenig muss Sie als Buddhist der Koran interessieren oder als Muslim die Veden. So ist es auch bei der EU-Gesetzgebung. Wenn Sie nicht Adressat der Vorschrift sind, braucht Sie die Vorschrift auch nicht weiter zu kümmern, es sei denn, Sie sind Lobbyist. Adressaten der DSGVO sind *Verantwortliche* und *Auftragsverarbeiter*.

Wann Sie *Verantwortlicher* sind und wann Sie zum *Auftragsverarbeiter* werden, erfahren Sie in Kapitel 4 *Die Protagonisten*. Im Wesentlichen geht es darum, dass Sie geschäftsmäßig irgendwie personenbezogene Daten verarbeiten und das nicht nur für private Zwecke tun.

Adressaten der DSGVO sind zunächst einmal

- ✔ öffentliche und
- ✔ nicht öffentliche Stellen

Öffentliche Stellen

Öffentliche Stelle ist nicht gleich jeder, der ein YouTube-Video veröffentlicht oder nachts im Suff peinliche Leserbriefe oder Kommentare schreibt.

Begriff

Wenn von *öffentlichen Stellen* die Rede ist, sind damit in der Regel *Behörden* oder *Gerichte* gemeint. Aber auch *Stiftungen* oder andere *Vereinigungen*, die *staatlich getragen* sind, zählen dazu. Je nachdem was die Mitgliedstaaten national geregelt haben, kann es auch vorkommen, dass Notare oder Rechtsanwälte als öffentliche Stellen gelten.

Ausnahmen

Ausdrücklich ausgenommen vom Geltungsbereich der DSGVO sind folgende öffentliche Stellen:

- ✔ Organe, Einrichtungen, Ämter oder Agenturen der *EU* (Art. 2 Abs. 3),
- ✔ Mitgliedstaaten bei Tätigkeiten gemeinsamer Außen- und Sicherheitspolitik (Art. 2 Abs. 2 b),

- ✔ zuständige Behörden zur Verhütung, Aufdeckung, Untersuchung oder Verfolgung von Straftaten und
- ✔ Behörden, die zuständig sind für die Vollstreckung von Strafen oder zum Schutz der öffentlichen Sicherheit vor Bedrohungen (Art. 2 Abs. 2 d).

Wundern Sie sich jetzt bitte nicht, wenn die Einrichtungen der EU sich nicht an die DSGVO halten müssen. Man hat ja schon alle Hände voll zu tun, Verordnungen wie die DSGVO überhaupt zu erlassen. Wenn man sich jetzt selbst auch noch an die selbst gemachten Vorschriften halten müsste, käme man ja gar nicht mehr zum Arbeiten.

Nicht öffentliche Stellen

Was *nicht öffentliche Stellen* sind, ist schnell erklärt. Das sind alle, die keine *öffentliche Stellen* sind. Also Sie und ich sowie Unternehmen, Vereine oder sonstige Zusammenschlüsse von Personen im *zivilrechtlichen* Bereich.

Haushaltsausnahme

Die DSGVO bemüht sich darum, geschäftsmäßige und private Datenverarbeitung auseinanderzuhalten. Wenn Sie sich Sorgen machen sollten, ob Sie Ihr Familienalbum weiterführen dürfen oder nicht, können wir Sie beruhigen. Das dürfen Sie. Sie dürfen auch gerne weiter in Ihren sozialen Netzwerken jeden Blödsinn posten, solange Sie das *ausschließlich zu persönlichen oder familiären Zwecken* machen. Es gibt nämlich die sogenannte *Haushaltsausnahme* nach Art. 2 Abs. 2 c. Um von der Haushaltsausnahme Gebrauch machen zu können, müssen Sie als Erstes einmal eine *natürliche* Person sein oder mit anderen Worten ein Mensch. Ob Sie auf natürlichem oder unnatürlichem Weg zustande gekommen sind oder Sie geklont wurden oder sich gar selbst geklont haben, ist dabei völlig egal. Wenn Sie zu dem Ergebnis gekommen sind, dass es sich bei Ihnen um einen Menschen handelt, dann erlaubt Ihnen die DSGVO personenbezogene Daten für *persönliche* oder *familiäre* Zwecke zu verarbeiten, ohne sich um Datenschutz besonders kümmern zu müssen. Allerdings dürfen Sie dabei den persönlichen und familiären Lebensbereich nicht verlassen. Falls doch: DSGVO.

Der persönliche oder familiäre Lebensbereich ist schnell überschritten! Zusammengefasst kann man sagen, dass das immer dann der Fall ist, wenn Sie Ihre *Privatsphäre* verlassen und anfangen, Daten von Leuten zu verarbeiten, die sich außerhalb dieser Privatsphäre befinden. Und das ist immer dann schon der Fall, wenn Sie diejenigen, deren Daten Sie verarbeiten, nicht kennen. Oder wenn Sie Daten von Leuten, die sie kennen und zu Ihrem persönlichen oder familiären Lebensbereich zählen, plötzlich anderen gegenüber offenlegen, die nicht in diesen Bereich gehören. Die Abgrenzung ist aber oft nicht leicht.

Besonders vorsichtig müssen Sie sein, wenn Sie in *sozialen Netzwerken* aktiv sind. Solange nur ein *begrenzter Personenkreis* auf die Daten zugreifen kann, gilt die Haushaltsausnahme. Wenn aber ein *unbestimmter Personenkreis* auf die Daten zugreifen kann, gilt die Ausnahme *nicht*! Auch die Begrenzung auf Gruppen ist in diesen Netzwerken oft nicht ausreichend, um von der Ausnahme Gebrauch machen zu können. Und natürlich schon gar nicht greift die Ausnahme, wenn Sie mit der Datenbereitstellung wirtschaftliche oder sonst geschäftsmäßige Zwecke verfolgen.

Bei der *Videoüberwachung* Ihrer privaten Lebensbereiche können Sie sich meist auf die Haushaltsausnahme berufen. Das gilt aber dann schon wieder nicht, wenn ein öffentlicher Bereich wie Straße, Bürgersteig oder angrenzende Parks und Nachbargrundstücke von der Überwachung erfasst werden. Die Haushaltsausnahme gilt auch nicht bei der Nutzung von *Dashcams* oder *Drohnen*, wenn Sie dabei fremde Personen filmen.

Sachlicher Anwendungsbereich der DSGVO

Der *sachliche Anwendungsbereich* der DSGVO ist nach Art. 2 DSGVO eröffnet für die geschäftsmäßige Verarbeitung *personenbezogener Daten*. die

- ✔ automatisiert oder
- ✔ nicht automatisiert stattfindet.

Verarbeitung personenbezogener Daten

Nur wenn Sie personenbezogene Daten verarbeiten, müssen Sie sich an die DSGVO halten, sonst nicht. Aber Moment, Sie wissen ja noch gar nicht, was im Datenschutz alles unter der Bezeichnung *personenbezogene Daten* verstanden wird. Das ist natürlich nachvollziehbar, denn wir erklären Ihnen das ja im Detail auch erst in den folgenden Kapiteln. An dieser Stelle sei aber schon einmal so viel verraten, dass es sich bei personenbezogenen Daten um Informationen über Menschen handelt. Das beginnt mit dem Namen, der Wohnanschrift, dem Familienstand und endet bei verschiedenen kryptischen Ziffern- und Buchstabenkombinationen, über die sich ein Personenbezug herstellen lässt. Manchmal lässt sich nicht leicht auseinanderhalten, ob bestimmte Informationen zu den personenbezogenen Daten gehören oder nicht. Deshalb ist den personenbezogenen Daten in diesem Dummies-Buch ein eigenes Kapitel gewidmet.

Blättern Sie gerne schon einmal vor zu Kapitel 2 *Personenbezogene Daten*, wenn Sie Genaueres zu personenbezogenen Daten wissen wollen!

Unter der Bezeichnung *Verarbeitung* versteht man übrigens laut Definition in Art. 4 Nr. 2, alles das, was Sie irgendwie mit *personenbezogenen Daten* machen können. Dazu zählen das *Erheben*, das *Erfassen*, die *Organisation*, das *Ordnen*, die *Speicherung*, die *Anpassung* oder *Veränderung*, das *Auslesen*, das *Abfragen*, die *Verwendung*, die *Offenlegung* durch Übermittlung, die *Verbreitung* oder eine andere Form der *Bereitstellung*, der *Abgleich* oder die *Verknüpfung*, die *Einschränkung* sowie das *Löschen* oder die *Vernichtung*. Also kurz gesagt, alles, was man mit Daten so anstellen kann.

Automatisierte Verarbeitung

Wenn Sie geschäftsmäßig personenbezogene Daten verarbeiten, kommt es zusätzlich darauf an, *wie* Sie diese Daten verarbeiten. Sobald die Verarbeitung *automatisiert* stattfindet, gilt die DSGVO. Darunter versteht man die *digitale* Datenverarbeitung.

Nicht automatisierte Verarbeitung

Abgesehen von der *automatisierten* Verarbeitung ist die DSGVO auch anwendbar bei der *nicht automatisierten* Verarbeitung. Das ist jedenfalls dann der Fall, wenn bei der nicht automatisierten Verarbeitung personenbezogene Daten in einem *Dateisystem* gespeichert werden. Damit meint man in erster Linie die Verarbeitung personenbezogener Daten in *Papierform*. Es könnte aber auch sein, dass Sie kein Papier benötigen und stattdessen in der Lage sind, in Ihrem *Kopf* personenbezogene Daten in einem *Dateisystem* zu speichern. Dann müssten wir Ihr Gehirn künftig leider auch regelmäßigen Datenschutzkontrollen unterziehen. Sollte das der Fall sein, melden Sie das also bitte dringend bei Ihrer zuständigen Aufsichtsbehörde!

Unter der Bezeichnung *Dateisystem* versteht die DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien sortiert sind.

Nach *Erwägungsgrund 15* sind lediglich solche Akten oder Aktensammlungen von dem Anwendungsbereich der DSGVO ausgenommen, die *nicht nach bestimmten Kriterien geordnet* sind.

Kommen Sie aber um Gottes Willen jetzt nicht auf den Gedanken, Ihre papierhaft gespeicherten Daten deshalb gleich alle wahllos durcheinanderzuwerfen, nur um der DSGVO einen Streich zu spielen! Das könnte zwar funktionieren. Sie könnten mit Ihren Daten dann aber wahrscheinlich auch nichts mehr anfangen. Außerdem hilft es auch nicht, denn wenn Sie die Daten bereits einmal in einem Dateisystem gespeichert hatten, gilt: *Einmal Dateisystem, immer Dateisystem*.

Räumlicher Anwendungsbereich

Mit der Einführung der DSGVO gelten im Datenschutz jetzt das oben bereits erwähnte *Niederlassungsprinzip* und das sogenannte *Marktortprinzip* erstmalig nebeneinander. Auf den folgenden Seiten erfahren Sie, wann das Niederlassungsprinzip gilt und wann das Marktortprinzip.

Niederlassungsprinzip

Immer dann, wenn Sie *in der EU niedergelassen* sind und dort Ihre Tätigkeit entfalten und *nicht* der *Haushaltsausnahme* unterfallen, hat *Sauron* in Gestalt der Aufsichtsbehörden ein wachsames Auge auf Sie.

In welcher Gestalt Sauron Ihnen erscheinen wird, können Sie weiter unten in Kapitel 4 *Die Protagonisten* unter der Überschrift *Die Aufsichtsbehörden* nachlesen.

Dabei ist es egal, ob Sie Daten von EU-Bürgern verarbeiten oder Daten von Bürgern anderer Staaten. Wenn Sie in der EU ansässig sind, müssen Sie sich an die DSGVO halten. Maßgebend ist allein, ob Sie in der EU Ihren Sitz haben oder nicht. Man nennt das *Territorialprinzip*. Es kann aber auch passieren, dass Sie Ihren Sitz außerhalb der EU haben und sich trotzdem an die DSGVO halten müssen. Dazu gleich mehr unter der Überschrift *Marktortprinzip*. Das *Niederlassungsprinzip* – auch oft als *Territorialprinzip* bezeichnet – besagt also nichts anderes, als dass Unternehmen oder sonstige Organisationen, die sich in der EU *niedergelassen* haben, an die DSGVO halten müssen. Das ist nachvollziehbar. Was aber viele nicht so richtig wissen, ist, *wann* sie sich in der EU niedergelassen haben.

In der EU niedergelassene Unternehmen

Die DSGVO gilt also zunächst einmal für alle Unternehmen, die in der EU *niedergelassen* sind (Art. 3 Abs. 1).

Niederlassung bedeutet nicht *Hauptsitz* oder *Hauptverwaltung*, sondern nach *Erwägungsgrund 22* genügt eine *effektive und tatsächliche Ausübung einer Tätigkeit durch eine feste Einrichtung*. Die Rechtsform ist also nicht ausschlaggebend. Es ist egal, ob es sich bei Ihrer Niederlassung nur um eine Filiale oder gleich um ein eigenständiges Unternehmen mit einer bestimmten Rechtsform wie einer GmbH, AG oder Ähnlichem handelt. Selbst ein einzelner Vertreter kann Sie ohne Weiteres in der EU repräsentieren. Wenn Sie also innerhalb der EU wirtschaftlich tätig werden und irgendjemand Sie hier repräsentiert, haben Sie eine Niederlassung in der EU. Und nicht nur das. Sie haben auch eine schöne DSGVO, an die Sie sich jetzt halten müssen.

Konzernstrukturen

Was aber gilt, wenn mehrere selbstständige Organisationen oder Unternehmen mit jeweils *eigener Rechtsperson* in einer Konzernstruktur zusammengeschlossen sind?

Nehmen wir zum Beispiel einmal an, Ihr Konzern besteht zunächst aus einer Konzernmutter in Form einer *Aktiengesellschaft* (*AG*) beziehungsweise dem entsprechenden US-amerikanischen Pendant, also einer *Corporation*, mit Sitz in den USA. Diese Konzernmutter ist wiederum als herrschendes Unternehmen mit jeweils mehr als 50 Prozent an weiteren Unternehmen beteiligt, zum Beispiel verschiedenen Gesellschaften mit beschränkter Haftung (*GmbH*). Die eine GmbH sitzt in Singapur, eine andere in der Schweiz und eine klitzekleine GmbH sitzt in … sagen wir Spanien. Muss sich jetzt wegen dieser klitzekleinen GmbH mit Sitz in Spanien auch die Konzernmutter in den USA an die DSGVO halten? Lösung gleich unten.

Bereits vor Inkrafttreten der DSGVO musste sich der *Europäische Gerichtshof* (*EuGH*) mit der Frage befassen, wann bei Konzernstrukturen von *Niederlassungen* auszugehen sei. Es handelt sich dabei um die sogenannte *Google-Spain-Entscheidung* vom Mai 2014 (Rechtssache C-131/12). Es ging dabei um die Frage, ob das europäische Datenschutzrecht auch für das damals in den USA ansässige Mutterunternehmen *Google Inc*. anwendbar sei, obwohl das Mutter-Unternehmen in Europa lediglich Gesellschafter des selbstständigen Tochterunternehmens *Google Spain SL* war, aber selbst weder Büros noch andere eigene Zweigstellen in der EU unterhielt. Dass das Tochterunternehmen Google Spain SL vom europäischen Datenschutz erfasst war, stand außer Frage, denn das Unternehmen hatte seinen Sitz ja in Spanien und fiel damit über das *Niederlassungsprinzip* ganz automatisch unter das europäische Datenschutzrecht. Aber was war mit dem Mutterunternehmen in den USA? Konnte die rechtlich selbstständige *Google Spain SL* als *Niederlassung* von *Google Inc.* verstanden werden, mit der Folge, dass das europäische Datenschutzrecht auch für *Google Inc.* Geltung beanspruchen könne? Der EuGH hat das seinerzeit bejaht, weshalb Datenschützer davon ausgehen, dass er dies auch künftig nicht anders sehen wird. Der EuGH entschied, dass es für die Annahme einer *Niederlassung* in der EU ausreiche, dass die selbstständige Tochtergesellschaft in Spanien als *feste Einrichtung eine Tätigkeit* ausübe. Außerdem seien die Tätigkeiten der beiden Unternehmen untrennbar miteinander verbunden. Zwar fördere *Google Spain SL* als Vertriebsunternehmen *Google Inc*. in den USA nur wirtschaftlich. Ohne die Suchmaschinen-Dienstleistung von *Google Inc.* gäbe es jedoch kein Geschäft für *Google Spain SL*. Dies genüge, um die Muttergesellschaft in den USA mit der Pflicht zur Anwendung des europäischen Datenschutzrechts zu *infizieren*. Aber dabei bleibt es nicht. In weiteren Urteilen, wie zum Beispiel *Weltimmo* vom 01.10.2015 und Amazon vom 28.07.2016, stellte der EuGH klar, dass selbst ein *einzelner Vertreter* eines außereuropäischen Unternehmens – vorausgesetzt, es gebe einen gewissen Grad an *Beständigkeit* und eine *effektive Ausübung* der wirtschaftlichen Tätigkeit – als *Niederlassung* im datenschutzrechtlichen Sinn zu verstehen sei. Die *Infizierung* mit europäischem Datenschutzrecht findet also immer statt, wenn irgendeine Einrichtung in der EU, sei es ein Unternehmen oder eine Einzelperson, für das Mutterunternehmen einigermaßen beständig und effektiv wirtschaftlich tätig wird.

Lösung des Beispiels von oben: Die klitzekleine Niederlassung Ihres Mutterunternehmens in Spanien führt nach der bisherigen Rechtsprechung des EuGH dazu, dass sich auch die Muttergesellschaft an die Vorgaben der DSGVO halten muss, vorausgesetzt, die Tätigkeiten der Muttergesellschaft und der Niederlassung in der EU sind *untrennbar miteinander verbunden*.

Verarbeitungen im Zusammenhang mit einer Niederlassung in der EU

Daneben gilt die DSGVO aber auch umgekehrt für solche Unternehmen, die außerhalb der EU tätig sind, aber mit einer *Niederlassung* in der EU *in Zusammenhang* stehen (Art. 3 Abs. 1). In diesen Fällen hat nicht – wie im Google-Spain-Fall – ein außereuropäisches Unternehmen in der EU eine Niederlassung und wird deshalb dem europäischen Datenschutzrecht unterworfen, sondern ein europäisches Unternehmen betreibt Datenverarbeitung irgendwo im außereuropäischen Ausland. Dann unterliegt auch die Datenverarbeitung im außereuropäischen Ausland dem Regime der DSGVO.

Ein Unternehmen mit Hauptniederlassung in Frankreich betreibt ein Rechenzentrum in Russland. Findet die DSGVO auf die Datenverarbeitung in Russland Anwendung? Antwort: Die DSGVO findet auf das Rechenzentrum in Russland Anwendung, da die Verarbeitungstätigkeiten in Russland mit der Hauptniederlassung in Frankreich *in Zusammenhang* stehen.

Im Rahmen des *Niederlassungsprinzips* ist es völlig egal, ob die personenbezogenen Daten, die von Ihnen verarbeitet werden, solche von EU-Bürgern sind oder von Bürgern aus anderen Staaten! Sie müssen die DSGVO in Ihrer Niederlassung anwenden!

Marktortprinzip

Wenn Sie als Unternehmen in einem Staat ansässig sind, der kein Mitgliedstaat der EU ist, kann es also sein, dass Sie eine Niederlassung im datenschutzrechtlichen Sinne in der EU betreiben, was offenbar schneller gehen kann, als man so denken würde.

Im Zusammenhang mit den verwendeten Begriffen *Mitgliedstaat* und *Union* ist übrigens zu beachten, dass auch die EWR-Staaten (Staaten des Europäischen Wirtschaftsraums), aktuell Norwegen, Island und Liechtenstein, am 6. Juli 2018 die DSGVO übernommen haben. Somit gilt die DSGVO auch in diesen Staaten.

Aber das ist noch lange nicht alles. Auch wenn Sie in der EU nicht *niedergelassen* sind, kann es für Sie brenzlig werden. Denn neben dem Niederlassungsprinzip gilt jetzt auch das sogenannte *Marktortprinzip*. Über Art. 3 Abs. 2 erklärt die DSGVO sich nämlich auch dann für anwendbar, wenn von Ihnen

- ✔ *personenbezogene Daten* von solchen Personen verarbeitet werden, die sich in der EU befinden,
- ✔ und die Datenverarbeitung im Zusammenhang damit steht, betroffenen Personen in der EU *Waren oder Dienstleistungen* anzubieten, (Art. 3 Abs. 2 a) oder
- ✔ das *Verhalten* betroffener Personen zu *beobachten*, soweit ihr Verhalten in der Union erfolgt (Art. 3 Abs. 2 b).

Verarbeitung personenbezogener Daten von Personen, die sich in der EU befinden

Personen, die dem Schutz der DSGVO unterfallen, müssen nicht zwangsläufig Bürger der EU sein. Es genügt, wenn Sie sich in der EU *befinden*. Auf die Staatsangehörigkeit oder den Status als Unionsbürger kommt es dabei nicht an. Es genügt ein lediglich *kurzfristiger Aufenthalt*.

Anbieten von Waren oder Dienstleistungen in der EU

Sämtliche Unternehmen, die in der EU *Waren oder Dienstleistungen anbieten* und dabei personenbezogene Daten von Personen verarbeiten, die sich in der EU *befinden*, sind dem

Rechtsregime der DSGVO unterworfen (Art. 3 Abs. 2 a). Das gilt übrigens unabhängig davon, ob die Waren oder Dienstleistungen dabei gegen Bezahlung angeboten werden oder kostenlos zu erhalten sind. Damit werden auch Anbieter großer sozialer Netzwerke von den europäischen Datenschutzvorgaben erfasst und können bei Verstößen zur Rechenschaft gezogen werden.

Sie sind Onlinehändler mit Sitz in Brasilien, USA, Russland, China, Indien oder Timbuktu (nicht abschließende Aufzählung) und bieten Ihre Produkte auch auf dem europäischen Markt an? Bingo!

Auch Auftragsverarbeiter, die in der EU Dienstleistungen anbieten, sind unabhängig von ihrem Sitz verpflichtet, sich an die Vorgaben der DSGVO zu halten, wenn sie bei ihrer Tätigkeit personenbezogene Daten von Menschen verarbeiten, die sich in der EU befinden.

Bei einem *Auftragsverarbeiter* handelt es sich um einen Dienstleister, den Sie damit beauftragen, personenbezogene Daten für Sie zu verarbeiten. Das kann zum Beispiel ein Cloud-Anbieter sein, dem Sie personenbezogene Daten anvertrauen, ein ausgelagertes Rechenzentrum, aber auch eine externe Lohnbuchhaltung oder ein Lettershop, über den Sie Weihnachtsgrußkarten verschicken. Was Sie generell beachten müssen, wenn Sie einen Dienstleister mit der Verarbeitung personenbezogener Daten beauftragen wollen, und was es mit einem *Vertrag über die Auftragsverarbeitung* (*AVV*) nach Art. 28 auf sich hat, können Sie in Kapitel 7 *Zusammenarbeit von Unternehmen* unter der Überschrift *Auftragsverarbeitung* ausführlicher nachlesen.

Beobachtung des Verhaltens betroffener Personen in der EU

Wenn eine Datenverarbeitung dazu dient, das *Verhalten betroffener Personen in der EU zu beobachten*, ist das verantwortliche Unternehmen ebenfalls verpflichtet, sich bei der Verarbeitung personenbezogener Daten an die Vorschriften der DSGVO zu halten (Art. 3 Abs. 2 b).

Ob eine *Beobachtung des Verhaltens betroffener Personen* vorliegt, hängt zum Beispiel davon ab, ob deren *Internetaktivitäten* von dem Unternehmen nachvollzogen werden (*Erwägungsgrund 24*).

Die Vorschrift zielt vor allem auf solche Aktivitäten ab, durch die *Profile* (Art. 4 Nr. 4) von natürlichen Personen erstellt werden, anhand derer persönliche Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen. Unabhängig davon also, ob Waren oder Dienstleistungen angeboten werden, müssen sich auch all die Unternehmen an die DSGVO halten, die Daten von Personen, die sich in der EU befinden, zum Zwecke des *Profilings* verarbeiten.

Unter *Profiling* versteht man gemäß Art. 4 Nr. 4 die automatisierte Verarbeitung personenbezogener Daten, um bestimmte Aspekte, die sich auf Menschen beziehen, zu bewerten und daraus Vorhersagen abzuleiten. Das Ziel ist es dabei, Vorhersagen über die Arbeitsleistung, die wirtschaftliche Lage, die Gesundheit, persönliche Vorlieben, Interessen, die Zuverlässigkeit, das Verhalten, den aktuellen Aufenthaltsort oder Ortswechsel dieser Person zu analysieren und vorherzusagen.

Von dieser Vorschrift betroffen sind vor allem Unternehmen, die Aktivitäten von Personen im Internet beobachten und aufzeichnen (*Tracking*), um diese Informationen für Marktforschung zu nutzen, wie zum Beispiel Google über das Tracking Tool *Google Analytics*. Dieser Fall wird auch in *Erwägungsgrund 24* der DSGVO beispielhaft erwähnt.

Die Zähne des Monsters

Wenn Sie also nicht gerade eine Privatperson sind, die nur für persönliche oder familiäre Zwecke tätig ist, sondern geschäftsmäßig Daten von Personen verarbeiten, die sich in der EU befinden, müssen Sie sich mit sehr großer Wahrscheinlichkeit an die DSGVO halten. Und wenn Sie sich dabei erwischen lassen, dass Sie gegen die Vorgaben der DSGVO verstoßen, wird man Sie bestrafen. Ersteres lässt sich vielleicht noch vermeiden, Letzteres aber nach den bisherigen Erfahrungen nicht.

Wenn Sie auf Bestrafungen stehen und wissen wollen, wer Sie wie bestrafen wird, blättern Sie hemmungslos vor zu Kapitel 4 *Die Protagonisten* unter der Überschrift *Die Aufsichtsbehörden*. Alles kann, nichts muss.