Bird & Bird

Fragen zur Europäischen Datenschutzgrundverordnung

Juni 2016

Inhalt

Einleitung

Am 25. Mai 2016 ist mit der Datenschutzgrund-verordnung eine neue rechtliche Grundlage zum Datenschutz in der EU verabschiedet worden.

Betroffen sind alle größeren Unternehmen sowie alle Unternehmen der digitalen Wirtschaft, nicht nur solche, zu deren Geschäftsmodell die Erfassung und Verarbeitung von (personenbezogenen) Daten gehört. Einige der Neuigkeiten sind grundlegender Natur und können sogar Geschäftsmodelle in Frage stellen. Sie müssen von den Unternehmen daher bereits jetzt adressiert werden, um eine rechtzeitige Anpassung der Geschäftsprozesse und ggf. -modelle bis zum Inkrafttreten des neuen Rechts 2018 sicher zu stellen.

Die nachfolgenden 37 Fragen und Antworten zur Datenschutzgrundverordnung helfen Ihnen, die Auswirkungen der Datenschutzgrundverordnungen auf Ihr Geschäft einzuschätzen und die ggf. notwendigen Schritte zur Anpassung in die Wege zu leiten.

Bei Rückfragen stehen wir Ihnen sehr gerne zur Verfügung.

Dr. Fabian Niemann
Partner, Düsseldorf/Frankfurt

Tel: +49 (0)211 2005 6238
fabian.niemann@twobirds.com

Lennart Schüßler
Partner, Düsseldorf

Tel: +49 (0)211 2005 6238
lennart.schuessler@twobirds.com

Valerian Jenny
Counsel, Frankfurt

Tel: +49 (0)69 74222 6140
valerian.jenny@twobirds.com

Dr. Simon Assion
Associate, Frankfurt

Tel: +49 (0)69 74222 6140
simon.assion@twobirds.com

"Dr. Fabian Niemann ist 'für internationale Datenschutzprojekte unschlagbar' und 'sehr kompetent'."

JUVE Handbuch 2016/2107

37 Fragen zur Datenschutzgrund-verordnung

1 Welche Daten und Handlungen sind von der Datenschutzgrund-verordnung erfasst?

Der Begriff der personenbezogenen Daten ist ähnlich umfassend, wie unter den bisher bestehenden Regelungen. Unter "personenbezogene Daten" versteht man nach der Datenschutzgrundverordnung

> *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden "betroffene Person") beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.“*

Im Ergebnis ist von personenbezogenen Daten und damit grundsätzlich einer Anwendbarkeit des Datenschutzrechts nach der Datenschutzgrundverordnung immer auszugehen, wenn Informationen oder Daten in irgendeinem Zusammenhang mit einer natürlichen Person stehen oder ein solcher Zusammenhang hergestellt werden kann. Die Definition ist also sehr weit.

Unternehmensdaten, wie nach österreichischem Vorbild diskutiert, wurden nicht in den Anwendungsbereich der Verordnung einbezogen. Dafür werden die Begriffe „genetische Daten“ und „biometrische Daten“ erstmals ausdrücklich definiert. Sie alle stellen besondere Kategorien personenbezogener Daten dar (sog. „sensible Daten“, siehe dazu Frage 16.e.).

Auch der Begriff der Verarbeitung ist weit gefasst, als jeder

> *„mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.“*

Somit beinhaltet Verarbeitung praktisch jede Art des Umgangs mit personenbezogenen Daten. Insbesondere wird jeder Umgang mit personenbezogenen Daten erfasst, die in Computern oder anderen digitalen Medien gespeichert sind.

Der Begriff des Profilings wird ausdrücklich definiert und geregelt (siehe hierzu näher Frage 17). Anonyme Daten werden nach den Erwägungsgründen vom Anwendungsbereich der Verordnung ausdrücklich nicht abgedeckt, für sie gelten die datenschutzrechtlichen Regeln nicht. Schließlich enthält die Verordnung spezifische Bestimmungen für die Verarbeitung von Daten von Kindern.

2 Welche weiteren datenschutzrechtlichen Regelungen bleiben neben der Datenschutzgrund-verordnung bestehen?

Das Ziel der Datenschutzgrundverordnung ist es, die Harmonisierung des Datenschutzrechts in der EU weiter voranzutreiben. Jedoch ist dies nur eingeschränkt gelungen. Es wird auch in Zukunft in vielen Bereichen Spielraum für nationale Regelungen geben. Die Verordnung enthält eine ganze Reihe von Öffnungsklauseln, die es den Mitgliedstaaten erlauben oder auftragen, abweichende bzw. ergänzende Regelungen zu treffen.

Mitgliedstaaten dürfen beispielsweise anordnen, dass die Einwilligung keine adäquate Rechtsgrundlage für die Verarbeitung (bestimmter Kategorien von) sensiblen Daten (siehe dazu Frage 16.e.) sein soll. Auch können nationale Regelungen Rechtsgrundlage für die Verarbeitung von sensiblen Daten vorsehen (für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke). Andere Bereiche, in denen mitgliedstaatliches Recht weiter relevant sein wird, umfassen etwa

- bestimmte Regelungen zum Zwecke der nationalen Sicherheit und der Strafprävention/-verfolgung;
- die mögliche Absenkung der Altersgrenze zur Einwilligung durch Kinder von 16 auf bis zu 13 Jahre;
- die Einschränkung des Rechts auf Datenlöschung des Betroffenen (Speicherpflichten);
- die Erweiterung der Befugnisse der verantwortlichen Stelle im Zusammenhang mit automatisierten Einzelentscheidungen (einschließlich Profiling);
- die Schaffung gewisser bindender Rechtsinstrumente für die Verarbeitung durch einen Auftragsdatenverarbeiter;
- die Einführung von Regelungen zur Verarbeitung und Zugang der Öffentlichkeit zu amtlichen Dokumenten;
- die Einschränkung der Informationspflichten im Bereich der Berufsgeheimnisse und sonstiger Geheimhaltungspflichten; und
- den Erlass von Regelungen für die Verarbeitung von nationalen Kennziffern.

Mitgliedstaaten dürfen zudem Abweichungen oder Ausnahmen für die Verarbeitung von Daten zu journalistischen Zwecken oder zu wissenschaftlichen, künstlerischen oder literarischen Zwecken vorsehen, wenn dies erforderlich ist, um das Recht auf Schutz der personenbezogenen Daten mit der Freiheit der Meinungsäußerung und der Informationsfreiheit in Einklang zu bringen.

Eine für die Praxis ganz relevante Öffnungsklausel besteht schließlich für die Datenverarbeitung im Beschäftigungskontext: Im Recht der Mitgliedstaaten oder in Kollektivvereinbarungen (einschließlich 'Betriebsvereinbarungen') können spezifische Vorschriften für die Verarbeitung personenbezogener Beschäftigtendaten im Beschäftigungskontext vorgesehen werden. Hierzu zählen insbesondere Vorschriften über die Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen, über die Verarbeitung dieser Daten für Zwecke der Einstellung, der Erfüllung des Arbeitsvertrags einschließlich der Erfüllung von durch Rechtsvorschriften oder durch Kollektivvereinbarungen festgelegten Pflichten, des Managements, der Planung und der Organisation der Arbeit, der Gleichheit und Diversität am Arbeitsplatz, der Gesundheit und Sicherheit am Arbeitsplatz sowie für Zwecke der Inanspruchnahme der mit der Beschäftigung zusammenhängenden individuellen oder kollektiven Rechte und Leistungen und für Zwecke der Beendigung des Beschäftigungsverhältnisses. Im Grunde ist damit der Arbeitnehmerdatenschutz von der EU-weiten Vereinheitlichung ausgenommen.

In welchem Umfang und in welcher Form die Mitgliedstaaten ihre Regelungsbefugnisse insoweit ausüben werden, bleibt abzuwarten. Die weiteren Entwicklungen (insbesondere in den nächsten zwei Jahren) sollten aufmerksam verfolgt werden.

3 Wen betrifft die Datenschutzgrundverordnung in welchem Ausmaß?

Die Datenschutzgrundverordnung stellt klar, dass "Verantwortlicher" jede natürliche oder juristische

Person, Behörde, Einrichtung oder andere Stelle sein kann, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Für all diese Personen und Stellen gilt die Verordnung – ihr Anwendungsbereich ist also breit.

Für Behörden (wie etwa Justizbehörden, Steuer- und Zollbehörden, Finanzermittlungsstellen, unabhängige Verwaltungsbehörden oder Finanzmarktbehörden) und Gerichte gelten eine Reihe von Ausnahmen und besonderen Vorschriften und der nationale Gesetzgeber kann insoweit bestimmte weitere nationale Regelungen treffen.

Für Privatpersonen bleibt es dabei, dass die Verarbeitung von personenbezogenen Daten, die von einer natürlichen Person zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten (und somit ohne Bezug zu einer beruflichen oder wirtschaftlichen Tätigkeit) vorgenommen wird, nicht erfasst wird.

Auch Auftragsdatenverarbeiter sind Gegenstand der Datenschutzgrundverordnung (in der Datenschutzgrundverordnung als sog. „Auftragsverarbeiter“ bezeichnet) und ihre Pflichten werden ausgeweitet (insbesondere auch im Bereich der Haftung – vgl. insoweit näher Frage 24).

Räumlich findet die Datenschutzgrundverordnung zunächst auf die Verarbeitung personenbezogener Daten Anwendung, wenn und soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsdatenverarbeiters in der Europäischen Union (EU) erfolgt, und zwar unabhängig davon, ob die Verarbeitung in der Union stattfindet. Kurz gesagt: die Verordnung findet Anwendung auf alle Verantwortlichen und Auftragsdatenverarbeiter in der EU.

Für Verantwortliche und Auftragsdatenverarbeiter außerhalb der EU, für welche bisher nach der Datenschutzrichtlinie 95/46/EG das - vom Europäischen Gerichtshof („EuGH“) allerdings deutlich abgeschwächte - Territorialitätsprinzip galt, wird nun das Marktortprinzip eingeführt und damit der Anwendungsbereich stark erweitert. Die Verordnung findet Anwendung, wenn sich

- ein Angebot an einen bestimmten nationalen Markt in der EU richtet oder
- wenn die Datenverarbeitung der Beobachtung des Verhaltens von Personen in der EU dient.

Umfasst sind also auch außereuropäische Unternehmen, die auf dem europäischen Markt tätig sind. Auch hier ist der Anwendungsbereich wieder sehr weit gewählt und gießt die (rechtlich teils sehr konstruiert wirkende) gegenwärtige „gelebte“ Praxis der Datenschutzbehörden und des EuGH, europäisches Datenschutzrecht auch auf (EU-Verbraucher betreffende) Vorgänge außerhalb der EU zu erweitern, im Ergebnis in eine ausdrückliche Regelung.

4 Wie definiert die Datenschutzgrundverordnung personenbezogene, pseudonyme und anonyme Daten?

Die Verordnung definiert “personenbezogene Daten” als alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (“betroffene Person”) beziehen; als identifizierbar wird eine Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Art. 4 Nr. 1).

Der Begriff „pseudonyme Daten“ ist selbst nicht definiert, bezeichnet aber Daten, die durch Pseudonymisierung verändert wurden. „Pseudonymisierung“ ist definiert als die „Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“ (Art. 4 Nr. 5).

Der Begriff „anonyme Daten“ wird in der Verordnung selbst nicht definiert und auch nicht verwendet. In Erwägungsgrund 26 finden sich jedoch entsprechende Hinweise, was hierunter zu verstehen ist und dass die Datenschutzgrundsätze insoweit keine Anwendung finden. Dort heißt es:

„[...]Die Grundsätze des Datenschutzes sollten [...] nicht für anonyme Informationen gelten, d.h. für Informationen, die sich nicht auf eine identifizierte oder identifizierbare natürliche Person beziehen, oder personenbezogene Daten, die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann. Diese Verordnung betrifft somit nicht die Verarbeitung solcher anonymer Daten, auch für statistische oder für Forschungszwecke.“ Es bleibt abzuwarten, ob das bisherige Verständnis nach dem Bundesdatenschutzgesetz hiermit deckungsgleich ist. Nach § 3 (6) BDSG bezeichnet „anonymisieren“ das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.

5 Benötige ich zur Nutzung anonymer Daten eine Einwilligung oder anderweitige Rechtfertigung?

Grundsätzlich nein. Anonyme Daten sind keine personenbezogenen Daten im Sinne der Datenschutzgrundverordnung. Die Datenschutzgrundverordnung ist somit von vornherein auf solche Daten nicht anwendbar.

Zu beachten ist aber, dass viele Daten, die auf den ersten Blick „anonym“ zu sein scheinen, im Zeitalter von „Big Data“ und Vorratsdatenspeicherung als personenbezogene Daten einzuordnen sind. Ein Datum ist nämlich bereits dann personenbezogen, wenn es von dem Verantwortlichen oder einer anderen Person einer betroffenen Person zugeordnet werden kann (Erwägungsgrund 26). Im Zweifel reicht es also aus, wenn irgendjemand den Betroffenen ermitteln kann – dies kann z.B. auch eine Behörde sein, die privilegierten Zugriff z.B. auf bestimmte Datenbanken hat (z.B. zur Zuordnung von IP-Adressen). Es kommt dann darauf an, ob nach den bestehenden Umständen mit einer gewissen Wahrscheinlichkeit damit zu rechnen ist, dass die Person identifiziert werden könnte.

6 Benötige ich zur Nutzung pseudonymer Daten eine Einwilligung oder anderweitige Rechtfertigung?

Grundsätzlich ja, denn pseudonyme Daten sind – im Unterschied zu anonymen Daten – weiterhin personenbeziehbar. Das heißt, es ist bei solchen Daten weiterhin möglich, die betreffenden Daten einer konkreten Person zuzuordnen.

Bei pseudonymen Daten werden die Identifikationsmerkmale eines Datensatzes (z.B. Name, Adresse, Datum) aber „ausgesondert“ und entweder gelöscht oder getrennt vom übrigen Datensatz gespeichert. Der Datensatz ist also nicht sofort personenbeziehbar, sondern nur, indem zusätzliche Informationen herangezogen werden (Erwägungsgrund 26). Die Pseudonymisierung von Daten ist somit eine datenschutzfreundliche Maßnahme, die von der Datenschutzgrund-verordnung an verschiedenen Stellen gefordert oder belohnt wird. Insbesondere gilt dies in Fällen, wo die Verwendung von Daten auf Basis einer Interessenabwägung zulässig ist. Die Pseudonymisierung kann dann dabei helfen, diese Abwägung zu Gunsten der datenverarbeitenden Stelle ausfallen zu lassen. Die Pseudonymisierung ist außerdem eine „technische und organisatorische Maßnahme“ des Datenschutzes, die im Betrieb des Betroffenen umgesetzt werden muss, soweit sie angemessen ist (Art. 25 und Art. 32).

7 Wann benötige ich eine Einwilligung für die Verarbeitung von Daten?

Immer dann, wenn keine andere (gesetzliche) Erlaubnisvorschrift greift. Die Einwilligung ist eine von mehreren möglichen Ausnahmen, die die Datenschutzgrundverordnung von dem Verbot mit Erlaubnisvorbehalt vorsieht. Das heißt, eine Einwilligung ist nicht die einzige Möglichkeit, personenbezogene Daten zu verarbeiten, sondern nur eine von mehreren Möglichkeiten. Sie ist aber umgekehrt immer erforderlich, wenn kein gesetzlicher Erlaubnistatbestand einschlägig ist.

8 Was sind die Voraussetzungen für eine wirksame Einwilligung?

Die Datenschutzgrundverordnung ist sehr restriktiv, was die Wirksamkeit einer Einwilligung angeht. In vielen Fällen erklärt sie eine

Einwilligung, die eigentlich vorliegt, für unbeachtlich.

Eine Einwilligung muss insbesondere den folgenden Kriterien entsprechen:

- **Bezogen auf einen bestimmten Fall und einen bestimmten Zweck:** Eine „Pauschaleinwilligung“ wäre unwirksam. Sie muss sich auf einen konkreten Fall beziehen, nicht auf eine eher abstrakt beschriebene Vielzahl von Fällen. Und sie muss den Verarbeitungszweck konkret benennen, eine zu abstrakte Beschreibung führt zur Unwirksamkeit.
- **Freiwillig**: Eine Einwilligung ist nach dem Konzept der Datenschutzgrundverordnung nur dann „freiwillig“, wenn der Einwilligende die „echte oder freie Wahl hat und somit in der Lage ist, die Einwilligung zu verweigern oder zurückzuziehen, ohne Nachteile zu erleiden“ (Erwägungsgrund 42). Die Datenschutzgrundverordnung verlangt hier eine Abwägungsentscheidung.
- **In informierter Weise**: Die einwilligende Person muss wissen, dass und in welchem Umfang die Einwilligung erteilt wird. Vor allem sollte die Einwilligung klar auf eine bestimmte verantwortliche Stelle bezogen sein, auf die sich die Einwilligung bezieht. Gleichzeitig sollte der Einwilligende auf die Möglichkeit hingewiesen werden, die Einwilligung mit Wirkung (nur) für die Zukunft auch widerrufen zu können.
- **Unmissverständlich**: Sowohl das Ersuchen um Einwilligung als auch die Einwilligung selbst sollten in verständlicher und leicht zugänglicher Form und in einer klaren und einfachen Sprache erfolgen. Es besteht aber kein strenger Schriftformvorbehalt. Es reicht jede Form einer Erklärung oder einer sonstigen eindeutig bestätigenden Handlung, aus der sich ergibt, dass der Einwilligende mit der Verarbeitung der Daten einverstanden ist. Es gilt allerdings ein generelles „Opt-In“-Prinzip, d.h. reines Schweigen bzw. Untätigbleiben gilt nicht als Einwilligung. Vorausgewählte Checkboxen führen deshalb nicht zu einer wirksamen Einwilligung.
- **Nachweisbar**: Das reine Behaupten einer Einwilligung reicht im Zweifelsfall (z.B. in einem Gerichtsverfahren oder bei Audits einer Behörde) nicht aus. Die Beweispflicht für das Vorliegen einer Einwilligung liegt bei der verantwortlichen Stelle.
- **Vereinbar mit AGB-Recht**: Einwilligungsklauseln unterfallen darüber hinaus häufig auch der allgemeinen AGB-Inhaltskontrolle. Sie sind also z.B. auch dann unwirksam, wenn sie „missbräuchlich“ oder „überraschend“ sind.

Insgesamt sind die Vorgaben für wirksame Einwilligungserklärungen so eng geworden, dass Datenverarbeitungen, die sich ausschließlich auf Einwilligungserklärungen stützen in vielen Fällen in eine rechtliche Grauzone geraten.

9 Was muss eine wirksame Einwilligung inhaltlich beinhalten?

Eine Einwilligungserklärung muss konkret bezeichnen, auf welche Person, auf welche verantwortliche(n) Stelle(n) und auf welche Verwendungszwecke sie sich bezieht.

Eine „Pauschaleinwilligung“ wäre unwirksam – sowohl wenn sie sich auf ungenau bezeichnete Vielzahl von Fällen bezieht, als auch wenn sie keine konkrete Zweckbeschreibung enthält. Empfehlenswert ist es, auch Hinweise auf die Nutzung von Betroffenenrechten (Rücknahme der Einwilligung, Berichtigungs- und Löschungsrechte etc.) direkt in die Einwilligung aufzunehmen.

Vor der Erteilung einer Einwilligung ist in vielen Fällen ohnehin eine Information des Betroffenen über die Verwendung seiner personenbezogenen Daten verpflichtend. Eine Einwilligungserklärung kann hierauf Bezug nehmen.

10 Welche Reichweite hat eine Einwilligung innerhalb einer Organisation?

Grundsätzlich bezieht sich eine Einwilligung immer auf eine konkret zu benennende „verantwortliche Stelle“ – das ist im Zweifel nur ein einzelnes Unternehmen, keine ganze Unternehmensgruppe. Es ist aber möglich, eine Einwilligung so zu formulieren, dass sie auch mehrere Unternehmen gleichzeitig erfasst. Hierfür muss dann aus der Einwilligung klar erkennbar sein, welche Unternehmen der Einwilligende gemeint hat.

Es sind Konstellationen denkbar, in denen eine Einwilligung von einem einzelnen Konzernunternehmen eingeholt wird, dieses die Daten dann aber dennoch aus organisatorischen Gründen an andere Konzernunternehmen

weitergeben möchte. Dies kann ggf. auch auf Basis gesetzlicher Erlaubnisse erfolgen. Die arbeitsteilige Zusammenarbeit mehrerer Unternehmen innerhalb einer Unternehmensgruppe stellt häufig eine datenschutzrechtlich wirksame Rechtfertigung dar (Erwägungsgrund 48).

11 In welcher Form muss eine Einwilligung eingeholt werden, um wirksam zu sein?

Die Datenschutzgrundverordnung enthält – anders als das noch geltende Bundesdatenschutzgesetz in § 4a BDSG – keinen Vorrang der Schriftform. Es reicht somit letztlich jede hinreichend eindeutige Erklärung des jeweiligen Betroffenen aus. Weil das Vorliegen einer Einwilligung aber nachweisbar sein muss (Art. 7 Abs. 1), sollte die Erteilung der Einwilligung in jedem Fall zweifelsfrei dokumentiert werden – entweder durch Aufbewahrung der Dokumente, durch beweisfeste Protokolldaten oder auf anderem Weg.

12 Kann eine Einwilligung zur Bedingung für die Erbringung einer Leistung gemacht werden?

Nicht in jedem Fall, und nicht mit Rechtssicherheit. Denn die Datenschutzgrundverordnung sagt, dass an der „Freiwilligkeit“ der Einwilligung bereits dann zu zweifeln ist, wenn der Betroffene in größerem Umfang in die Verwendung seiner Daten einwilligt, als es für die Erbringung der Leistung notwendig ist (Art. 7 Abs. 4 und Erwägungsgrund 43). Dies gilt vor allem für Fälle, bei denen ein Bürger seine personenbezogenen Daten als „Zahlungsmittel“ einsetzt, indem er die datenschutzrechtliche Einwilligung gegen eine Dienstleistung „eintauscht“. Dies betrifft vor allem unentgeltliche Internetservices (z.B. Webmail), die hierdurch in eine rechtliche Grauzone geraten.

Die Datenschutzgrundverordnung bedeutet in diesem Punkt eine erhebliche Verschärfung gegenüber der früheren Rechtslage. Denn unter dem noch geltenden BDSG ist das „Koppeln“ eines Dienstleistungsangebotes an eine Einwilligung grundsätzlich zulässig, es sei denn diese Leistung ist für den Nutzer nicht auf anderem Weg erhältlich (§ 28 Abs. 3b BDSG). Das Koppeln ist aber auch nach der Datenschutzgrundverordnung nicht vollständig ausgeschlossen: Ob „Freiwilligkeit“ noch vorliegt, ergibt sich erst im Rahmen einer Abwägung, die alle Umstände des Einzelfalles mit einbezieht.

Rechtssicher ist das „Koppeln“ von Leistungsangebot und Einwilligung jedenfalls nur dann, wenn die betreffenden Daten auch für die Erbringung der angebotenen Leistung notwendig sind. Allerdings bedarf die Erhebung von Daten, die für die Erbringung einer vertraglich geschuldeten Dienstleistung notwendig sind, ohnehin keiner zusätzlichen Einwilligung (Art. 6 Abs. 1 b)).

13 Kann ein Arbeitgeber von einem Mitarbeiter im Rahmen des Arbeitsverhältnisses eine Einwilligung verlangen?

Grundsätzlich ja, aber gerade in solchen Fällen kann die „Freiwilligkeit“ einer Einwilligung zum Problem werden. Denn in vielen Fällen befindet sich ein Arbeitnehmer in einer Abhängigkeitsbeziehung zu seinem Arbeitgeber, er kann nicht „Nein sagen“. Ob dies der Fall ist, ist aber am Einzelfall zu beurteilen. Der Arbeitgeber kann die Freiwilligkeit der Einwilligung seiner Arbeitnehmer auch durch organisatorische Maßnahmen herstellen, z.B. indem er ausdrücklich betont, an eine Verweigerung der Einwilligung keine negativen Folgen anzuknüpfen. Hierbei können auch Betriebsvereinbarungen helfen, denn die Datenschutzgrundverordnung erkennt ausdrücklich an, dass die „Bedingungen, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage der Einwilligung des Beschäftigten verarbeitet werden dürfen“, auch im Kontext einer Betriebsvereinbarung geregelt werden können (Erwägungsgrund 155).

14 Können Minderjährige eine rechtswirksame Einwilligung abgeben?

In vielen Fällen nur mit Einverständnis ihres gesetzlichen Vertreters, in Deutschland also des Sorgeberechtigten. Eine wirksame Einwilligung ohne Mitwirkung des Sorgeberechtigten ist grundsätzlich erst ab dem Alter von sechzehn möglich (Art. 8). Auch bei sechzehn- oder siebzehnjährigen Personen sind allerdings an deren Vorabinformation zur Bedeutung ihrer Einwilligungserklärung besonders hohe Anforderungen zu stellen (Art. 12).

Die Mitgliedsstaaten können durch ein eigenes nationales Gesetz oder eine vergleichbare Anordnung die Altersgrenze auf bis zu dreizehn senken. Ob Deutschland oder andere Staaten hiervon Gebrauch machen werden, bleibt abzuwarten.

15 Ist eine Einwilligung zwischen Unternehmen übertragbar (z.B. im Rahmen von Adresshandel)?

Nein. Eine Einwilligung in den Adresshandel müsste sich von vornherein konkret auf das Empfängerunternehmen beziehen. Dies schließt die „typischen" Adresshandelskonstellationen aber aus, denn die Käufer solcher Adressdaten sind zum Zeitpunkt der Einwilligungserklärung normalerweise nicht bekannt, geschweige denn, dass sie in der Einwilligungserklärung einzeln benannt werden.

Nach der Datenschutzgrundverordnung bleibt Adresshandel aber auf Basis einer gesetzlichen Erlaubnisregel denkbar. Denn grundsätzlich ist die Übermittlung personenbezogener Daten bei einem „berechtigten Interesse" auch ohne Einwilligung des Empfängers erlaubt (Erwägungsgrund 47). Ob und unter welchen Bedingungen dies Adressdatenhandel ermöglichen wird, lässt sich auf Basis des Wortlauts noch nicht genau ablesen. Hier werden erst Stellungnahmen der Datenschutzbehörden und evtl. Gerichtsurteile Klarheit bringen.

16 Unter welchen Bedingungen darf ich Daten ohne Einwilligung verarbeiten?

Das bekannte Regelungskonzept des Verbots mit Erlaubnisvorbehalt bleibt auch nach der Verordnung bestehen. Das bedeutet, dass eine Datenverarbeitung nur zulässig ist, wenn die betroffene Person eingewilligt hat oder eine gesetzliche Erlaubnis die Verarbeitung legitimiert. Die gesetzlichen Erlaubnistatbestände sind dabei weitgehend deckungsgleich mit den bestehenden Regelungen.

a Vertragszweck

Eine in der Praxis besonders wichtige Erlaubnis bleibt auch nach der Verordnung die Verarbeitung von Daten zur Erfüllung eines Vertrages mit der betroffenen Person. Der Text der Verordnung entspricht weitgehend den Regelungen in der Datenschutzrichtlinie und im BDSG, so dass hier keine wesentlichen Änderungen zu erwarten sind. Es bleibt also weiterhin zulässig, personenbezogene Daten der betroffenen Person zu verarbeiten, wenn und soweit dies für die Begründung, Durchführung oder Beendigung eines Vertrages mit dem Betroffenen erforderlich ist. Welche Daten und Verarbeitungsvorgänge hiervon erfasst sind, ist dann im jeweiligen Einzelfall zu beurteilen.

b Interessensabwägung

Ebenfalls weiterhin zulässig bleibt eine Verarbeitung von personenbezogenen Daten, wenn und soweit dies zur Wahrung der berechtigten Interessen der verantwortlichen Stelle oder eines Dritten erforderlich ist, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen. Diese Regelung entspricht ebenfalls weitestgehend der bestehenden, so dass hier auch hier inhaltlich keine wesentlichen Änderungen zu erwarten sind. Ein Hauptanwendungsfall bleiben auch nach der Neuregelung die konzerninterne Übermittlungen von Kunden- und Beschäftigtendaten (siehe Erwägungsgrund 48).

In den Erwägungsgründen ist jedoch auch erwähnt, dass eine Verarbeitung für Direktmarketingzwecke auf diesen Erlaubnistatbestand gestützt werden kann. Neu ist, dass die Interessen besonders sorgfältig abzuwägen sind, wenn es sich bei der betroffenen Person um ein Kind handelt, da Kinder besonders schutzwürdig sind. Entsprechend sind an die berechtigten Interessen besonders hohe Anforderungen zu stellen, wenn Kinder betroffen sind (vgl. Art. 6 (f) am Ende). Eine weitere Neuerung ist, dass wenn eine Datenverarbeitung auf diesen Erlaubnistatbestand gestützt wird, die jeweiligen berechtigten Interessen im Rahmen der Informationspflichten mitzuteilen sind (vgl. Art. 14(2)(b)). Der Umfang dieser Informationspflicht, insbesondere ob auch nähere Informationen zur Abwägung mitzuteilen sind, ist derzeit noch nicht klar.

c Was gilt bei einer Zweckänderung/-erweiterung?

Auch nach der Verordnung besteht weiterhin der Zweckbindungsgrundsatz. Er wird jedoch dahingehend konkretisiert, dass für einen genau festgelegten, eindeutigen und rechtmäßigen Zweck erhobene personenbezogene Daten nicht in einer

mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden dürfen (Art. 5 (1)(b)). Um festzustellen, dass bei einer Zweckänderung keine solche unzulässige, also mit dem ursprünglichen Zweck unvereinbare, Verarbeitung erfolgt, hat die verantwortliche Stelle unter anderem nachfolgende Punkte zu beachten und im Rahmen ihrer Rechenschaftspflicht zu dokumentieren:

- jede Verbindung zwischen den Zwecken, für welche die Daten erhoben wurden, und den Zwecken der beabsichtigten Weiterverarbeitung;
- den Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere in Bezug auf das Verhältnis zwischen den Betroffenen und dem für die Verarbeitung Verantwortlichen;
- die Art der personenbezogenen Daten, insbesondere ob sensible Daten oder Daten in Bezug auf strafrechtliche Verurteilungen und Straftaten verarbeitet werden;
- die möglichen Folgen der beabsichtigten Weiterverarbeitung für die betroffenen Personen; sowie
- das Vorhandensein angemessener Garantien, die in einer Verschlüsselung oder einer Pseudonymisierung bestehen können.

Damit können Daten nunmehr grundsätzlich auch für andere Zwecke verarbeitet werden. Es muss jedoch eine Prüfung der oben genannten Punkte erfolgen und das Ergebnis der Prüfung sowie die wesentlichen Überlegungen sind im Rahmen der Rechenschaftspflicht zu dokumentieren.

d Sonderfall automatische Entscheidungen (z.B. Scoring)

Nach Art. 20 der Verordnung hat jeder das Recht, nicht einer allein auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die rechtliche Wirkung entfaltet oder auf andere vergleichbare Weise erheblich beeinträchtigt. Das heißt, grundsätzlich sind automatisierte Entscheidungen, die rechtliche Wirkungen haben oder in sonstiger Weise beeinträchtigen, unzulässig. Von diesem Grundsatz gibt es jedoch drei Einschränkungen, nämlich wenn die Entscheidung

1 für den Abschluss oder die Erfüllung eines Vertrages zwischen der betroffenen Person und der verantwortlichen Stelle erforderlich ist, oder

2 aufgrund von Rechtsvorschriften der EU oder eines Mitgliedstaates zulässig ist und die jeweilige Rechtsvorschrift geeignete Maßnahmen zur Wahrung der Rechte, Freiheiten und berechtigten Interessen der betroffenen Person enthalten, oder

3 mit ausdrücklicher Einwilligung erfolgt.

Im wichtigsten ersten sowie im dritten Fall hat die verantwortliche Stelle jedoch zum Schutz des Betroffenen geeignete Maßnahmen zu ergreifen, um die Interessen und Rechte des Betroffenen zu waren. Hierzu gehört mindestens das Recht auf persönliches Eingreifen des für die Verarbeitung Verantwortlichen, auf Darlegung des eigenen Standpunkts sowie das Recht auf Anfechtung der Entscheidung. Dadurch soll sichergestellt werden, dass der Betroffene eine Überprüfung der automatisierten Entscheidung erreichen kann und dieser nicht schutzlos ausgeliefert ist. Zudem sollen keine automatischen Entscheidungen gegenüber Kindern ergehen oder wenn sensible Daten betroffen sind (Erwägungsgrund 71).

e Voraussetzungen für die Verarbeitung von sensitiven Daten, insbesondere Gesundheitsdaten

Die Definition von „besonderen Kategorien personenbezogener Daten“ (=sensitive Daten) umfasst die bekannten Datenarten, d.h. Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit oder Informationen über Gesundheitszustand, Sexualleben oder sexuelle Orientierung hervorgehen, jedoch nunmehr auch ausdrücklich genetische und biometrische Daten. Wie nach den bestehenden Regelungen in der Datenschutzrichtlinie und dem Bundesdatenschutzgesetz gelten strengere Vorschriften für die Verarbeitung dieser sensitiven Daten. Teilweise decken sich die Erlaubnistatbestände mit den bestehenden Regelungen; es sind jedoch auch neue hinzugekommen, insbesondere für die Verarbeitung von Gesundheitsdaten. Nach den Erlaubnistatbeständen in der Verordnung ist eine Verarbeitung sensitiver Daten zulässig:

1 Wenn die Verarbeitung mit Einwilligung der betroffenen Person erfolgt. Dies entspricht der bisherigen Regelung, wobei die Mitgliedstaaten nunmehr ausdrücklich auch Fälle regeln können, in denen die Verarbeitung nicht auf eine Einwilligung gestützt werden kann.

2 Wenn die Verarbeitung erforderlich ist, um arbeits- oder sozialrechtliche Rechte und Pflichten des Betroffenen oder der verantwortlichen Stelle zu erfüllen; hierunter können auch Verarbeitungen zur Erfüllung von Vertriebsvereinbarungen fallen.

3 Wenn die Verarbeitung zum Schutz lebenswichtiger Interessen der betroffenen oder einer anderen Person erforderlich ist und die betroffenen Person aus physischen oder rechtlichen Gründen außer Stande ist, ihre Einwilligung zu geben. Dies entspricht der bisherigen Regelung.

4 Wenn die Verarbeitung durch Organisationen erfolgt, die politisch, philosophisch, religiös oder gewerkschaftlich ausgerichtet sind und keine Erwerbszwecke erfolgen, soweit dies für die Tätigkeit der Organisation erforderlich ist. Auch hier ist keine Änderung erfolgt.

5 Wenn (wie bisher) die betroffene Person die Daten offenkundig öffentlich gemacht hat.

6 Wenn die Verarbeitung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen (insoweit wie bisher) oder bei Handlungen der Gerichte in ihrer gerichtlichen Eigenschaft (das ist neu) erforderlich ist.

7 Wenn dies nach einer Rechtsvorschrift eines Mitgliedstaats zur Wahrung öffentlicher Interessen erforderlich ist. Diese weitere Öffnungsklausel ermöglicht es den Mitgliedstaaten, zusätzliche Erlaubnistatbestände im öffentlichen Interesse zu schaffen.

8 Wenn die Verarbeitung für Zwecke der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Arbeitnehmers, zum Schutz vor schwerwiegenden grenzüberschreitenden Gesundheitsbedrohungen, zur Gewährleistung hoher Standards bei der Gesundheitsversorgung oder zu weiteren in der Verordnung genannten Zwecken aus dem Bereich der Gesundheitsvorsorge und auf der Grundlage eines Unionsakts oder einer mitgliedstaatlichen Regelung erfolgt. Diese Regelungen erweitern die bisherigen Erlaubnistatbestände und schließen bestehende Lücken, indem sie beispielsweise die Übermittlung von Daten an Dienstleister im Gesundheitsbereich erleichtern. Wie ausgeführt, sind jedoch die jeweiligen mitgliedstaatlichen oder unionsrechtlichen Regelungen im Einzelfall zu prüfen und zu beachten.

9 Wenn die Verarbeitung für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungs- oder statistische Zwecke erforderlich ist.

17 Welche Anforderungen werden an die Bildung von Nutzerprofilen gestellt?

Die Regelungen zur Bildung von Nutzungsprofilen („Profiling“) wurden im Gesetzgebungsverfahren mehrfach diskutiert, insbesondere waren einschränkende Regelungen, darunter ein explizites Einwilligungserfordernis geplant, die jedoch letztlich nicht verabschiedet wurden. Ausweislich Erwägungsgrund 58a der Verordnung kann der Europäische Datenschutzausschuss (Nachfolgeinstitution der Art. 29 Gruppe) jedoch noch nähere Regeln zu Profiling verabschieden, was angesichts der überschaubaren Regelungen noch zu erwarten ist. Bis dahin besteht leider ein erhebliches Maß an Rechtsunsicherheit.

Der Begriff „Profiling“ ist in der Verordnung definiert als „jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen“ (Art. 4 Nr. 4).

a Wann ist dies zulässig?

Bei der Frage nach der Zulässigkeit von Profiling ist zu trennen zwischen den Anforderungen an das Profiling an sich und der zugrundeliegenden jeweiligen Datenverarbeitung, z.B. die Generierung von Nutzungsprofilen anhand von Internetnutzungsdaten für Werbezwecke. Denn das Profiling bezeichnet nur eine bestimmte Art der Datenverarbeitung (siehe Definition oben), welche die Datenschutzinteressen der Betroffenen jedoch in besonderem Maße berührt und daher gegenüber sonstigen Verarbeitungen zusätzlichen Anforderungen unterliegt (hierzu unten). Die Zulässigkeit der jeweiligen Datenverarbeitung ist nach den allgemeinen Erlaubnistatbeständen zu beurteilen.

b Welche zusätzlichen Anforderungen muss ich einhalten?

Die zusätzlichen Anforderungen beim Profiling sind ein Widerspruchsrecht des Betroffenen sowie erweiterte Informationspflichten.

Ein Widerspruchsrecht besteht, wenn Profiling eingesetzt wird, um Direktwerbung zu betreiben sowie wenn die Datenverarbeitung auf die Erlaubnistatbestände der berechtigten Interessen oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse gestützt wird. Damit dürfte für den wichtigen Anwendungsfall des Profilings für Werbezwecke stets ein Widerspruchsrecht bestehen. Übt der Betroffene sein Widerspruchsrecht aus, dürfen die Daten nicht mehr weiterverarbeitet werden, es sei denn es bestehen zwingende schutzwürdige Gründe für die Verarbeitung, welche die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen oder die Verarbeitung dient der Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen. Diese hohen Anforderungen werden selten erfüllt sein. Hinsichtlich der Ausübung des Widerspruchsrechts ist nunmehr ausdrücklich geregelt, dass dies (unbeschadet der Vorgaben der ePrivacy Directive) auch durch technische Verfahren (z.B. Browservoreinstellungen) ausgeübt werden kann.

Weitere Anforderung ist, dass der Betroffene über eine Verarbeitung im Wege des Profiling zu informieren ist und dabei sind auch Angaben über die verwendete Logik sowie zur Tragweite und zu den angestrebten Auswirkungen einer derartigen Verarbeitung für die betroffene Person zu machen.

Schließlich ist für den Sonderfall der ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung (siehe dazu auch Frage 16.d.) auf der Basis von Profiling geregelt, dass in diesem Fall die betroffene Person stets das Recht hat, keiner solchen Entscheidung unterworfen zu sein, wenn diese ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dies soll jedoch nicht gelten, wenn die Entscheidung für den Abschluss oder die Erfüllung eines Vertrags zwischen der betroffenen Person und dem Verantwortlichen erforderlich ist, mit ausdrücklicher Einwilligung der betroffenen Person oder aufgrund von mitgliedstaatlichen oder unionsrechtlichen Vorschriften erfolgt.

c Ist die Verordnung das Ende von Big Data?

Die Verordnung wird mit Sicherheit nicht das Ende von Big Data bedeuten. Im Gegenteil: Im Vergleich zu den während des Gesetzgebungsverfahrens diskutierten Einschränkungen (die praktisch immer die in der Realität meist nicht einholbare Einwilligung verlangt hätten) sind die letztlich verabschiedeten Regelungen vergleichsweise Big Data-freundlich (siehe dazu auch den vorherigen Absatz). Es ist jedoch noch zu früh, hierzu eine Prognose abzugeben und es bleibt abzuwarten, wie die neuen Regelungen in der Praxis angewandt und von den Datenschutzbehörden und Gerichten verstanden werden. Zudem ist davon auszugehen, dass der Europäische Datenschutzausschuss in diesem Bereich noch tätig wird und Richtlinien und Handlungsanweisungen veröffentlicht.

18 Muss ich betroffenen Personen Zugang zu den über sie gespeicherten personenbezogenen Daten gewähren?

Betroffene Personen (zum Begriff oben Frage 4) haben nach Art. 15 der Verordnung Auskunftsansprüche. Zunächst ist ihnen auf Nachfrage mitzuteilen, ob über sie personenbezogene Daten gespeichert sind. Ist dies der Fall, so haben Sie Anspruch auf eine Kopie der gespeicherten Daten. Einmal jährlich ist die Kopie unentgeltlich, für weitere Kopien kann ein angemessenes Entgelt verlangt werden. Im Falle eines elektronischen Antrags der betroffenen Person können diese Informationen in elektronischer Form erteilt werden.

19 Welche Informationen müssen bei einer Anfrage durch eine betroffene Person übermittelt werden?

Neben den Auskünften gemäß obiger Frage 18 sind betroffene Personen zu Auskunft über folgende Punkte berechtigt:

- Verarbeitungszwecke,
- verarbeitete Datenkategorien,
- Empfänger oder Kategorien von Empfängern denen Daten offengelegt werden, insbesondere bei Empfängern in Drittstaaten oder internationalen Organisationen,
- geplante Speicherdauer bzw. Kriterien für die Festlegung der Speicherdauer

- Herkunft der Daten, und
- darüber, ob die Daten für automatisierte Entscheidungsfindung oder Profiling verwendet werden.

Außerdem sind betroffene Personen auf die Rechte der Berichtigung und Löschung, Widerspruch gegen die Verarbeitung und das Beschwerderecht gegenüber der Aufsichtsbehörde hinzuweisen.

Falls die Daten in Drittländern oder bei internationalen Organisationen übermittelt werden, sind betroffene Personen auch dazu berechtigt, über die geeigneten Garantien nach Art. 46 im Zusammenhang mit der Übermittlung (siehe dazu Frage 23) unterrichtet zu werden.

20 Wann müssen Informationen auch ohne Anfrage proaktiv zur Verfügung gestellt werden?

Betroffene Personen sind über sie betreffende Datenverarbeitungsvorgänge zu informieren. Werden die zu verarbeitenden Daten von ihnen direkt erhoben, hat die Information zum Zeitpunkt der Erhebung zu erfolgen. Ansonsten muss die Information innerhalb angemessener Frist erfolgen, spätestens nach einem Monat. Nimmt der Verantwortliche mit der betroffenen Person Kontakt auf, hat die Information bei der ersten Kontaktaufnahme zu erfolgen. Ist beabsichtigt, die erhobenen Daten anderen offenzulegen, muss die Information spätestens gleichzeitig mit der Offenlegung erfolgen.

Der Verantwortliche muss der betroffenen Person umfangreiche Informationen über die beabsichtigte Datenverarbeitung zur Verfügung stellen. Dazu gehören

- Name und Kontaktdaten des Verantwortlichen, seiner gesetzlichen Vertreter und des etwa bestellten Datenschutzbeauftragten,
- Zwecke und Rechtsgrundlage der Datenverarbeitung,
- Empfänger bzw. Kategorien von Empfängern falls die Daten an Dritte übermittelt werden sollen, sowie
- Angaben zu einer beabsichtigten Übermittlung von Daten in Drittländer oder internationale Organisationen sowie zu deren Rechtsgrundlage.

Außerdem müssen Verantwortliche den betroffenen Personen Informationen zur Verfügung stellen, um die Fairness und Transparenz der Verarbeitung sicherzustellen. Hierzu gehören Angaben zur Speicherdauer, zur Widerruflichkeit einer etwa erteilten Einwilligung, und zu den Betroffenenrechten auf Auskunft, Berichtigung, Löschung und Beschwerde bei den Aufsichtsbehörden.

Soll der Verarbeitungszweck für gespeicherte Daten später geändert werden, müssen betroffene Personen erneut informiert werden.

21 Welchen Pflichten zur Datenlöschung muss ich nachkommen?

Die Datenschutzgrundverordnung enthält eine Reihe von Fällen, in denen der Verantwortliche zur Löschung personenbezogener Daten verpflichtet ist. Der wichtigste und häufigste Fall dürfte sein, dass gespeicherte Daten nicht mehr für die Zwecke erforderlich sind, für die sie ursprünglich erhoben wurden. Weitere eine Löschungspflicht begründende Fälle sind, dass die betroffene Person ihre Einwilligung widerruft und eine andere Rechtsgrundlage für die Datenverarbeitung nicht zur Verfügung steht, die Datenverarbeitung sich als rechtswidrig erweist oder (spezifische) rechtliche Pflichten zur Datenlöschung aus Unionsrecht oder dem Recht der Mitgliedstaaten resultieren.

Wenn der Verantwortliche die zu löschenden Daten an Dritte weitergegeben hat, so muss er grundsätzlich im Falle der Löschung alle Empfänger darüber informieren, es sei denn, dies ist unmöglich oder verursacht unverhältnismäßigen Aufwand.

22 Muss ich einem Nutzer ermöglichen, die von ihm hinterlegten Daten zu einem anderen Dienst überführen zu können?

Die Datenschutzgrundverordnung enthält ein Recht auf Datenportabilität. Danach haben Betroffene das Recht, auf Grundlage von Einwilligung oder Vertrag automatisiert verarbeitete Daten, die sie dem Verantwortlichen zur Verfügung gestellt haben, in maschinenlesbarer Form in Kopie zu erhalten, um sie zu einem anderen Anbieter zu portieren. Dazu dürfen betroffene Personen auch verlangen, dass die Portierung direkt vom alten zum neuen Verantwortlichen erfolgt, soweit dies technisch machbar ist. Jedoch darf diese Direktportierung die

Rechte und Freiheiten Dritter nicht beeinträchtigen, wobei fraglich ist, wie die beteiligten Verantwortlichen dies feststellen und beurteilen sollen.

Insgesamt ist dies jedoch in jedem Fall eine grundlegende Neuerung und eine Regelung, die über den eigentlichen Kernbereich des Datenschutzes (Schutz der Privatsphäre) hinausgeht. Die Auswirkungen auf die Praxis können erheblich sein.

23 Welche speziellen Anforderungen gibt es für internationale Datentransfers, insbesondere in die USA?

Datentransfers in Drittstaaten (also in Länder außerhalb des Europäischen Wirtschaftsraumes) werden auch weiterhin durch die Datenschutzgrundverordnung reguliert und beschränkt. Die Voraussetzungen für einen Transfer sind grundsätzlich die Gleichen, wie nach gegenwärtigem Recht. Die bisherigen Instrumente für eine Datenübermittlung, wie ‚Binding Corporate Rules' und ‚Standardvertragsklauseln' oder die Möglichkeit des Datentransfers auf Grundlage einer Einwilligung oder zur Erfüllung eines Vertrages, bleiben bestehen. Die auf Grundlage der Datenschutzrichtlinie 95/46/EG von der Kommission erlassenen Beschlüsse über ein angemessenes Datenschutzniveau in verschiedenen Ländern werden ebenfalls in Kraft bleiben (können aber natürlich, wie bisher auch, durch neue Beschlüsse der Kommission aufgehoben, ersetzt oder abgeändert werden).

Neu ist aber vor allem Folgendes:

- Die Kommission darf mit Wirkung für die gesamte Union beschließen, dass auch ein Gebiet oder ein bestimmter Sektor eines Drittlands oder eine internationale Organisation ein angemessenes Datenschutzniveau bietet (früher war dies nur für ein bestimmtes Drittland möglich).
- Ausnahmsweise sollen auch Übermittlungen, die als nicht wiederholt erfolgend gelten können und nur eine begrenzte Zahl von betroffenen Personen betreffen, auch zur Wahrung zwingender berechtigter Interessen des Verantwortlichen möglich sein, sofern die Interessen oder Rechte und Freiheiten der betroffenen Person nicht überwiegen.
- Die Datenschutzgrundverordnung regelt nunmehr ausdrücklich ‚Binding Corporate Rules' und legt insoweit bestimmte Mindestanforderungen bezüglich des notwendigen Inhalts fest.

Daneben sieht die Verordnung nun auch bestimmte Verhaltensregeln (sog. „Code of Conduct") und die Möglichkeit einer Zertifizierung vor, welche vorbehaltlich einer Genehmigung durch die zuständige Aufsichtsbehörden ebenfalls Grundlage für eine Datenübermittlung sein können.

Datentransfers in Drittstaaten werden daher nach wie vor für Unternehmen ein wichtiges Compliance-Thema bleiben, gerade auch vor dem Hintergrund, dass die entsprechenden Vorschriften vom Katalog umfasst sind, für den potentiell Strafen in Höhe von 4 Prozent des gesamten weltweit erzielten Jahresumsatzes eines Unternehmens verhängt werden können und dass Non-Compliance nunmehr nicht nur die verantwortliche Stelle sondern auch den Auftragnehmer treffen kann.

24 Unter welchen Umständen wird eine Auftragsdaten-verarbeitungsvereinbarung benötigt?

Die Datenschutzgrundverordnung basiert in weiten Teilen auf dem in Deutschland anerkannten Konzept der Auftragsdatenverarbeitung und ist an vielen Stellen § 11 BDSG nachgebildet. Die Verwendung eines Auftragsdatenverarbeiters bedarf daher auch in Zukunft generell eines schriftlichen oder in elektronischer Form geschlossenen Vertrages. Eine Ausnahme soll nur gelten, wenn ein anderes Rechtsinstrument nach dem Unionsrecht oder dem Recht der Mitgliedstaaten besteht, welches den Auftragsdatenverarbeiter in Bezug auf den Verantwortlichen bindet und in dem Gegenstand und Dauer der Verarbeitung, Art und Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Pflichten und Rechte des Verantwortlichen festgelegt sind. Inwieweit und in welchem Umfang solche Rechtsinstrumente zur Verfügung stehen werden, ist derzeit ebenfalls noch nicht abzusehen.

Für Dienstleister in diesem Zusammenhang besonders relevant ist, dass im Falle eines Verstoßes gegen die Verpflichtungen eines Auftragsdatenverarbeiters (d.h. ein Handeln entgegen der (vertraglichen) Weisungen des

Verantwortlichen) der Auftragsdatenverarbeiter selbst zum Verantwortlichen wird. Auch haben Betroffene nunmehr nicht nur einen direkten Schadensersatzanspruch gegen den Verantwortlichen, sondern auch gegen den Auftragsdatenverarbeiter – die Haftung wurde insoweit also ausgeweitet.

25 Was muss eine Auftragsdatenverarbeitungsvereinbarung beinhalten?

Inhaltlich entsprechen die Vorgaben der Datenschutzgrundverordnung mehr oder weniger den Vorgaben von § 11 Abs. 2 BDSG, so dass deutsche verantwortliche Stellen mit entsprechenden Auftragsdatenverarbeitungsverträgen die neuen Regelungen bereits grundsätzlich erfüllen (kleinere Anpassungen werden wohl trotzdem notwendig sein). Es ist zu erwarten, dass die Kommission (unmittelbar) oder Aufsichtsbehörden im Kohärenzverfahren Standardvertragsklauseln zur Einhaltung der neuen Regelungen zur Verfügung stellen werden (die entsprechende Ermächtigung ist jedenfalls geregelt). Insoweit wäre ein Gleichlauf mit den bisher bestehenden Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Drittländer(n) (2010/87/EU) wünschenswert.

Sowohl der Verantwortliche als auch der Auftragsdatenverarbeiter sind nach wie vor verpflichtet, geeignete technische und organisatorische Maßnahmen für die Sicherheit der Datenverarbeitung zu treffen.

Ähnlich dem deutschem Vorbild muss sich der Verantwortliche auch nach der Verordnung vor Beginn der Datenverarbeitung davon überzeugen, dass der Auftragsdatenverarbeiter hinreichende Garantien dafür bietet, dass technische und organisatorische Maßnahmen – auch für die Sicherheit der Verarbeitung – getroffen werden, insbesondere auch im Hinblick auf Fachwissen, Zuverlässigkeit und Ressourcen des Auftragsdatenverarbeiters. Insoweit kann – und das ist neu – die Einhaltung der Verpflichtungen bezüglich der technisch-organisatorischen Maßnahmen durch den Auftragnehmer durch die Einhaltung von genehmigten Verhaltensregeln (sog. „Code of Conduct“) oder durch eine genehmigte Zertifizierung nachgewiesen werden.

26 Wofür muss ich mich registrieren oder sogar (vorab) eine Genehmigung der Aufsichtsbehörde einholen?

Eine der positiven Errungenschaften der Datenschutzgrundverordnung ist die Reduzierung der formalen Anforderungen. Das wirkt sich sowohl auf aufsichtsbehördliche Registrierungs- bzw. Genehmigungspflichten als auch auf die Bestellung eines Datenschutzbeauftragten aus. Nach dem geltenden Recht unter der Richtlinie 95/46/EG sind die Mitgliedsstaaten verpflichtet, umfassende Meldepflichten einzuführen, die allerdings teilweise entfallen können, wenn nach dem Recht der Mitgliedstaaten in den jeweiligen Unternehmen Datenschutzbeauftragte bestellt werden. Von dieser Möglichkeit hat insbesondere Deutschland Gebrauch gemacht. In den meisten anderen europäischen Ländern ist das aber nicht der Fall. Hier bestehen nach geltendem Recht umfassende Meldepflichten bezüglich der Verarbeitung von personenbezogenen Daten als solche bzw. den relevanten Datenverarbeitungsvorgehen gegenüber den lokalen Datenschutzbehörden. Diese allgemeinen Meldepflichten wurden nun in der Datenschutzgrundverordnung abgeschafft.

Stattdessen führt die Datenschutzgrundverordnung verschiedene Verfahren und Mechanismen ein, die sich mit besonders sensiblen Datenverarbeitungen befassen (neben neuartigen Datenverarbeitungen kommt hier insbesondere der Einsatz neuer Technologien in Betracht). Hier ist vor allem das Verfahren der vorherigen Konsultation zu nennen, welches Anwendung finden soll, wenn aus einer Datenschutz-Folgenabschätzung (siehe hierzu näher Frage 30) hervorgeht, dass aus der Verarbeitung ein hohes Risiko resultieren würde, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft. ‚Ex post‘ Meldepflichten bestehen auch im Fall von bestimmten Verletzungen des Schutzes personenbezogener Daten (siehe hierzu näher Frage 32).

Genehmigungspflichten sind in der Datenschutzgrundverordnung über verschiedene Abschnitte verteilt geregelt. Sie bestehen insbesondere im Zusammenhang mit:

- vorheriger Konsultation bei im öffentlichen Interesse liegenden Aufgaben gemäß Artikel 36 Absatz 5;

- Verhaltensregeln („Code of Conduct“) gemäß Artikel 40 Absatz 5;
- Erteilungen von Zertifizierungen nach Artikel 42 Absatz 5,
- individuelle Vertragsklauseln im Rahmen einer Datenübermittlung in ein Drittland gemäß Artikel 46 Absatz 3 Buchstabe a, und
- verbindlichen internen Vorschriften gemäß Artikel 47 („Binding Corporate Rules“).

Weitere Genehmigungspflichten können durch mitgliedstaatliches Recht vorgesehen werden, etwa bei der Verarbeitung zur Erfüllung einer im öffentlichen Interesse liegenden Aufgabe, einschließlich der Verarbeitung zu Zwecken der sozialen Sicherheit und der öffentlichen Gesundheit.

27 Wann benötige ich einen Datenschutzbeauftragten?

Die Pflicht, einen Datenschutzbeauftragten zu bestellen, ist für Verantwortliche in der Datenschutzgrundverordnung weniger stringent ausgeprägt, als dies im derzeitigen deutschen Recht der Fall ist. Dies heisst aber nicht, dass die Pflichten insbesondere für internationale Unternehmen insoweit grundsätzlich heruntergefahren werden. Zwar bedeutet die zukünftige Regelung eine Erleichterung für kleinere Unternehmen, dadurch dass nicht mehr automatisch die Bestellung eines Datenschutzbeauftragten nach deutschem Recht erforderlich ist. Auf der anderen Seite erstreckt sich nun die Verpflichtung (wenn einschlägig) auf die gesamte europäische Union beziehungsweise alle in den Mitgliedstaaten befindlichen Niederlassungen eines Unternehmens. Auch wird die Aufgabe des Datenschutzbeauftragten aufgrund der gestiegenen Compliance-Anforderungen (dazu siehe die Fragen 29 ff.) größer.

Nach der Verordnung besteht die Pflicht, einen Datenschutzbeauftragten zu bestellen, zunächst grundsätzlich für öffentliche Stellen (Ausnahme: Gerichte für den Bereich der Rechtspflege). Sie besteht daneben für alle nicht-öffentlichen Stellen, (i) deren Kerntätigkeit in Verarbeitungsvorgängen liegt, (ii) die eine umfangreiche regelmäßige und systematische Überwachung der betroffenen Personen bewirken, sowie (iii) die in großem Umfang mit sensitiven Daten oder Daten über strafrechtliche Verurteilungen oder Straftaten umgehen. Die Verpflichtung zur Bestellung eines Datenschutzbeauftragten dürfte damit sehr viele Unternehmen treffen, insbesondere regelmäßig Unternehmen der Digitalwirtschaft sowie größere Unternehmen.

Dazu kommt, dass die Mitgliedstaaten im nationalen Recht die Pflicht zur Bestellung von Datenschutzbeauftragten ausweiten können. Im Einklang mit dem bisherigen deutschen Recht ist es gut möglich, dass der deutsche Gesetzgeber diese Möglichkeit nutzen wird und die Pflicht zur Bestellung eines Datenschutzbeauftragten ausweiten wird.

28 Welche Datenschutzbehörde ist für mich zuständig, national und international?

Die Datenschutzgrundverordnung führt den sog. „One-Stop-Shop-Mechanismus“ (also das Prinzip, dass für ein Unternehmen nur noch eine Datenschutzbehörde zuständig ist) ein, zumindest ist dies das erklärte Ziel der Verordnung. In der Umsetzung ist der „One-Stop-Shop“ allerdings stark verwässert worden.

Zwar gilt zunächst der Grundsatz, dass für ein Unternehmen, welches Niederlassungen in mehreren EU-Mitgliedstaaten hat, formell nur die Aufsichtsbehörde am Hauptsitz des Unternehmens zuständig ist (sog. „federführende Aufsichtsbehörde“). Allerdings gelten zahlreiche Einschränkungen. Erstens können sich Betroffene auch weiterhin mit Beschwerden an die Datenschutzaufsichtsbehörde an ihrem jeweiligen Wohnsitz wenden. Diese werden somit involviert und ihre (gegebenenfalls abweichende) Meinung einbringen. Zu noch mehr Komplikationen dürfte in der Praxis die Verpflichtung der federführenden Aufsichtsbehörde führen, andere nationale Datenschutzbehörden einzuschalten, wenn natürliche Personen aus ihren Ländern betroffen sind. Immer dann wird ein Abstimmungsmechanismus zwischen den Aufsichtsbehörden erforderlich werden. Die federführende Aufsichtsbehörde soll lediglich Hauptansprechpartner sein und für die Durchsetzung des Datenschutzrechts gegenüber dem Verantwortlichen zuständig sein. Wenn immer mehrere Aufsichtsbehörden betroffen sind, werden diese im Rahmen eines neu eingeführten Kooperationsmechanismus jedoch in das Verfahren einbezogen. Die federführende Behörde muss im Rahmen ihres Beschlusses der Stellungnahme der betroffenen Aufsichtsbehörden „gebührend Rechnung“ tragen. Was dies in der Praxis genau heißt und wie sich dieses System bewähren wird,

bleibt abzuwarten. Es besteht aber zu befürchten, dass hier erhebliche Bürokratie erzeugt wird und die erhofften Vorteile des One-Stop-Mechanismus nicht oder nur eingeschränkt erreicht werden.

Soweit der Verantwortliche keine Niederlassung in der EU hat, die Datenschutzgrundverordnung aber dennoch anwendbar ist (in sog. „Marktortfällen"), greift der zuvor genannte Abstimmungsmechanismus aber nicht. Insoweit soll jede Aufsichtsbehörde im Hoheitsgebiet ihres Mitgliedstaats zuständig sein und für die entsprechende Rechtsdurchsetzung sorgen (es kann hierbei also durchaus zu abweichenden/divergierenden Entscheidungen kommen).

Im öffentlichen Bereich erhalten die Datenschutzbehörden neue Befugnisse und werden unter anderem ermächtigt, gegenüber anderen Behörden tätig zu werden und Anordnungen zu erlassen (dies ist in dieser Form ein Novum im deutschen Verwaltungsrecht).

29 Was sind meine sonstigen Compliance-Anforderungen? Was muss ich evaluieren und was muss ich dokumentieren?

Zunächst ist festzuhalten, dass die Compliance-Anforderungen an Unternehmen nach der Datenschutzgrundverordnung stark ansteigen werden. Es ist erklärtes Ziel der Verordnung, dass Unternehmen mehr in die Pflicht genommen werden, relevante Datenverarbeitungsvorgänge vernünftig zu dokumentieren und ihre Organisation so auszugestalten, dass die Einhaltung des Datenschutzrechts sichergestellt wird. Eine umfassende Zusammenfassung aller Compliance-Anforderungen nach der Verordnung würde den Rahmen sprengen. Neben der Bestellung eines Datenschutzbeauftragten (dazu Frage 27) sind folgende Anforderungen besonders zu erwähnen:

- Datenverarbeitungen im Auftrag müssen vertraglich geregelt werden. Entsprechende Verträge müssen insbesondere Aufsichts- und Weisungsrechte des Auftraggebers sowie die Maßnahmen zur Gewährleistung der Datensicherheit festlegen.
- Verantwortliche und deren Auftragsdatenverarbeiter müssen geeignete technische und organisatorische Maßnahmen ergreifen, um gespeicherte Daten und deren Verarbeitungsvorgänge vor Verlust, unerlaubtem Zugriff und vergleichbaren Risiken zu schützen.
- Verantwortliche müssen ein Verzeichnis der Verarbeitungstätigkeiten führen. Dies ähnelt dem bislang in Deutschland bekannten Verfahrensverzeichnis. Inhalt sind etwa Angaben zu den Zwecken der Datenverarbeitung, Kategorien von betroffenen Personen und verarbeiteten Daten, Angaben zu einer etwa beabsichtigten Offenlegung von Daten an Dritte und ggfs in Drittländer sowie eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Gewährleistung der Datensicherheit. Unternehmen mit weniger als 250 Beschäftigten sind unter gewissen Voraussetzungen von dieser Pflicht ausgenommen.
- Unternehmen müssen bei der Entwicklung ihrer Prozesse und Produkte dem Datenschutz durch „privacy by design" Rechnung tragen und bei besonders kritischen Vorgängen ein „data protection impact assessment" vornehmen (zu beiden siehe unten Frage 30).

Insgesamt ist die interne Organisation so aufzustellen, dass Datenschutzverstöße vermieden werden. Dazu gehören interne Audits und Code of Conducts. Lässt ein Unternehmen es diesbezüglich an der notwendigen Sorgfalt vermissen, wird dies insbesondere bei Datenschutzverstößen und der Frage, ob diese mit Strafen geahndet werden (und in welcher Höhe), relevant sein. Angesichts der hohen Strafandrohungen nach der Datenschutzgrundverordnung (bis zu 4 Prozent des Jahresumsatzes) ist das ein ganz wesentlicher Punkt.

30 Was meint "privacy by design" und was ist das „data protection impact assessment"?

Es handelt sich hierbei um zwei unterschiedliche Anforderungen der Richtlinie.

„Privacy by Design" (Deutsch: Datenschutz durch Technikgestaltung) ist eine allgemeine Anforderung an die Auslegung von Datenverarbeitungsvorgängen. Der Verantwortliche soll organisatorische und technische Maßnahmen treffen, die darauf ausgerichtet sind, Datenschutzgrundsätze wie etwa die Datenminimierung bereits bei der Planung unternehmensinterner Prozesse sowie von Produkten und Dienstleistungen wirksam

umzusetzen und die Datenverarbeitung so zu gestalten, dass sie den Anforderungen der Richtlinie genügt. Hier handelt es sich letztlich um einen allgemeinen Grundsatz, der in der Grundverordnung bisher nicht konkretisiert ist und der daher noch der Ausgestaltung durch Vorgaben der Datenschutzbehörden und/oder Industriestandards bedarf. Man wird aber zumindest davon ausgehen müssen, dass es in Zukunft schwerer sein wird zu argumentieren, dass umfassende Verarbeitungen personenbezogener Daten aufgrund unternehmensinterner Prozesse oder des Designs von Produkten unumgänglich sind. Vielmehr steht das Erfordernis, bereits bei der (insbesondere technischen) Gestaltung von Produkten und Abläufen den Datenschutz im Blick zu haben.

„Data Protection Impact Assessment“ (Deutsch: Datenschutz-Folgenabschätzung) ist demgegenüber eine deutlich konkretere Anforderung. Sie ist vorzunehmen, wenn eine Datenverarbeitung besondere Risiken für die Rechte und Freiheiten betroffener Personen beinhaltet. Dazu gehören insbesondere Datenverarbeitungen, die eine systematische und umfassende Bewertung persönlicher Aspekte der Betroffenen beinhalten und als Grundlage für rechtserhebliche Entscheidungen dienen (Beispiele: Profiling und Scoring) sowie umfangreiche Verarbeitungen sensitiver Daten (siehe dazu Frage 16 e.). Die Aufsichtsbehörden sollen Listen von Verarbeitungsvorgängen veröffentlichen, für die eine Folgenabschätzung durchzuführen ist.

Eine Datenschutz-Folgenabschätzung soll mindestens folgende Punkte abdecken:

- Beschreibung der Datenverarbeitungsvorgänge und ihrer Zwecke,
- Bewertung von Notwendigkeit und Erforderlichkeit der Datenverarbeitung bezogen auf ihren Zweck,
- Bewertung von Risiken für Rechte und Freiheiten der Betroffenen,
- Beschreibung von zur Bewältigung der Risiken beabsichtigten Abhilfemaßnahmen, wozu etwa Maßnahmen zum Schutz der Daten und Nachweise zur Einhaltung der Verordnung gehören. Dabei kann auch die Einhaltung von Codes of Conduct (dazu Frage 31) berücksichtigt werden.

31 Wozu dient ein “Code of Conduct” und eine Zertifizierung?

„Codes of Conduct“ sind Verhaltensregeln (so auch die deutsche Bezeichnung in der Verordnung) für den Umgang mit personenbezogenen Daten, die von Verbänden ausgearbeitet werden und von den Aufsichtsbehörden geprüft und genehmigt werden. Sie sollen die wirksame Einhaltung der Verordnung erleichtern. Ihre Einhaltung kann als Nachweis dienen, dass auch die Verordnung eingehalten wird. Die Einhaltung von Verhaltensregeln selbst ist durch dazu von den Aufsichtsbehörden zugelassene („akkreditierte“) Stellen zu überprüfen.

Zertifizierungen haben ebenfalls eine Nachweisfunktion für die Einhaltung der Verordnung. Nachdem ein Verantwortlicher eine Zertifizierung erfolgreich durchlaufen hat, gilt diese für drei Jahre. Der Verantwortliche darf die Zertifizierung dann auch werblich nutzen, etwa indem er Geschäftspartner und Kunden darauf hinweist. Zertifizierungen werden von dafür durch die Aufsichtsbehörden oder nationale Akkreditierungsstellen zugelassene Zertifizierungsstellen vorgenommen, können aber auch durch die Aufsichtsbehörden selbst erfolgen. Die Kriterien für die Zertifizierung werden durch die Aufsichtsbehörden erstellt. Es ist auch vorgesehen, europaweit geltende Zertifizierungskriterien durch den Europäischen Datenschutzausschuss aufstellen zu lassen. Deren Einhaltung soll dann zu einer gemeinsamen Zertifizierung, dem Europäischen Datenschutzsiegel, führen. Alle Zertifizierungsverfahren sollen vom Datenschutzausschuss in einer zu veröffentlichenden Liste publik gemacht werden.

Zertifizierungen dürften nach der Datenschutzgrundverordnung damit weiter an Bedeutung gewinnen. Insbesondere für Dienstleister (Auftragsdatenverarbeiter) im digitalen Umfeld können Zertifizierungen ein Qualitätssiegel darstellen. Es ist auch vorstellbar, dass Zertifizierungen sich in bestimmten Branchen als notwendiger Standard herausbilden, um überhaupt Kundengeschäft zu akquirieren.

32 Gibt es eine gesonderte Informationspflicht bei Datenverlusten oder einem Hackerangriff oder gar Datenschutzverstößen im Allgemeinen?

Nach dem geltenden deutschen Recht gibt es unter bestimmten Umständen eine Informationspflicht gegenüber Datenschutzbehörden und/oder den betroffenen Datensubjekten. Dies ist aber beschränkt auf besondere Daten (insbesondere sensitive Daten) und gilt nur für den Fall der unrechtmäßigen Kenntniserlangung durch Dritte. Nach der Datenschutzgrundverordnung wird die Informationspflicht erheblich ausgeweitet.

Zum einen beschränkt sich die Informationspflicht nicht auf die unrechtmäßige Kenntniserlangung durch Dritte, sondern gilt für jegliche Verletzung des Schutzes personenbezogener Daten. Anders als nach derzeitiger Rechtslage werden diese Informationspflichten des Weiteren nicht auf Fälle beschränkt, in denen besonders sensible Daten von dem Vorfall betroffen sind. Nach dem Wortlaut der Datenschutzgrundverordnung (Art. 33 f.) greifen somit bei **jeder** Verletzung des Schutzes personenbezogener Daten die abgestuften Dokumentations-, Melde-, und Informationspflichten. Die Pflichten variieren je nach den Risiken, die der Vorfall für die betroffenen Personen hat:

- Alle Datenschutzverletzungen sind intern zu dokumentieren.
- Datenschutzverletzungen sind an die Aufsichtsbehörden zu melden, außer wenn der Vorfall voraussichtlich nicht zu einem Risiko für die Betroffenen führt. Die Meldung soll binnen 72 Stunden erfolgen und eine Beschreibung des Vorfalls, der wahrscheinlichen Folgen, der vorgeschlagenen oder ergriffenen Abhilfemaßnahmen und Kontaktinformation für Rückfragen enthalten.
- Ist zu befürchten, dass eine Datenschutzverletzung ein hohes Risiko für die Betroffenen auslöst, so sind diese zu benachrichtigen. Die Benachrichtigung der Betroffenen soll die vorstehend genannten Informationen enthalten. Sofern eine individuelle Benachrichtigung aller Betroffenen unverhältnismäßig aufwendig ist, kann sie durch eine öffentliche Bekanntmachung ersetzt werden.

Insbesondere die Dokumentationspflichten und die Meldung an Aufsichtsbehörden von allen Datenschutzverletzungen bzw. solchen, die „voraussichtlich nicht zu einem Risiko für die Betroffenen führen“, können zu erheblichen Aufwänden führen und in der Praxis kaum praktikabel sein. Entscheidend wird sein, welche Maßstäbe Aufsichtsbehörden in der Zukunft tatsächlich an die Beurteilung eines „Risikos für die Betroffenen“ stellen und ob es *de minimis* Verstöße gibt, die nicht zu dokumentieren sind. Unternehmen müssen aber in diesem Bereich in jedem Fall in Zukunft sehr viel mehr als in der Vergangenheit tun, auch vor dem Hintergrund der hohen Strafen, die bei Verstößen drohen (siehe dazu Frage 33). Dazu gehört es, unternehmensinterne Verhaltensprozesse für den Fall einer wesentlichen Datenschutzverletzung einzuführen, insbesondere eines Datendiebstahls oder Hackings.

33 Welche Strafen/Bußgelder und andere behördlichen Konsequenzen sind bei Verstößen gegen die Datenschutzgrundverordnung zu erwarten?

Der Maßnahmenkatalog bei Datenschutzverstößen bleibt im Wesentlichen unverändert. Das heißt, die Konsequenzen bei Datenschutzverstößen sind ihrer Art nach dieselben wie bisher. Dazu gehören behördenseitig – zusätzlich oder anstelle von Bußgeldern und Strafen (hierzu weiter unten) – insbesondere Unterlassungsansprüche, Untersuchungsbefugnisse sowie weitere Anordnungen von Datenschutzbehörden (Erteilung von Auskünften, Untersagung bestimmter Vorgänge, Vorgaben zu bestimmtem Vorgehen, etc.). Ziel der Verordnung ist es, dass die Datenschutzbehörden in Zukunft insbesondere von ihren Untersuchungsbefugnissen zunehmend Gebrauch machen. Ob die Datenschutzbehörden bei Verstößen direkt zu Bußgeldern greifen, bleibt abzuwarten. Wahrscheinlicher ist es wohl (jedenfalls in Deutschland), dass die Datenschutzbehörden (außer bei gravierenden Fällen) zunächst von diesen Möglichkeiten Gebrauch machen, insbesondere um den (vermeintlichen) Verstoß aufzuklären, bevor sie ein Bußgeld verhängen.

a **Wer kann von möglichen Bußgeldern betroffen sein?**

Die verantwortliche Stelle und der Auftragsdatenverarbeiter (neu!), soweit die Verordnung für ihn gilt und er für Einhaltung der Verordnung verantwortlich ist (siehe hierzu oben Frage 3).

b **Höhe: Muss ich direkt mit einem Bußgeld in Höhe von 4 Prozent des Jahresumsatzes rechnen? Wovon hängt die Höhe der Strafe ab?**
Wie auch nach dem Bundesdatenschutzgesetz gibt es zwei qualitative Klassen von Verstößen. Die mildere Vorschrift erlaubt die Verhängung von Bußgeldern bis zu 10 Mio. EUR oder 2 Prozent des gesamten, weltweiten Umsatzes, je nachdem, was höher ist. Die in dieser Vorschrift aufgeführten Verstöße betreffen überwiegend Vorschriften, welche nicht die Zulässigkeit der Datenverarbeitung regeln, z.B. die Gebote Datenschutz durch Technik und Datenschutz durch Voreinstellungen sowie die Pflicht zur Implementierung angemessener technischer und organisatorischer Maßnahmen. Die zweite, strengere Vorschrift sanktioniert hingegen überwiegend Verstöße gegen Vorschriften, welche die Zulässigkeit der Datenverarbeitung regeln, insbesondere die Erlaubnistatbestände sowie Datentransfers und berechtigt zur Verhängung von Bußgeldern bis zu 20 Mio. EUR oder 4 Prozent des gesamten, weltweiten Umsatzes, je nachdem, was höher ist.

Die Höhe des Bußgelds ist im Einzelfall zu bestimmen; sie soll „wirksam, verhältnismäßig und abschreckend“ sein. Anhaltspunkte zur Bestimmung der Höhe des Bußgelds sind insbesondere:

- Art, Schwere und Dauer des Verstoßes unter Berücksichtigung der Art, des Umfangs oder des Zwecks der betreffenden Verarbeitung sowie der Anzahl der von der Bearbeitung betroffenen Personen und des Ausmaßes des von ihnen erlittenen Schadens;
- Vorsätzlichkeit oder Fahrlässigkeit des Verstoßes;
- die zur Minderung des Schadens getroffenen Maßnahmen;
- etwaige einschlägige, frühere Verstöße;
- das Maß der Zusammenarbeit mit der Aufsichtsbehörde;
- auf welche Weise die Aufsichtsbehörde Kenntnis vom Verstoß erlangt hat, z.B. ob sich freiwillig gemeldet wurde.

Insgesamt muss abgewartet werden, wie die Aufsichtsbehörden (und ggf. die Gerichte) mit den Bußgeldtatbeständen in Zukunft umgehen. Es ist davon auszugehen, dass es hier (zumindest in den ersten Jahren) erhebliche Unterschiede zwischen verschiedenen Aufsichtsbehörden gibt. Im Ergebnis bedeutet die neue Rechtslage aber eindeutig eine „Aufforderung“ an die Aufsichtsbehörden strenger vorzugehen. Erklärtes Ziel ist es, durch (dem Kartellrecht ähnliche) harte Strafen Unternehmen anzuhalten, den Datenschutz ernster zu nehmen und Verstöße zu vermeiden.

34 Was können weitere Konsequenzen von Verstößen sein?

Zusätzlich zu den behördlichen Maßnahmen, insbesondere den Bußgeldern, kann auch weiterhin jede Person, der durch eine unzulässige Verarbeitung ihrer personenbezogenen Daten ein materieller oder immaterieller Schaden entsteht, Schadensersatz verlangen. Da ein Schaden jedoch selten entsteht oder schwer nachzuweisen ist, ist das Risiko in der Praxis relativ gering. Hieran wird sich nach der neuen Regelung vermutlich nichts ändern.

Weiter drohen Unterlassungsansprüche der betroffenen Datensubjekte und von Verbraucherschutzorganisationen.

Darüber hinaus können Datenschutzverstöße schlechte Publicity auslösen und den Ruf des eigenen Unternehmens schädigen (z.B. die Datenskandale bei Telekom, Lidl und der Deutschen Bahn).

35 Ab wann gilt die Datenschutzgrundverordnung und was muss ich bis dahin tun?

Die Datenschutzgrundverordnung ist am 25. Mai 2016 in Kraft getreten. Genau zwei Jahre später, also ab dem 25. Mai 2018, wird sie dann „wirksam“. Diese Trennung von in Kraft treten und Wirksamkeit erscheint auf den ersten Blick merkwürdig. Sie ist aber gewollt. Denn viele der Verpflichtungen, die ab dem 25. Mai 2018 wirksam werden, also spätestens ab dann umzusetzen sind, bedürfen einer erheblichen Vorlaufzeit.

Unternehmen müssen sich also bereits jetzt ihre Prozesse und Abläufe anschauen und sie so umstellen, dass sie mit der zukünftigen Rechtsordnung in Einklang stehen. Ab Mai 2018 gilt die Datenschutzgrundverordnung unmittelbar in allen EU-Mitgliedsstaaten, es bedarf keines weiteren Umsetzungsaktes und angesichts der großen Vorlaufzeit werden sich Unternehmen nicht damit herausreden können, dass Sie nicht genügend Zeit zur Umsetzung hatten. Vielmehr sind sie zur Umsetzung der Datenschutzgrundverordnung ab dem 25. Mai 2016 verpflichtet, spätestens in zwei Jahren müssen die Unternehmen dann vollständig „compliant“ sein.

Des Weiteren hat die Datenschutzgrundverordnung eine weitere (gewisse) „Vorwirkung“: Es ist zu erwarten, dass die Datenschutzbehörden ihre Aufsichtstätigkeit auch schon jetzt so ausrichten werden, dass ein geordneter Übergang zum neuen EU-Datenschutzrecht möglich ist. Speziell in Fällen, in denen ein bestimmtes Verhalten nach der Datenschutzgrundverordnung explizit zulässig sein wird, ist es unwahrscheinlich (und unter Umständen auch rechtswidrig), dass eine Datenschutzbehörde für die Übergangszeit noch zwangsweise das alte Recht durchsetzt.

36 Was sollte juristisch in der zweijährigen Übergangsfrist geprüft werden?

Alle betroffenen Unternehmen müssen in der Übergangszeit prüfen, ob ihre Prozesse, Geschäftsmodelle und insbesondere die auf Datenschutz bezogenen Compliance-Pflichten (z.B. „technische und organisatorische Maßnahmen“) mit der Datenschutzgrundverordnung vereinbar sind.

Die Datenschutzgrundverordnung ist dem deutschen Datenschutzrecht in vielen Punkten zwar sehr ähnlich, aber es bestehen in etlichen Punkten auch wesentliche Unterschiede, die zu erheblichen Änderungen in der Praxis und – diesen vorausgeschickt – dem Bedarf einer sorgfältigen juristischen Prüfung führen. Zum Teil führt die Datenschutzgrundverordnung auch gänzlich neue Konzepte ein, z.B. die in einigen Fällen verpflichtend durchzuführende „Datenschutz-Folgenabschätzung“ oder das Recht auf Datenportabilität. Zur Erfüllung dieser neuen Pflichten muss ein datenverarbeitendes Unternehmen die für sich relevanten ermitteln. Hierfür ist es zunächst erforderlich, eine juristische und tatsächliche „Gap-Analyse“ vorzunehmen. Deren Ergebnisse sind dann zu implementieren.

37 Was muss technologisch und organisatorisch in der zweijährigen Übergangfrist umgesetzt werden?

Im Grundsatz ist ein „Compliance-Check“ für alle Prozesse notwendig, in denen personenbezogene Daten vorkommen. Die Datenschutzgrundverordnung erklärt nur in wenigen Fällen bereits bestehende Beschlüsse oder rechtliche Beurteilungen für weiterhin geltend; dies gilt z.B. für bereits bestehende Genehmigungen von Standardvertragsklauseln für den Datentransfer in Drittländer (Art. 46 Abs. 5). Im Übrigen sind alle datenschutzrelevanten Prozesse zu prüfen und ggf. anzupassen.

Was in einzelnen Fällen dann zu tun ist, hängt von den jeweiligen Unternehmen, insbesondere deren Tätigkeiten, Prozessen und bisherigen Compliance-Standards ab und ist in der juristischen Gap-Analyse (siehe Frage 36.) zu ermitteln. Es gibt jedoch eine Reihe von allgemeinen Themen, die viele Unternehmen betreffen dürften. Dazu gehören:

- Aufgrund des nun eingeführten Marktortprinzips müssen Unternehmen zukünftig das Datenschutzrecht jeden europäischen Staates umsetzen, in dem sie ihre Leistungen anbieten. Aufgrund der vielen einzelstaatlichen Rechtsakte, die von der Datenschutzgrundverordnung zugelassen sind, wird dies eine erhebliche Herausforderung.
- Unternehmen mit Sitz im EU-Ausland, die Daten innerhalb der EU erheben oder in der EU ihre Produkte vermarkten, unterfallen ab Geltungsbeginn 2018 definitiv der EU-Datenschutzgrundverordnung. Sie müssen also die datenschutzrechtlichen Vorgaben spätestens ab diesem Zeitpunkt vollständig umsetzen – die einzige Alternative wäre, sich aus dem EU-Markt vollständig zurückzuziehen.
- Aufgrund der noch engeren Voraussetzungen für eine wirksame Einwilligung geraten viele Einwilligungs-basierte Datenverarbeitungsvorgänge und Geschäftsmodelle in eine Grauzone. Hier müssen Unternehmen prüfen, ob sie Einwilligungsformulare anzupassen haben oder auf andere Erlaubnisvorschriften ausweichen

müssen (die dann auch andere rechtliche Vorgaben bedeuten). Einwilligungen aus der Zeit von vor Inkrafttreten der DSGVO behalten ihre Wirksamkeit auch später – allerdings nur, wenn sie bereits den Kriterien der DSGVO entsprochen haben. Es spricht deshalb viel dafür, die Abläufe bei der Einholung von Einwilligungen bereits jetzt an den strengeren Standard der DSGVO anzupassen.

- Sanktionen für Verstöße gegen die EU-Datenschutzgrundverordnung können im Extremfall bis zu 4 Prozent des weltweiten (Konzern-) Jahresumsatzes betragen. Die internen Compliance-Strukturen und das Risikomanagement in Unternehmen müssen an dieses erhöhte Risiko angepasst werden.
- Unternehmen, die Daten im Auftrag verarbeiten (z.B. Cloud-Hosting-Anbieter oder Softwareanbieter, die IT-Support gewährleisten), hatten bisher deutlich weniger Pflichten und müssen ihre datenschutzrechtliche Compliance anpassen. Beispielsweise müssen auch Auftragsdatenverarbeiter zukünftig ein eigenes Verfahrensverzeichnis führen (Art. 30 Abs. 2). Auftragsdatenverarbeiter mit Sitz außerhalb der EU müssen außerdem einen Vertreter in der EU benennen, der für die Datenschutz-Compliance zuständig ist (Art. 27).

Die genauen Anforderungen werden sich in einer Reihe von Fällen in den nächsten Monaten und Jahren weiter konkretisieren. Denn in vielen Bereichen haben die Mitgliedsstaaten oder die EU-Kommission die Möglichkeit, noch konkretisierende Rechtsakte zu erlassen. Dies betrifft auch zentrale Bereiche, beispielsweise den Ausgleich der Datenschutzgrundverordnung mit dem Recht auf Meinungs- und Informationsfreiheit (Art. 85). In anderen Bereichen werden einzelne Datenschutzbehörden oder der neu einzurichtende gemeinsame Datenschutzausschuss noch konkretisierende Richtlinien und Empfehlungen herausgeben. Diese sind für private Unternehmen zwar rechtlich nicht bindend, stellen aber eine Selbstbindung der Behörden dar und sollten bei der Anpassung von datenschutzrelevanten Prozessen zumindest beachtet werden. Jedoch kann dies nicht als Grund herangeführt werden, um mit der Umsetzung der Anforderung der Datenschutzgrundverordnung abzuwarten. Vielmehr ist die Datenschutzgrundverordnung ganz bewusst so konzipiert, dass sie bereits jetzt in Kraft ist und umzusetzen ist (siehe Frage 35 oben). Die Unternehmen müssen also die nächsten zwei Jahre bis zur Wirksamkeit der Datenschutzgrundverordnung am 25. Mai 2018 (siehe Frage 35) aktiv nutzen. Ansonsten drohen Sanktionen.

twobirds.com

Aarhus & Abu Dhabi & Beijing & Bratislava & Brussels & Budapest & Copenhagen & Dubai & Dusseldorf & Frankfurt & The Hague & Hamburg & Helsinki & Hong Kong & London & Luxembourg & Lyon & Madrid & Milan & Munich & Paris & Prague & Rome & Shanghai & Singapore & Stockholm & Sydney & Warsaw