INTERVIEW MIT DR. KRISTINA SCHREIBER UND
DR. STEFAN MAASSEN, LOSCHELDER, ZUR DS-GVO

„MEHR AUFWAND, ABER IN VIELEN PUNKTEN PRAXISNÄHER“

Am 25. Mai 2018 tritt die neue, EU-weit gültige DS-GVO (Datenschutz-Grundverordnung) in Kraft. Für viele Unternehmen der Werbeartikelbranche bedeutet das, ihre Datenschutzmaßnahmen zu hinterfragen und auf ein höheres Niveau zu hieven. Ein komplexes Unterfangen, das viele Fragen aufwirft: Was sind personenbezogene Daten? Wann darf man Bestandskunden anrufen? Wie müssen Dienstleister mit auftragsbezogenen Daten umgehen? Welche Strafen drohen bei Verstößen? Was macht eigentlich ein Datenschutzbeauftragter? Die *WA Nachrichten* klärten diese und ähnliche Fragen mit den Rechtsanwälten Dr. Kristina Schreiber und Dr. Stefan Maaßen, LL.M.

Der Schutz der persönlichen Daten hat im deutschen Recht traditionsgemäß einen hohen Stellenwert. Warum gibt es mit der DS-GVO überhaupt Neuerungen im Datenschutz?

In der Tat genießt der Schutz der persönlichen Daten in Deutschland seit Langem einen hohen, sogar grundgesetzlich geschützten Stellenwert. Dennoch war ein neues Datenschutzrecht überfällig: Zum einen, da das noch geltende Recht in vielen Aspekten durch den technischen Wandel überholt ist. Wenn Sie den alten Text lesen, merken Sie an vielen Stellen, dass der Gesetzgeber noch die Datenverarbeitung „im Hängeregister“ vor Augen hatte und nicht den Einsatz digitaler Medien. Dies ist jetzt anders.

Zum anderen bringt das neue Recht endlich im Wesentlichen einheitliche Bedingungen in ganz Europa und gleicht damit die Wettbewerbsbedingungen für die europäischen Unternehmen an. Die neue DS-GVO gilt unmittelbar und einheitlich in der ganzen EU. Exakt gleich sind die Bedingungen aber damit noch nicht: Die nationalen Gesetzgeber können (und müssen teils sogar) Konkretisierungen, Ergänzungen und Abweichungen vornehmen.

Double-Opt-in, Löschpflichten, Dokumentations- und Aufbewahrungspflichten, revisionssichere E-Mail-Archivierung … Vieles was jetzt breit diskutiert wird, ist ohnehin schon seit Jahren Pflicht. Ergeben sich durch das Inkrafttreten der DS-GVO tatsächlich wesentliche Neuerungen für Unternehmen?

Viele der inhaltlichen Pflichten, die Unternehmen durch die DS-GVO auferlegt werden, sind für deutsche Unternehmen keine wesentlichen Neuerungen. In anderen EU-Mitgliedsstaaten sieht das aber ganz anders aus, und auch in Deutschland hatte die umfassende Einhaltung des Da-

tenschutzrechts bislang nicht immer die höchste Priorität bei den Unternehmen.

Deutlich ausgeweitet sind zudem die formalen Pflichten: Hinter dem Stichwort „Rechenschaftspflicht" verbirgt sich die umfassende Pflicht eines jeden Unternehmens, jederzeit nachweisen zu können, dass Double-Opt-in, Löschpflichten und vieles mehr eingehalten werden. Hier ist jeder Einzelne in der Verantwortung, seine interne Organisation hinreichend zu gestalten – dies weitet die Dokumentationsanforderungen aus.

Außerdem sind deutlich mehr Pflichten bußgeldbewehrt als dies bislang der Fall war: Allein das Fehlen eines „Verarbeitungsverzeichnisses" kann beispielsweise mit einem Bußgeld belegt werden, das – dies ist hinreichend betrachtet worden in den vergangenen Monaten – viel höher ausfallen kann als bislang.

Bleiben frühere Datenprivilegien bei ausschließlich im B2B-Bereich tätigen Unternehmen erhalten?

Die DS-GVO unterscheidet nicht zwischen Unternehmen, die im B2B-Bereich tätig sind, und solchen, die sich im B2C-Bereich bewegen. Im Fokus stehen die personenbezogenen Daten. Diese werden regelmäßig auch im B2B-Bereich verarbeitet, z.B. durch die Abspeicherung von Ansprechpartnern beim Vertragspartner.

Auch in der DS-GVO gibt es aber Anhaltspunkte, dass im B2B-Bereich ein geringeres Datenschutzniveau akzeptabel ist als im B2C-Bereich. Dies zeigt sich beispielsweise daran, dass das jeweils notwendige Schutzniveau auch nach dem Risiko eines Datenverlusts für die betroffenen Personen zu bemessen ist und dieses beim Verlust von Privatdaten regelmäßig höher ist als bei Bekanntwerden der beruflichen Kontaktdaten. Überdies entscheidet oft eine Interessenabwägung („Unternehmen vs. betroffene Personen") über die Zulässigkeit einer Datenverarbeitung. Und auch dort wiegen die Interessen der betroffenen Personen an einem Ausschluss der Verarbeitung beruflicher Informationen regelmäßig weniger schwer als in Bezug auf Privatinformationen.

Sie sagen, im Fokus der DS-GVO ständen personenbezogene Daten: Was genau sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die einen Bezug zu einer bestimmten oder bestimmbaren natürlichen Person aufweisen. Wir brauchen also immer einen (möglichen) Personenbezug, der aber denkbar weit zu verstehen ist. Es reicht, wenn das Unternehmen selbst oder mithilfe von Dritten, die das Unternehmen zur Hilfestellung potenziell verpflichten kann, einen einzelnen Menschen identifizieren kann.

Konkret: Name, Alter, Bankverbindung oder namenbezogene E-Mail-Adresse sind per se personenbezogen, auch wenn es sich dabei um berufliche Kontaktdaten handelt. Und selbst die bloße IP-Adresse ist als „Nummernfolge" ein personenbezogenes Datum, wenn ein Anspruch auf Zuordnung dieser zu einer bestimmten Person gegeben sein kann – der Internetprovider z.B. kann die Nummer regelmäßig einer bestimmten Person zuordnen (und muss dies auch tun, wenn es um straf- oder urheberrechtlich relevante Sachverhalte geht). In der Praxis sollte daher im Zweifelsfall immer eher von personenbezogenen Daten ausgegangen werden, außer, es liegen belastbare Gründe vor, warum der Personenbezug zu verneinen ist.

ZUR PERSON

Dr. Kristina Schreiber und Dr. Stefan Maaßen, LL.M., sind Partner der Sozietät Loschelder in Köln. Dr. Schreiber ist auf den Bereich Datenschutzrecht und öffentliches Wirtschaftsrecht spezialisiert; Dr. Maaßen konzentriert sich auf Werbung und Markenrecht. Loschelder berät mit über 40 Anwälten in- und ausländische Mandanten in allen Bereichen des Wirtschaftsrechts.

Müssen Firmen jeder Größenordnung alle DS-GVO-Forderungen erfüllen, oder gibt es Einschränkungen?

Im Grundsatz müssen Firmen jeder Größenordnung alle DS-GVO-Forderungen erfüllen. Es gibt nur einzelne Erleichterungen – so z.B. muss ein Datenschutzbeauftragter in Deutschland erst ab zehn Beschäftigten, die automatisiert personenbezogene Daten verarbeiten, bestellt werden, es sei denn, die Datenverarbeitung ist ein Kerngeschäft. Kaum Anwendungsbereich dürfte dagegen die Ausnahme von der Pflicht zur Führung eines Verarbeitungsverzeichnisses finden: Davon kann bei weniger als 250 Mitarbeitern abgesehen werden, aber nur, wenn keine regelmäßige Verarbeitung personenbezogener Daten stattfindet – diese Ausnahme greift daher schon dann nicht mehr, wenn die Arbeitnehmerdaten elektronisch geführt und Gehaltszahlungen abgewickelt werden.

In der Praxis deutet sich aber an, dass die DS-GVO-Vorgaben für kleine und mittlere Unternehmen weniger streng ausgelegt werden; sowohl die EU-Kommission als auch das BayLDA (Bayerische Landesamt für Datenschutzaufsicht) haben für diese Unternehmen bereits Hilfestellungen veröffentlicht, die pragmatischer gefasst sind als die für größere Unternehmen formulierten Anforderungen.

Der Gesetzgeber fordert Transparenz: Unternehmen sind daher aufgefordert, eine verständliche und vollständige Datenschutzerklärung zu veröffentlichen. Was muss diese enthalten, und wo muss sie veröffentlicht werden?

Das Transparenzgebot ist wirklich ein ganz wichtiger Grundpfeiler des neuen Datenschutzrechts. Jeder soll – Stichwort: Verbraucherschutz – sicher und klar wissen, was mit seinen eigenen Daten geschieht. Das gilt zunächst auch im Internet: Jeder Homepage-Betreiber muss einfach, verständlich und umfassend erläutern, wie er mit den Informationen über die Homepagebesucher umgeht. Die bisherigen Datenschutzerklärungen sind daher regelmäßig auszubauen, der Rückgriff auf „Standardbausteine" ist mit Vorsicht zu hinterfragen. Wesentliche Änderungen sind dabei die Pflicht zur Angabe der Rechtsgrundlage und der Kontaktdaten (ggf. auch des Datenschutzbeauftragten) sowie eine umfassende Belehrung über die verschiedenen Betroffenenrechte. Abrufbar sein muss diese Datenschutzerklärung, wie auch bisher schon, von jedem Standpunkt des Internetangebots binnen maximal „zwei Klicks".

Aber auch im Übrigen gilt eine umfassende Informationspflicht: Jede Datener-

hebung ist mit umfassenden Informationen zur Art und Weise der folgenden Datenverarbeitung zu begleiten. Dafür sind „Beipackzettel" für ganz unterschiedliche Situationen zu erstellen, die den betroffenen Personen auf dem üblichen Kommunikationsweg mitzuteilen sind. Das heißt konkret: Eine Videoüberwachung muss vor Ort durch einen Aushang erläutert werden, bei einem Gewinnspiel kann ein „Beiblatt" erforderlich werden oder zumindest eine Zusammenfassung der „First Level-Informationen" mit Verweis auf eine leicht zugängliche Internetseite, auf der weitere Informationen hinterlegt sind. Wichtig ist immer: Die Informationen müssen für den Betroffenen leicht zugänglich sein. Dies kann zu ganz unterschiedlichen Anforderungen im Einzelfall führen.

Muss die Datenschutzerklärung bei jedem Auftrag oder jeder Auftragsanbahnung mitgeliefert werden oder reicht ein allgemeiner Verweis auf die Stelle, wo die Datenschutzerklärung zu finden ist?
Grundsätzlich gilt: Bei jedem Erstkontakt sind die Informationen mitzuliefern. Der bloße Verweis auf eine Stelle, an der die Angaben hinterlegt sind, dürfte nur im Ausnahmefall genügen. Das bedeutet aber natürlich nicht, dass bei längerdauernden Geschäftsbeziehungen für jeden E-Mail-Kontakt ein „Beipackzettel" erforderlich ist. Informiert werden muss immer nur bei Datenerhebung und wenn vorhandene personenbezogene Daten zu einem neuen Zweck verarbeitet werden sollen.

Die Datenspeicherung unterliegt dem Gebot der Zweckbindung. Was heißt das konkret?
Konkret bedeutet dies, dass erhobene personenbezogene Daten grundsätzlich nur zu dem Zweck verarbeitet (also auch gespeichert) werden dürfen, zu dem sie erhoben wurden. Die Frage „warum und wozu brauche ich die Daten" muss zu Beginn der Datenverarbeitung feststehen und eingehalten werden. Beispielsweise dürfen Sie also die Kontaktdaten aus einem Gewinnspiel nicht ohne Weiteres dazu verwenden, um die Gewinnspielteilnehmer über die neuesten Unternehmensangebote zu informieren oder ihnen einen Newsletter zu übersenden.

„Deutlich mehr Pflichten sind bußgeldbewehrt als dies bislang der Fall war: Allein das Fehlen eines ‚Verarbeitungsverzeichnisses' kann beispielsweise mit einem Bußgeld belegt werden."

Allerdings ist dieses Zweckbindungsgebot in der DS-GVO nicht mehr so streng wie im bisherigen Datenschutzrecht. Eine Verarbeitung zu einem „kompatiblen" Zweck kann künftig zulässig sein, z.B. wenn bei Vorliegen einer wirksamen Werbeeinwilligung eine Information zu sehr ähnlichen Produkten desselben Anbieters erfolgt.

Der Gesetzgeber fordert, die erhobenen Daten grundsätzlich nach Zweckerfüllung zu löschen. Wie lange dürfen denn Daten, die zu einem Auftrag gehören, z.B. die Versendung von 1.000 personalisierten Kugelschreibern an Einzelempfänger, gespeichert werden?
Auch wenn der originäre Zweck „Übersendung personalisierter Kugelschreiber" mit dem Versand erfüllt ist, können Aufbewahrungsrechte und -pflichten aus anderen Gesetzen eine weitere Speicherung der Datensätze insgesamt oder zumindest ausschnittsweise erfordern. So besteht z.B. ein – datenschutzrechtlich anerkanntes – berechtigtes Interesse an einer Speicherung bis zum Ablauf der Verjährung etwaiger Gewährleistungsansprüche, auch muss den steuer- und handelsrechtlichen Aufbewahrungsrechten von bis zu zehn Jahren genügt werden. Wichtig ist dabei aber, dass diese Aufbewahrungsrechte und -pflichten oft nicht für sämtliche Daten gelten, sodass u.U. einzelne Bestandteile der Datensätze wie z.B. die Handynummer des Empfängers – wenn technisch irgend möglich – früher zu löschen sind als andere.

Wenn die Daten grundsätzlich nach Zweckerfüllung zu löschen sind: Darf ich sie dann intern auch nicht für andere Zwecke wie Vertriebsaktivitäten weiter benutzen?
Die Weiterbenutzung von personenbezogenen Daten zu anderen Zwecken stellt eine Zweckänderung dar. Dies ist nur dann möglich, wenn Sie eine Erlaubnis hierfür im Datenschutzrecht selbst finden, die jenseits der gesetzlichen Pflichten wie der steuerrechtlichen Aufbewahrungspflicht liegen kann, z.B. in einer gesonderten Einwilligung oder einem berechtigten Unternehmensinteresse. Dies ist im Einzelfall sorgfältig zu prüfen, als Leitfaden gilt: Ähnliche Zwecke (Stichwort: Kompatibilität) sind eher miteinander vereinbar, als eine Verwendung zu einem ganz anderen Zweck, die Werbung an die berufliche Adresse ist weniger belastend und daher eher zulässig als ein Telefonanruf auf dem Privatanschluss. Wichtig ist dabei: Die DS-GVO erwähnt ausdrücklich, dass Direktmarketing ein berechtigtes Interesse darstellt. Dies eröffnet viele Möglichkeiten, wenn die Interessenabwägung sorgsam durchgeführt und dokumentiert wird.

Im Fokus stehen personenbezogene Daten, wie sie z.B. auf einer Visitenkarte vermerkt sind. Sollen diese Daten zu einem neuen Zweck verarbeitet werden, muss die betroffene Person informiert werden.

Ist es denn zukünftig einfacher oder schwieriger, datenschutzkonforme Direktmarketingmaßnahmen durchzuführen?
Sicher ist zum jetzigen Zeitpunkt nur, dass die datenschutzrechtliche Zulässigkeit unsicherer wird: Während wir (jenseits der immer möglichen Einwilligung) bisher mit den Vorgaben des § 28 BDSG alt einen detaillierten Paragraphen zu zulässigen Werbe-

maßnahmen hatten, gibt es künftig nur noch den Verweis auf eine notwendige Interessenabwägung. Dies ist einerseits positiv, da die bisherige Regelung schwer zugänglich und komplex war, bringt andererseits gerade zu Beginn der Anwendung aber auch Unsicherheit mit sich, wie Behörden und Gerichte die Interessenabwägung bewerten werden. Als Faustformel gilt: Die Orientierung an den bisherigen Anforderungen und die genaue Einhaltung der Anforderungen des UWG (Gesetz gegen den unlauteren Wettbewerb) bieten einen guten Start.

Können Newsletter auch ohne Double-Opt-ins an einen bestehenden Kundenstamm verschickt werden?
Was Newsletter anbelangt, so ist das „Double-Opt-in" weniger wichtig als Erlaubnisvoraussetzung, aber zentral für die Erfüllung der den Unternehmen obliegenden Nachweispflichten wie z.B. Einwilligung und Erfüllung der Informationspflichten. Ohne eine solche Absicherung könnte ein Newsletter-Versand u.U. vertretbar sein, wenn er im berechtigten Interesse erfolgt, was allenfalls bei Versand an Bestandskunden mit enger Beziehung zu den bereits bezogenen Produkten denkbar ist. Dabei ist dann auch im Blick zu halten, dass eine weitere EU-Verordnung (sog. ePrivacy-Verordnung) derzeit das Gesetzgebungsverfahren durchläuft. Tritt diese in Kraft, so sind auch deren Vorgaben zu berücksichtigen.

Zur Vermeidung von Missverständnissen: Am UWG ändert sich jetzt nichts. Mit der ePrivacy-VO entfällt aber § 7 UWG. Dann werden dort die Karten neu gemischt.

Sind bestimmte Werbemaßnahmen einfacher durchzuführen als andere?
Wie bisher gilt hier ganz klar – immer vorausgesetzt, es liegt keine explizite Einwilligung vor, die Werbemaßnahmen erlaubt –: Postsendungen können zulässig sein, Telefonanrufe im B2B-Bereich u.U. auch, E-Mail-Zusendungen regelmäßig nicht. Dies folgt nicht nur aus dem Datenschutzrecht, sondern insbesondere auch aus dem Wettbewerbsrecht nach UWG.

Gehen wir mal einige konkrete Beispiele durch: Ein Aussteller erhält auf der Messe eine Anfrage für ein Muster. Er versendet das Muster an die Person, erhält den Auftrag aber nicht. Darf er ohne die ausdrückliche Einwilligung des Messebesuchers diesen über andere Angebote aus dem eigenen Haus informieren?
Hat die Person nicht in die Zusendung von Informationen über andere Angebote eingewilligt, kann dies über ein „berechtigtes Interesse" des Unternehmens datenschutzrechtlich zulässig sein. Dies ist stets im Einzelfall zu bewerten (und zu dokumentieren), allgemein aber gilt: Bei Angeboten, die mit dem angefragten Muster in eine ähnliche Kategorie fallen, ist dies eher zulässig als bei ganz anderen Produkten. Auch die Form der Ansprache ist wesentlich: Postalisch dürfte dies möglich sein, via Telefon ist die Ansprache schon wettbewerbsrechtlich (und dann auch datenschutzrechtlich) kritisch, via E-Mail unzulässig. Erfolgt eine Ansprache, sind die Informationspflichten nebst Verweis auf das Widerspruchsrecht („Opt-out") einzuhalten.

Ein Händler lädt Kunden zur Teilnahme an einer Messe ein: Darf er diejenigen Besucher, die sich angemeldet haben, ohne deren ausdrückliche Einwilligung auch zu einer Folgemesse im nächsten Jahr einladen?
Hier haben wir einen eng verknüpften Zweck, sodass eine Erlaubnis über ein berechtigtes Interesse eher in Betracht

kommt als in anderen Konstellationen: Bei der Interessenabwägung spricht der Umstand, dass die Besucher sich im Vorjahr angemeldet und damit ihr Interesse an solchen Veranstaltungen bekundet haben, für ein überwiegendes Interesse des Händlers. Zu beachten ist aber – auch wettbewerbsrechtlich – die Form der Ansprache. Auch hier gilt: Per Post ist die Einladung eher unbedenklich als auf elektronischem Weg.

Ein Einkäufer bestellt im Internet T-Shirts für eine Messeaktion und hinterlässt seine Kontaktdaten: Darf dieser Kunde anschließend auch telefonisch oder per E-Mail für andere Produktbereiche des Unternehmens (z.B. Arbeitskleidung) akquiriert werden?
Datenschutzrechtlich kann dies womöglich über ein „berechtigtes Interesse" gerechtfertigt werden, zumal wenn der Kunde beruflich tätig wird. Allerdings wird, jedenfalls wettbewerbsrechtlich, eine Ansprache per Telefon nur dann zulässig sein, wenn noch ein enger Zusammenhang mit den T-Shirts für die Messeaktion besteht, der bei Arbeitskleidung u.U. noch gegeben ist, z.B. bei Musikinstrumenten aber dann wohl nicht mehr. Je weiter sich die Angebote vom bestellten Artikel entfernen, desto eher ist Vorsicht geboten und desto eher finden sich Argumente für die Unzulässigkeit der Werbung unter datenschutzrechtlichen Aspekten. Eine E-Mail-Ansprache kommt – schon wettbewerbsrechtlich – nur nach erfolgtem Geschäftsabschluss in Betracht, wenn auch die weiteren Voraussetzungen des § 7 Abs. 3 UWG vorliegen.

„Auch in der DS-GVO gibt es Anhaltspunkte, dass im B2B-Bereich ein geringeres Datenschutzniveau akzeptabel ist als im B2C-Bereich."

Ein Unternehmen verschickt an 1.000 Kunden einen Kalender mit dem Aufdruck des persönlichen Namens. Darf es das überhaupt?
Ein personalisiertes Giveaway wird viele Kunden freuen, manche aber auch nicht. Datenschutzrechtlich zulässig kann es sein, wenn ein „berechtigtes Interesse" des Unternehmens besteht. Dies kann – als Direktmarketingmaßnahme – im Einzelfall eher bejaht werden, wenn der Kalender die Kunden wie ein Brief erreichen kann, also keinen Sonderaufwand bei der Zustellung erfordert, wie er durch ein Paket ausgelöst werden kann. Zudem ist zu berücksichtigen, welche Bilder der Kalender enthält und wie der Kontakt zu den Kunden ausgestaltet ist: Alle beteiligten Interessen sind sorgsam abzuwägen, zu dokumentieren und mit einem Widerspruchshinweis an den Kunden zu vervollständigen.

Darf man potenzielle Kunden zukünftig noch anrufen? Laut DS-GVO ja, sofern ein „berechtigtes Interesse" besteht. Was ein „berechtigtes Interesse" ist, gilt es im Einzelfall zu prüfen. Man darf gespannt auf die Rechtsprechung der nächsten Zeit sein.

Ein Händler übernimmt für dieses Unternehmen die Durchführung des Auftrags und versendet die Kalender an die Empfänger: Was ist bzgl. der DS-GVO zu beachten?
In einem solchen Fall kann es sich um eine „Auftragsverarbeitung" handeln, wenn der Händler im Auftrag des Unternehmens weisungsgebunden für dieses tätig wird. Wichtig ist in einem solchen Fall, dass ein Auftragsverarbeitungsvertrag nach neuem DS-GVO-Recht abgeschlossen wird und dessen Vorgaben eingehalten werden. Hier hat die BayLDA bereits ein erstes Muster für Standardsituationen online veröffentlicht.

Der Händler gibt die Daten an einen Kalenderlieferanten, einen Drucker oder einen Versender weiter. Was ist zu beachten?
Die Weitergabe der Daten ist immer dann möglich und zulässig, wenn die eingeschalteten Unternehmen weisungsgebunden für den Händler tätig werden, mit ihnen ein Auftragsverarbeitungsvertrag nach Maßgabe des Art. 28 DS-GVO abgeschlossen ist, dessen Anforderungen eingehalten werden, und das den Händler beauftragende Unternehmen diese „Unter-Beauftragung" genehmigt. Eine solche Genehmigung ist – strenger als nach bisherigem Recht – von der DS-GVO vorgesehen und daher auch im Auftragsverarbeitungsvertrag angelegt. Erleichternd kann vereinbart werden, dass eine Information des Auftraggebers reicht, wenn dieser nicht widerspricht.

Besteht eine DS-GVO-konforme Kette von Auftragsverarbeitungsverträgen, haftet der Auftraggeber gegenüber den betroffenen Personen nach außen und kann sich im Innenverhältnis entlang der Kette schadlos halten. Der Händler muss also u.U. auch für Fehler seiner Sub-Auftragnehmer einstehen. Gegenüber den Aufsichtsbehörden ist jeder bußgeldbewehrt verantwortlich – auch der Händler dafür, dass er seine Unter-Auftragnehmer sorgsam auswählt, überwacht und ggf. bei Mängeln der Datensicherheit o.Ä. einschreitet.

Was passiert, wenn in die Verarbeitung der Daten auch Unternehmen außerhalb des Geltungsbereichs der DS-GVO – z.B. Produktionsbetriebe in Fernost – eingeschaltet werden?
Werden Unternehmen aus sog. „Drittstaaten", also Ländern außerhalb der EU, als Auftragnehmer eingeschaltet, muss über den Auftragsverarbeitungsvertrag hinaus sichergestellt werden, dass durch ausreichende Garantien ein hinreichendes Datenschutzniveau auch im Zielland gesichert wird. Hierfür gibt es verschiedene Instrumente, z.B. können Angemessenheitsbeschlüsse der EU-Kommission existieren oder es kann ein Rückgriff auf die EU-Standardvertragsklauseln für die Auftragsdatenverarbeitung erfolgen, die vereinbart werden müssen.

Zur DS-GVO gehört auch eine Dokumentationspflicht: Was beinhaltet diese? ►

Die Dokumentationspflicht, die die DS-GVO normiert, hat einen beträchtlichen Umfang. Ziel ist es, die Einhaltung datenschutzrechtlicher Vorgaben umfassend und stets aktuell nachzuweisen. Diese „Rechenschaftspflicht" obliegt jedem Unternehmen, das personenbezogene Daten verarbeitet.

Ausgangspunkt ist das sogenannte Verarbeitungsverzeichnis, das alle Verarbeitungsvorgänge, in denen personenbezogene Daten einbezogen sind, stets aktuell erfasst. Das Verzeichnis muss also bei jeder relevanten Änderung überarbeitet werden. Hilfreich sind hier die Mustererklärungen, die von den Aufsichtsbehörden im Rahmen des Düsseldorfer Kreises erstellt wurden und online abrufbar sind.

Damit sind aber noch nicht sämtliche Dokumentationspflichten erfüllt – auch die Einwilligungen müssen dokumentiert werden, die berechtigten Interessen, die Auftragsverarbeitungsverträge, geeignete Garantien für den Drittstaatentransfer, die Erfüllbarkeit und Erfüllung der Betroffenenrechte u.Ä.

Gibt es bei der Sensibilität erhobener Daten Unterschiede? Sind z.B. Daten, bei denen Textilgrößen Einzelnamen zugeordnet werden können, sensibler als Daten mit Einzelnamen und Funktion innerhalb eines Unternehmens?
Ja, im Hinblick auf die Sensibilität gibt es ganz erhebliche Unterschiede: Umso riskanter das Bekanntwerden für den Betroffenen ist, umso höher die Schutzanforderungen. Da die Textilgröße mehr Informationen über eine Person preisgibt als die berufliche Position, ist die Textilgröße auch besser zu schützen. Generell gilt: Das Datenschutzrecht erfasst alle personenbezogenen Daten. Wie hoch die Schutzanforderungen im Einzelfall sind, hängt dann aber davon ab, wie wesentlich die Informationen für den jeweils Betroffenen sind.

„Das Transparenzgebot ist ein ganz wichtiger Grundpfeiler des neuen Datenschutzrechts. Jeder soll – Stichwort: Verbraucherschutz – sicher und klar wissen, was mit seinen eigenen Daten geschieht."

Wenn Versender die Weiterverarbeitung personenbezogener Daten übernehmen, muss mit ihnen ein Auftragsverarbeitungsvertrag nach Maßgabe des Art. 28 DS-GVO abgeschlossen werden.

Vertriebskräfte erfahren in Gesprächen oft persönliche Dinge von ihren Kunden (z.B. Geburtstage, Anzahl der Kinder etc.). Sollte darauf verzichtet werden, diese persönlichen Informationen in der Software zu speichern?
Pauschal betrachtet, sollte auf eine Speicherung verzichtet werden. Nur wenn für ein spezifisches Datum auch ein berechtigtes Unternehmensinteresse vorliegt und keine entgegenstehenden Kundeninteressen überwiegen, kann eine Speicherung erfolgen. Was dabei künftig immer wichtig ist: Das berechtigte Interesse und die Interessenabwägung sind zu dokumentieren. Einer möglichst umfassenden Datensammlung steht die DS-GVO entgegen.

Wann braucht ein Unternehmen einen Datenschutzbeauftragten? Und was sind dessen Rechte und Pflichten?
Hier ist das deutsche Recht künftig strenger als die DS-GVO. Unternehmen müssen immer dann einen Datenschutzbeauftragten benennen und diesen der Aufsichtsbehörde melden sowie die Kontaktdaten veröffentlichen, wenn sie mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen oder – unabhängig von der Zahl der Mitarbeiter – besonders riskante Datenverarbeitungen vornehmen (Fälle der Datenschutz-Folgenabschätzung) oder personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten. Gerade in der Werbebranche wird aus der letzten Fallgruppe heraus oft ein Datenschutzbeauftragter zu bestellen sein.

Die Rechte und Pflichten des Datenschutzbeauftragten sind umfangreich. Knapp gefasst: Er berät und kontrolliert das Unternehmen in Sachen Datenschutz und ist Kontaktstelle für Aufsichtsbehörde und Betroffene. Das Unternehmen muss ihm dies durch Einbindung, Bereitstellung der nötigen Ressourcen, Gewährleistung der erforderlichen Unabhängigkeit etc. ermöglichen. Ermöglicht das Unternehmen all dies und kommt der Datenschutzbeauftragte dennoch seinen Aufgaben nicht nach, kann er u.U. auch haften – dies ist im Einzelfall zu betrachten und unterscheidet sich auch danach, ob es ein interner oder externer Beauftragter ist. Benannt werden kann jedenfalls jeder, der über eine ausreichende Fachkunde und Erfahrung verfügt.

Auch wenn ein Datenschutzbeauftragter benannt wurde, bleibt die Verantwortlichkeit für die Einhaltung des Datenschutzrechts bei der Unternehmensleitung selbst.

Wie sehr sind Unternehmen verpflichtet, sich gegen illegale Zugriffe von Hackern oder anderen Datenmissbrauch abzusichern?
Unternehmen müssen eine „angemessene" Datensicherheit gewährleisten. Was angemessen ist, hängt von den betroffenen Daten – also dem Risiko für die betroffenen Personen, wenn die Daten ungerechtfertigt bekannt werden –, dem Stand der Technik und den Implementierungskosten ab. Kurz gefasst: Bankdaten müssen besser geschützt werden als eine Adressdatenbank mit beruflichen E-Mail-Adressen.

Was muss man tun, falls mal eine Panne passiert?
In einem solchen Fall ist zeitnah, maximal 72 Stunden nach erster Kenntnis, der entsprechende Vorfall der zuständigen Aufsichtsbehörde zu melden, es sei denn, ein Risiko für die betroffenen Personen ist ausgeschlossen. Eine Meldung muss immer binnen 72 Stunden erfolgen, auch wenn

Bildquelle: Shutterstock.com

zu diesem Zeitpunkt noch nicht alle Umstände bekannt sind. In bestimmten Fällen müssen zudem die vom Vorfall Betroffenen benachrichtigt werden.

Mit welchen Strafen müssen Unternehmen rechnen, wenn sie gegen einzelne Punkte der DS-GVO verstoßen? Und wer kontrolliert das eigentlich alles?
Bei Verstößen gegen die DS-GVO kommen unterschiedliche Konsequenzen in Betracht. Neben Schadenersatzforderungen von Betroffenen drohen Geldbußen. Je nachdem, gegen welche Pflichten aus der DS-GVO verstoßen wird, können Geldbußen von bis zu 10 Mio. Euro oder 2% bzw. sogar 20 Mio. Euro oder 4% des weltweit erzielten Jahresumsatzes – es gilt der jeweils höhere Wert – verhängt werden. Kontrolliert wird die Einhaltung des Datenschutzrechts durch die für das jeweilige Bundesland zuständige Aufsichtsbehörde. Betroffene können sich dort beschweren und damit ein Verfahren einleiten. Auch können Wettbewerber marktrelevante Verstöße abmahnen und auch im Wege der einstweiligen Verfügung unterbinden; dies ist aber auch heute schon möglich. Es gibt damit letztlich drei Einfallstore für die Überwachung – Betroffene, Wettbewerber (u.U. auch Verbände) und Aufsichtsbehörden.

Stichtag für das Inkrafttreten der DS-GVO ist der 25. Mai 2018: Was passiert, wenn Unternehmen bis dahin nicht alle Punkte der DS-GVO erfüllt haben?
Ab dem 25. Mai können die Aufsichtsbehörden die Einhaltung aller Vorgaben der DS-GVO durchsetzen. Faktisch kann allerdings nicht jedes Unternehmen im Hinblick auf die Einhaltung des Datenschutzrechts (sofort) kontrolliert werden; es ist aber unklar, welche Unternehmen in den Fokus der Aufsichtsbehörden geraten und wie diese bei der Auswahl zu prüfender Unternehmen vorgehen. Wenn sich ein Unternehmen um die Umsetzung der DS-GVO-Vorgaben bemüht, aber noch nicht alle Punkte umgesetzt hat, wird dies sicherlich zu weniger weitreichenden Folgen führen, als wenn mit der Umsetzung am 25. Mai noch nicht begonnen wurde.

Jenseits eines möglichen Vorgehens der Aufsichtsbehörden ist zu berücksichtigen, dass den Betroffenen ab diesem Zeitpunkt erweiterte Rechte zustehen, die sie jederzeit geltend machen können, und dass Wettbewerber sowie Verbände marktrelevante Verstöße gegen die DS-GVO abmahnen können.

„Jede Datenerhebung ist mit umfassenden Informationen zur Art und Weise der folgenden Datenverarbeitung zu begleiten. Dafür sind ‚Beipackzettel' für ganz unterschiedliche Situationen zu erstellen, die den betroffenen Personen auf dem üblichen Kommunikationsweg mitzuteilen sind."

Abschließend eine Einschätzung: Ist die DS-GVO ein einziges Bürokratiemonster oder gibt es aus Ihrer Sicht auch Erleichterungen und Verbesserungen im Bereich des Datenschutzes?
Sicherlich bringt die DS-GVO erheblich erweiterte Dokumentations- und Rechenschaftspflichten mit sich, die zunächst einmal Aufwand bedeuten. Dies bringt allerdings auch Chancen mit sich, die Abläufe im eigenen Unternehmen zu durchleuchten, die Datensicherheit anzupassen und Synergien z.B. durch neue Digitalisierungsstrategien anzugehen.

Auch jenseits dessen hat die DS-GVO gegenüber dem bisherigen Recht einen ganz entscheidenden Vorteil: Sie ist in vielen Punkten praxisnäher, so z.B. bei der expliziten Berücksichtigungsfähigkeit der Implementierungskosten bei der Prüfung des angemessenen Datensicherheitsniveaus und der Anerkennung von Direktmarketingmaßnahmen und Übermittlungen im Konzernverbund als berechtigte Interessen eines Unternehmens.

Mit Dr. Kristina Schreiber und Dr. Stefan Maaßen sprach Dr. Mischa Delbrouck.

Der Stichtag fürs Inkrafttreten der DS-GVO ist der 25. Mai 2018. Mit der Umsetzung der Vorgaben sollte jedoch vorher begonnen werden.