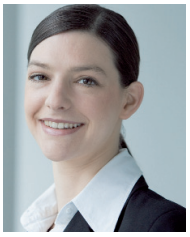
MAYER·BROWN

Perspektiven
Sommer | 2010

Datenschutz

Aktuelle Entwicklungen und Entscheidungen

Tim Wybitul
Partner, Frankfurt
T: +49 69 79 41 2271
twybitul@mayerbrown.com



Dr. Andrea Patzak
Associate, Frankfurt
T: +49 69 79 41 1471
apatzak@mayerbrown.com

Einleitung

Datenschutz ist für Unternehmen zu einem wesentlichen Wirtschaftsfaktor geworden. Die Bedeutung von Datenschutz in der Wirtschaft hat in der letzten Zeit erheblich zugenommen. Die vorliegende Publikation ist die erste in einer Reihe von Beiträgen, die Entscheidungsträger bei der Beantwortung von Fragen und Lösung von Problemen aus dem Bereich Datenschutz unterstützen soll.

Technische Entwicklungen wie das Internet haben die Wirtschaft in den letzten Jahrzehnten umfassend verändert. Die Weiterentwicklung der Informationstechnologie ermöglicht das Sammeln von Informationen und die Auswertung von Daten in völlig neuem Umfang. Enorme Rechen- und Speicherkapazitäten sind für überschaubare Kosten erhältlich. Bei vielen Datenverarbeitungen gibt inzwischen nicht mehr die Technik die Grenzen vor, sondern der Datenschutz. Die rechtlichen Rahmenbedingungen für den Umgang mit den Daten anderer Personen verändern sich ähnlich schnell wie die technischen Möglichkeiten. Noch vor etwa einem Jahrzehnt hatte das Datenschutzrecht für viele Unternehmen eine eher begrenzte Bedeutung. Das hat sich – auch durch die sogenannten Datenschutzaffären seit 2008 – gründlich geändert. Der Kreis der Personen, die Entscheidungen zum Datenschutz im Unternehmen treffen müssen, hat sich erheblich erweitert, die Komplexität der zu treffenden Entscheidungen hat sich vergrößert.

Gesetzesvorhaben: Neues Beschäftigtendatenschutzgesetz in Vorbereitung

Bereits seit Jahren wird die Einführung eines eigenen Beschäftigtendatenschutzgesetzes gefordert. Als Reaktion auf Datenschutzskandale bei einer Reihe von Großunternehmen beschloss der Gesetzgeber 2009 am Ende der Legislaturperiode eine weitere Reform des BDSG. Bereits am 31. März 2010 hatte das Bundesinnenministerium ein Eckpunktepapier vorgelegt, in dem es zeitnah weitere Änderungen des Gesetzes im Bereich des Beschäftigtendatenschutzes ankündigte. Kurz darauf kursierte auch schon ein Referentenentwurf zu einem neuen Beschäftigtendatenschutzgesetz, dessen einzelne Regelungen teilweise kontrovers diskutiert wurden. Am 28. Mai 2010 veröffentlichte das Bundesministerium des Inneren einen weiteren Referentenentwurf, zu dem Gewerkschaften, Verbände und andere Interessenvertretungen eine Vielzahl von Stellungnahmen abgaben. Am 19. Juli 2010 stellte dann die Bundestagsfraktion der Grünen einen eigenen Rohentwurf für ein Beschäftigtendatenschutzgesetz im Internet vor. In einem hierfür eingerichteten Blog (http://beschaeftigtendatenschutz.de/) stellen sie ihren Gesetzentwurf öffentlich zur Diskussion.

Zwischen den am Referentenentwurf der Bundesregierung beteiligten Ministerien scheint Einigkeit darüber zu bestehen, dass der neue Beschäftigtendatenschutz in einem eigenen Abschnitt des BDSG geregelt werden soll und dass viele Einzelfallregelungen in das Gesetz aufgenommen werden sollen. Viele Fälle sollen detailliert geregelt werden, wie etwa Vorschriften zu Compliance-Kontrollen, Videoüberwachung von Beschäftigten und Überwachung der Nutzung von IT-Systemen. Einwilligungen von Beschäftigten sollen nur noch in dem Umfang zulässig sein, in dem dies in dem Gesetzesentwurf ausdrücklich vorgesehen ist. Anders als in den sonstigen Regelungen des BDSG soll die Erhebung von Beschäftigtendaten nach anderen Regeln ablaufen als deren spätere Verarbeitung oder Nutzung.

Zusammenfassend muss man feststellen, dass der Entwurf in seiner jetzigen Fassung komplex und schwer verständlich aufgebaut ist. Dem Wunsch vieler Rechtsanwender nach Vereinfachung des Datenschutzgesetzes und besserer Verständlichkeit wird er nicht gerecht. Es bleibt zu hoffen, dass die beteiligten Ministerien und Fraktionen sich die Zeit nehmen, eine gut durchdachte und verständliche Regelung auf den Weg zu bringen. Dabei sollte das neue Gesetz sowohl die Persönlichkeitsrechte der Beschäftigten hinreichend schützen als auch Unternehmen klare und praxisgerechte Vorgaben für einen vernünftigen und angemessenen Umgang mit den Daten ihrer Beschäftigten bieten. Es geht nicht um die Absenkung des bestehenden Datenschutzniveaus, sondern um die Schaffung der für alle Beteiligten dringend erforderlichen Transparenz der geltenden Datenschutzregeln.

Cloud Computing kann deutsches Datenschutzrecht verletzen

Der Begriff „Cloud Computing“ beschreibt das Bereitstellen von Services durch Drittanbieter, welche Unternehmen Zugang zu Softwareapplikationen, Datenbanken, Infrastruktur und ähnlichen Services über das Internet oder andere Netzwerke vermitteln. In der letzten Zeit ist ein erkennbarer Anstieg der Nutzung von Cloud Computing-Umgebungen zu verzeichnen. Dies begründet sich zum einen durch die erheblichen Kosteneinsparungen, die dadurch erzielt werden können, und zum anderen durch die mannigfaltigen sonstigen Vorteile von Cloud Computing. Aufgrund der erhöhten Gefährdung für personenbezogene Daten gehen die deutschen Datenschutz-Aufsichtsbehörden dazu über, stärkere Beschränkungen und höhere Anforderungen an Cloud Computing, aber auch an andere Outsourcing-Projekte, bei denen personenbezogene Daten betroffen sind, zu stellen. Unternehmen müssen nun sicherstellen, dass sie diese strengeren Voraussetzungen erfüllen. Unternehmen, denen es nicht gelingt, Cloud Computing-Umgebungen an diesen neuen Anforderungen auszurichten, drohen erhebliche Strafen, zivilrechtliche Streitigkeiten und Reputationsschäden.

DIE THESEN DER DATENSCHUTZ-AUFSICHTSBEHÖRDE IN SCHLESWIG-HOLSTEIN

Die Datenschutz-Aufsichtsbehörde für die private Wirtschaft in Schleswig-Holstein (unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, ULD) hat kürzlich ein Thesenpapier auf ihrer Webseite veröffentlicht, das die datenschutzrechtlichen Aspekte des Cloud Computing behandelt. Die in dem Papier geäußerten Ansichten des ULD sind für Unternehmen nicht rechtlich bindend. Dennoch zeigt das Thesenpapier deutlich, wie das ULD Cloud Computing-Umgebungen künftig beurteilen wird. Es ist anzunehmen, dass der Sicht des ULD auch andere Datenschutz-Aufsichtsbehörden in anderen Bundesländern folgen werden. In dem Thesenpapier äußert das ULD seine Bedenken, dass zahlreiche Datenübermittlungen in Cloud Computing-Umgebungen nicht im Einklang mit deutschem Datenschutzrecht stehen. Insbesondere Public Clouds werden vom ULD als oftmals nicht datenschutzkonform angesehen. Die datenschutzrechtlichen Bedenken sind jedoch keineswegs auf Public Clouds beschränkt.

Das deutsche Bundesdatenschutzgesetz (BDSG) setzt die Vorgaben der EU-Datenschutzrichtlinie um. § 11 BDSG normiert die Voraussetzungen an die Auftragsdatenverarbeitung. Diese Norm ist grundsätzlich nur anwendbar auf solche Auftragsdatenverarbeitungsverhältnisse, in denen der Auftragnehmer seinen Sitz innerhalb der EU hat. Das ULD hat nunmehr den Geltungsbereich ausgeweitet und wendet die strengen Voraussetzungen von § 11 BDSG auch auf solche Datenübermittlungen an, deren Empfänger Auftragnehmer außerhalb der EU sind. Das ULD stellt fest, dass es für eine zulässige Datenübermittlung in einer Cloud Computing-Umgebung nicht ausreicht, sich auf die EU-Standardvertragsklauseln zu verlassen. Diese waren bisher jedoch das in der Praxis am häufigsten verwendete Instrument für zulässige Datenübermittlungen in Länder außerhalb der EU. Vielmehr verlangt das ULD zusätzlich zu den EU-Standardvertragsklauseln, dass Auftraggeber nunmehr die strengen Anforderungen aus § 11 BDSG auch in Konstellationen der Auftragsdatenverarbeitung durch einen Auftragnehmer in einem Drittland berücksichtigen müssen.

Unabhängig davon, ob Cloud Computing-Anbieter innerhalb oder außerhalb Europas sitzen, fordert das ULD, dass Unternehmen, die Cloud Computing-Services verwenden, grundsätzlich angemessene Maßnahmen ergreifen, um die Integrität und Sicherheit der verarbeiteten personenbezogenen Daten zu gewährleisten. Zum Beispiel müssen sie entsprechende vertragliche Klauseln mit dem Cloud Computing Service-Anbieter vereinbaren, die die Voraussetzungen an die Auftragsdatenverarbeitung nach § 11 BDSG erfüllen – unabhängig davon, ob der Anbieter seinen Sitz in der EU oder außerhalb der EU hat. Unternehmen oder externe Sachverständige müssen regelmäßige Audits durchführen, ob Cloud Computing Service-Anbieter die Anforderungen des BDSG einhalten. Diese regelmäßigen Audits beinhalten auch die Kontrolle der technischen und organisatorischen Maßnahmen, die der Auftragnehmer zum Schutz der Daten implementieren muss.

Weder im BDSG noch in Stellungnahmen der Datenschutz-Aufsichtsbehörden findet man Hilfestellungen zu der Frage, was unter dem Begriff „regelmäßige Kontrollen“ zu verstehen ist und in welchem Ausmaß diese verlangt werden. Das ULD sieht zwei Möglichkeiten vor, wie Unternehmen ihrer Kontrollpflicht nachkommen können: erstens die verbindliche Zusage des Auftragnehmers in Form einer umfassenden Selbstbindung einholen oder zweitens die Kontrolle, ob diese Pflichten beachtet werden, an eine unabhängige und kompetente Stelle zu übertragen. Die externe Kontrolle kann durch das Einholen von Audits oder Zertifizierungen erfolgen.

DATENÜBERMITTLUNGEN INS EU-AUSLAND

Neben dem vom ULD ausdrücklich verlangten Erfordernis, dass für Cloud Computing-Umgebungen unter Einbeziehung außereuropäischer Länder grundsätzlich § 11 BDSG erfüllt sein muss, verlangt das ULD eines der zugelassenen Instrumente, die den Datentransfer in Länder außerhalb Europas rechtfertigen. Eine der in der Praxis am häufigsten genutzten Methoden ist die Verwendung der Standardvertragsklauseln, insbesondere die für die Auftragsdatenverarbeitung, welche von der EU erlassen wurden. Auch das eigens für eine zulässige Datenübermittlung in die USA geschaffene Safe Harbor-Abkommen stellte bis dato eine ausreichende Rechtfertigungsgrundlage für einen Datentransfer in die USA dar. Jedoch hat der Düsseldorfer Kreis, das Gremium der Vertreter der staatlichen Datenschutz-Aufsichtsbehörden für die private Wirtschaft, erst kürzlich erklärt, die Safe Harbor-Zertifikationen von US-Unternehmen nicht mehr als ausreichend ansehen zu wollen, um auf dieser Basis Daten in die USA zu übermitteln. Vielmehr müssten Datenübermittler strenge Regeln beachten (vgl. zu den verschärften Anforderungen an das Übermitteln von Daten an Safe Harbor zertifizierte Empfänger: http://www.mayerbrown.com/publications/article.asp?id=9156&nid=6).

In seinem Papier benennt das ULD einige Beispiele, wie Cloud Computing-Umgebungen mit dem BDSG und den Anforderungen an Übermittlungen in das EU-Ausland in Einklang zu bringen sind. Dabei ist zu beachten, dass das ULD erfordert, dass in sämtlichen Situationen die Anforderungen nach § 11 BDSG erfüllt sein müssen. Manche der Vorschläge sind jedoch kritisch zu bewerten, da sie nur entfernt auf die tatsächlichen Gepflogenheiten und die Art und Weise von Cloud Computing-Angeboten eingehen.

1. Möglichkeit der räumlichen Beschränkung

Der Cloud Computing-Anbieter kann den Nutzern die Möglichkeit einräumen, eine räumlich begrenzte Cloud zu nutzen und die Datenverarbeitung nur in Ländern innerhalb des europäischen Wirtschaftsraumes (EWR) bzw. der EU durchzuführen.

2. Angemessenheit des Datenschutzniveaus durch die EU-Kommission

Cloud Computing kann so angeboten werden, dass es nur in solche Länder hineinreicht, in denen die EU-Kommission ein angemessenes Datenschutzniveau nach § 4b Abs. 2 S. 3 BDSG festgestellt hat.

3. EU-Standardvertragsklauseln und zusätzliche Maßnahmen

Ein Unternehmen, das Cloud Computing Services nutzt, kann datenschutzrechtskonform handeln, indem es die EU-Standardvertragsklauseln anwendet und zusätzlich die Anforderungen von § 11 BDSG erfüllt. Wie zuvor erwähnt, wurden in Übereinstimmung mit der Praxis der Aufsichtsbehörden die EU-Standardvertragsklauseln für die Auftragsdatenverarbeitung bisher als ausreichend erachtet, um Daten zulässig in Länder außerhalb der EU zu übermitteln. Diese Sicht des ULD ist jedoch durchaus kritisch zu würdigen. Die Systematik des BDSG zeigt, dass die Anforderungen an eine Auftragsdatenverarbeitung nach § 11 BDSG auf Datenverarbeiter innerhalb der EU anzuwenden sind und nicht auf die Weitergabe von Daten an Datenverarbeiter außerhalb der EU. Die enge vertragliche Anbindung des Auftragnehmers an den Auftraggeber, wie in § 11 BDSG verlangt, ist der Grund für die Privilegierung nach § 11 BDSG. In der Praxis wird diese Privilegierung oftmals genutzt, denn eine Weitergabe von Daten innerhalb einer Auftragsdatenverarbeitung bedeutet keine Übermittlung, die ihrerseits durch

gesetzliche Erlaubnistatbestände des BDSG gerechtfertigt sein muss. Diese strengen Anforderungen, welche die Privilegierung im deutschen und europäischen Raum begründen, möchte das ULD nun auch auf Sachverhalte außerhalb Europas anwenden. Sitzt ein Auftragnehmer jedoch im EU Ausland, so sieht das BDSG diesen gemäß § 3 Abs. 8 Satz 3 BDSG als Dritten an, der nicht von der Privilegierung erfasst wäre. Das ULD wendet mithin diese strengen Voraussetzungen über den eigentlichen Anwendungsbereich von § 11 BDSG hinaus an. Es ist jedoch zu erwarten, dass die anderen Datenschutz-Aufsichtsbehörden in Deutschland dieser Ansicht folgen und sie genauso durchsetzen werden.

4. Anwendbarkeit von BCRs

Obwohl Binding Corporate Rules (BCR) ursprünglich für die Datenverarbeitung in internationalen Konzernen entworfen wurden, hat das ULD nun vorgeschlagen, BCRs als Instrument zu verwenden, um auch nicht im Konzern miteinander verbundene Auftragnehmer den BCRs zu unterwerfen. Andere Aufsichtsbehörden haben diese Ansicht jedoch noch nicht aufgegriffen bzw. bestätigt, so dass abzuwarten bleibt, ob sich die Anwendung der BCRs auf Unternehmen durchsetzt, die in keinem gemeinsamen Unternehmensverbund stehen.

KONSEQUENZEN FÜR IN DEUTSCHLAND TÄTIGE UNTERNEHMEN

Unternehmen sind gut beraten, ihre bestehenden Cloud Computing-Umgebungen oder andere Outsourcing-Strukturen, die personenbezogene Daten aus Deutschland beinhalten, auf die erforderliche Vereinbarkeit mit dem Datenschutzgesetz zu überprüfen. Unternehmen, die planen, Cloud Computing-Umgebungen für sich zu nutzen, sollten sich vergewissern, dass Cloud Computing-Umgebungen, Verträge und Kontrollmaßnahmen so ausgestaltet sind, dass sie den neuen Anforderungen, die durch das ULD aufgestellt wurden, entsprechen. Angesichts des enormen Anstiegs der Cloud Computing-Nutzung ist zu erwarten, dass auch andere EU-Datenschutz-Aufsichtsbehörden Stellungnahmen und Arbeitshilfen zu Datenschutz und Cloud Computing abgeben werden.

BISHERIGE UND ZUKÜNFTIGE ENTWICKLUNG DES DATENSCHUTZES IN DEUTSCHLAND

Das Themenpapier des ULD zeigt erneut, wie wichtig die Beachtung des Datenschutzrechts allgemein und die Verfolgung neuer Entwicklungen im Besonderen sind. Die Stellungnahme des ULD ist nur eine der vielen neueren Entwicklungen im Datenschutzrecht. Diese erfolgten als Reaktion auf zahlreiche Datenschutzverletzungen größerer Unternehmen. Erst kürzlich hat z. B. der Düsseldorfer Kreis strengere Anforderungen für solche Unternehmen aufgestellt, die personenbezogene Daten zu Safe Harbor zertifizierten Empfängern in die USA übermitteln (siehe Seite 12). Auch sind derzeit die Vorschriften über den Arbeitnehmerdatenschutz Gegenstand eines Gesetzgebungsverfahrens.

Grundsätzlich hat sich die Bedeutung des Datenschutzes als einer der Hauptbestandteile von Unternehmens-Compliance in den letzten Jahren erheblich vergrößert – und es kann nur vermutet werden, dass sich diese Entwicklung weiter verstärkt. Unternehmen in Deutschland sind deshalb gefordert, verstärkt ihre Datenschutzstruktur anhand der Neuerungen zu überprüfen und ihre Datenschutz-Compliance-Programme daraufhin auszurichten.

Neue EU-Standardvertragsklauseln für die Auftragsdatenverarbeitung

Die Europäische Kommission hat vor Kurzem neue Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter in Länder außerhalb der Europäischen Union (EU) und des Europäischen Wirtschaftsraums (EWR), sogenannte Drittländer, verabschiedet. Seit dem 15. Mai 2010 dürfen die bislang seitens der EU-Kommission vorgegebenen Standardvertragsklauseln nicht mehr angewendet werden. Die EU-Standardvertragsklauseln sind in der Praxis das wohl am häufigsten gebrauchte Instrument, um Übermittlungen personenbezogener Daten in Drittländer zu legitimieren. Dieser Überblick zeigt, welche Anforderungen an die grenzüberschreitenden Datenübermittlungen gestellt werden und wie Unternehmen diesen Anforderungen in der Praxis nachkommen können.

BEDEUTUNG DER AUFTRAGSDATENVERARBEITUNG FÜR EUROPÄISCHE UNTERNEHMEN

Für deutsche Unternehmen ist es oftmals eine wirtschaftliche Notwendigkeit, personenbezogene Daten an Empfänger in Drittländer zu übermitteln. Outsourcing-Projekte, zentralisierte Datenbanken und Joint Ventures sind nur einige Beispiele hierfür. Häufig schließen europäische Unternehmen aus Kostengründen IT-Outsourcing-Verträge mit Anbietern in Drittländern ab. Bei solchen IT-Dienstleistungen erhält der beauftragte Dienstleister zumeist auch Zugriff auf personenbezogene Daten (beispielsweise auf Daten der Mitarbeiter des Auftraggebers). Aus rechtlicher Sicht stellt ein solcher Sachverhalt eine Übermittlung personenbezogener Daten in ein Drittland dar. Derartige grenzüberschreitende Übermittlungen erlauben §§ 4b und 4c des Bundesdatenschutzgesetzes (BDSG) nur unter engen Voraussetzungen.

BEGRIFF DES ÜBERMITTELNS

Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten. Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Im Wirtschaftsleben sind dies etwa Mitarbeiter eines anderen Unternehmens oder sonstige unternehmensfremde Personen. Auch die Weitergabe personenbezogener Daten an eine andere Gesellschaft innerhalb desselben Konzerns ist eine Übermittlung. Das deutsche Datenschutzrecht stellt an den Datentransfer zwischen Konzernunternehmen die gleichen Voraussetzungen wie an jede andere Übermittlung, denn es kennt kein Konzernprivileg.

Eine Übermittlung kann beispielsweise in dem Weitergeben von personenbezogenen Daten an einen Dritten liegen. Eine weitere Form der Übermittlung ist das Bereithalten von Daten zur Einsicht oder zum Abruf durch einen Dritten. Sobald der Dritte die Daten einsieht oder abruft, sind die Daten an den Dritten übermittelt.

HOHE ANFORDERUNGEN AN DIE ZULÄSSIGKEIT DER ÜBERMITTLUNG

Deutsche Datenschutzaufsichtsbehörden prüfen die Zulässigkeit einer Datenübermittlung in Drittstaaten im Rahmen einer zweistufigen Prüfung.

Zulässigkeitsprüfung auf der ersten Stufe

Zunächst stellen die Behörden fest, ob die geplante Übermittlung personenbezogener Daten an einen Dritten nach allgemeinen Maßstäben des BDSG zulässig wäre. Grundsätzlich verbietet das BDSG jeden Umgang mit personenbezogenen Daten – es sei denn, eine Rechtsvorschrift oder eine wirksame Einwilligung des Betroffenen erlaubt diesen Datenumgang. Ein typisches Beispiel für eine nach den allgemeinen Regeln des BDSG zulässige Übermittlung von personenbezogenen Daten liegt vor, wenn die Übermittlung zur Wahrung berechtigter Interessen des Unternehmens nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG erforderlich ist. Zudem darf kein Grund zu der Annahme bestehen, dass schutzwürdige Interessen der von der Übermittlung ihrer Daten betroffenen Personen an dem Ausschluss der Übermittlung bestehen, die das Unternehmensinteresse überwiegen.

Für die Übermittlung muss ein berechtigtes wirtschaftliches Interesse des Unternehmens vorliegen. Die Senkung von Kosten beispielsweise kann durchaus ein solcher gebotener Geschäftszweck sein.

Außerdem darf eine Übermittlung nach § 28 Abs. 1 Satz 1 Nr. 2 BDSG nur dann vorgenommen werden, wenn sie *„erforderlich“* zur Interessenwahrnehmung ist. Das bedeutet, dass das übermittelnde Unternehmen nur die Daten übermitteln darf, die zur Verwirklichung des konkreten Geschäftszwecks wirklich nötig sind.

Der wichtigste Teil dieser rechtlichen Prüfung besteht darin, festzustellen, ob die Interessen der von der Übermittlung ihrer Daten betroffenen Personen angemessen gewahrt bleiben. Hierbei geht es um eine Abwägung zwischen den betroffenen Interessen des Unternehmens und denen der Personen, deren Daten übermittelt werden sollen.

FOLGEN FÜR DIE PRAXIS

In der Praxis empfiehlt es sich beispielsweise, Präzedenzfälle für zulässige Übermittlungen zu suchen (etwa aus der Rechtsprechung oder den Tätigkeitsberichten der Landesaufsichtsbehörden) und sich an deren Vorgaben zu orientieren.

Sind all diese Voraussetzungen gegeben, ist die Übermittlung an ein anderes Unternehmen in Deutschland, der EU oder dem EWR zulässig. Die Übermittlung an ein anderes Unternehmen in einem Drittland ist aber nur unter engen Voraussetzungen erlaubt. Diese werden im Folgenden dargestellt.

Zulässigkeitsprüfung auf der zweiten Stufe

Selbst wenn eine Übermittlung personenbezogener Daten nach den allgemeinen Grundsätzen des BDSG innerhalb Europas zulässig wäre, bedeutet dies noch nicht, dass die Übermittlung zugleich auch in ein Drittland ohne angemessenes Schutzniveau erlaubt wäre. Hier stellt § 4c BDSG deutlich höhere Anforderungen als an innerdeutsche oder innereuropäische Übermittlungen. Deshalb muss entweder ein angemessenes Datenschutzniveau durch zusätzliche Maßnahmen geschaffen werden, damit die Übermittlung erlaubt ist oder es muss eine Ausnahmeregelung vorliegen, die eine Datenübermittlung auch ohne vorherige Schaffung eines angemessenen Datenschutzniveaus erlaubt.

Häufig verwenden Unternehmen die von der EU-Kommission erlassenen Standardvertragsklauseln, um diese Anforderungen zu erfüllen. Anders als die in § 4c Abs. 2 Satz 1 BDSG genannten verbindlichen Unternehmensregelungen (Binding Corporate Rules – BCRs), müssen die EU-Standardvertragsklauseln nicht von der zuständigen Aufsichtsbehörde genehmigt werden, um eine zulässige Datenübermittlung in Drittländer zu ermöglichen.

Sinn und Zweck dieser verbindlich anzuwendenden Vertragsklauseln ist es, einen einheitlichen Standard zu schaffen, um Übermittlungen in ein Drittland zu ermöglichen. Daher bieten die Standardvertragsklauseln eine Möglichkeit, grenzüberschreitende Datenübermittlungen in Drittstaaten zeitnah und unbürokratisch durchzuführen. In der Vergangenheit hatten die Datenschutzaufsichtsbehörden unterschiedliche Auffassungen zu der Frage vertreten, ob die Standardvertragsklauseln möglicherweise nicht doch im Einzelfall der Aufsichtsbehörde vorgelegt oder sogar geprüft und genehmigt werden müssten. Zu dieser Frage hat der sogenannte Düsseldorfer Kreis Stellung bezogen. Die Aufsichtsbehörden für die Privatwirtschaft sind in Deutschland auf Landesebene angesiedelt. Die Vertreter dieser Aufsichtsbehörden der Länder für die Privatwirtschaft bilden den Düsseldorfer Kreis. Aus diesem Grunde sind in der Regel die Beschlüsse des Düsseldorfer Kreises für die Aufsichtsbehörden maßgebend. Der Düsseldorfer Kreis hat festgestellt, dass bei vollständiger, unveränderter Verwendung der Standardvertragsklauseln weder eine Genehmigungs- noch eine Vorlagepflicht an die Aufsichtsbehörden besteht.

DIE VERSCHIEDENEN STANDARDVERTRAGSKLAUSELN

Die EU-Kommission hat bislang drei unterschiedliche Standardvertragsklauseln beschlossen. Die ersten beiden Vertragsklauseln vom 15. Juni 2001 und vom 27. Dezember 2004 beziehen sich auf „normale" Übermittlungen an eine andere verantwortliche Stelle in einem Drittland. Die Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsdatenverarbeiter vom 27. Dezember 2001 regeln einen anderen Fall. Hierbei geht es um Datenübermittlungen an Datenverarbeitungsdienstleister, die aufgrund von Weisungen tätig werden. In einem innerdeutschen oder innereuropäischen Zusammenhang regelt § 11 BDSG die Bereitstellung an Auftragsdatenverarbeiter. Eine Auftragsdatenverarbeitung durch Auftragnehmer in Drittstaaten ist hingegen auf der Grundlage von § 11 BDSG nicht vorgesehen.

Die bisherigen Standardvertragsklauseln für die Auftragsdatenverarbeitung in Drittländern sind für ab dem 15. Mai 2010 abgeschlossene Verträge nicht mehr anwendbar. Bereits abgeschlossene Verträge mit den alten Standardvertragsklauseln gelten dagegen grundsätzlich weiter. Sie müssen nicht automatisch an den neuen Beschluss der EU-Kommission angepasst werden. Falls die Vertragsparteien jedoch Änderungen an bestehenden Verträgen über die Auftragsdatenverarbeitung in Drittstaaten vereinbaren wollen, oder falls der Auftragnehmer Unteraufträge vergeben möchte, müssen die Parteien einen neuen Vertrag mit den aktuellen Standardvertragsklauseln abschließen.

NEUE ANFORDERUNGEN AN DIE GRENZÜBERSCHREITENDE AUFTRAGSDATENVERARBEITUNG

Anders als nach den bisherigen Standardvertragsklauseln für die Übermittlung an Auftragsdatenverarbeiter in Drittländern darf der Auftragnehmer auf der Grundlage der neuen Standardvertragsklauseln künftig unter bestimmten Voraussetzungen Unterauftragsverhältnisse eingehen. Das Fehlen einer solchen Regelung war bei der alten Standardvertragsklausel massiv kritisiert worden.

Voraussetzungen für Unterauftragsverhältnisse

Eine solche Unterbeauftragung ist allerdings an einige Zulässigkeitsvoraussetzungen geknüpft:

- Der Auftraggeber muss der Vergabe des Unterauftrages zuvor schriftlich zustimmen.

- Der Unterauftrag muss schriftlich vereinbart werden. Diese Vereinbarung muss dem Unterauftragnehmer dieselben Pflichten auferlegen, die auch dem Auftragnehmer nach dem Hauptauftrag durch die verantwortliche Stelle in Deutschland obliegen.

- Der Auftragnehmer muss gegenüber dem Auftraggeber für Vertragsverstöße des Unterauftragnehmers vollständig verantwortlich bleiben. Auftragnehmer und Unterbeauftragter müssen eine sogenannte Drittbegünstigtenklausel vereinbaren. Nach dieser Klausel müssen Betroffene Schadensersatzansprüche gegebenenfalls auch gegenüber dem Unterauftragnehmer geltend machen können.

- Wie auch schon nach den alten Standardvertragsklauseln muss auch für die neuen Standardvertragsklauseln das Recht des Staates gelten, in dem der Auftraggeber seinen Sitz hat. Für Datenverarbeitungen durch den Unterbeauftragten muss nun auch zwingend das für den Auftraggeber geltende Datenschutzrecht Anwendung finden. Übermittelt ein deutsches Unternehmen Daten an einen Auftragnehmer in einem Drittstaat, der einige dieser Daten wiederum an einen Unterauftragnehmer weitergibt, so muss auch auf den Vertrag zwischen Auftragnehmer und Unterauftragnehmer deutsches Recht Anwendung finden.

- Zudem müssen die Vertragsverhältnisse mit Unterauftragnehmern sorgfältig dokumentiert werden. Der Auftragnehmer muss den Auftraggeber vor der Vergabe eines Unterauftrages nicht nur informieren und dessen schriftliche Einwilligung einholen. Der Auftragnehmer muss dem Auftraggeber auch zusätzlich Kopien der Unteraufträge zukommen lassen.

- Schließlich muss der Auftraggeber ein jährlich zu aktualisierendes Verzeichnis über Vereinbarungen mit den Unterauftragnehmern führen. Dieses Verzeichnis muss der Auftraggeber den für ihn zuständigen Aufsichtsbehörden bereitstellen. Dabei ist nicht eindeutig, ob damit nur eine Aufstellung der bestehenden Unteraufträge gemeint ist, oder ob darüber hinaus auch die jeweiligen Klauseln ersichtlich sein müssen. Es ist aber eher anzunehmen, dass ein Auftragnehmer die Verträge zu seinen Unterauftragsnehmern nicht offenlegen muss. Denn nach der Auffassung des Düsseldorfer Kreises müssen die Auftraggeber den Aufsichtsbehörden schon nicht die zwischen Auftraggeber und Auftragnehmer abgeschlossenen Standardvertragsklauseln offenlegen. Dann spricht aber auch nichts dafür, dass ein Unter-Auftraggeber die mit seinem Unter-Auftragnehmer vereinbarten Standardvertragsklauseln, die die gleichen Regelungen wie die im Auftragsverhältnis abgeschlossenen Standardvertragsklauseln enthalten müssen, offenlegen muss.

Anwendbares Recht für das Auftragsverhältnis

Die Standardvertragsklauseln beziehen sich jedoch nur auf datenschutzrechtliche Regelungen. Ein vollständiges Vertragswerk über eine Auftragsdatenverarbeitung in einem Drittland muss darüber hinaus auch noch wesentliche wirtschaftliche Punkte regeln. Auftraggeber und Auftragnehmer des Auftragsdatenverarbeitungsvertrages dürfen natürlich auch diese Punkte im weiteren Vertragswerk regeln.[1] Der Wortlaut der Standardvertragsklauseln und der Erwägungen der EU-Kommission hierzu schreiben zwar vor, dass die Standardvertragsklauseln (die sich auf den Datenschutz im Rahmen der Übermittlung beziehen) dem Recht des Staates unterliegen müssen, in dem der Auftraggeber seinen Sitz hat. Nunmehr muss auch für die Datenverarbeitung des Unterbeauftragten das für den Auftraggeber geltende Datenschutzrecht Anwendung finden. Gegebenenfalls besteht aber die Möglichkeit, die sonstigen (wirtschaftlichen) Regelungen auch einem anderen Rechtssystem zu unterstellen. Das lässt sich in der Praxis dadurch erreichen, dass die Standardvertragsklauseln beispielsweise als separater Anhang zu einem Outsourcing- oder Services-Vertrag ausgestaltet werden. Dieser Anhang kann dann – unabhängig von dem Hauptvertrag – dem Recht des Staates, in dem der Auftraggeber seinen Sitz hat, unterworfen werden. Es bleibt abzuwarten, wie sich die Aufsichtsbehörden gegenüber einer solchen Vorgehensweise positionieren werden.

ANWENDUNG DER NEUEN STANDARDVERTRAGSKLAUSELN BEI VERTRAGSÄNDERUNGEN

Hinsichtlich der Frage, ob die alten oder schon die neuen Standardvertragsklauseln angewendet werden müssen, weil eine geringfügige Veränderung eines bestehenden Vertrages vorgenommen wird, werden die Aufsichtsbehörden wahrscheinlich eher einen strengen Maßstab anlegen. Es ist zu erwarten, dass sie jede Änderung des Vertragsgegenstandes als Vertragsänderung im Sinne der Entscheidung der EU-Kommission werten. Die Frage, wann bereits eine solche geringfügige Änderung besteht, ist bei Verträgen, die aus einer Vielzahl von Vertragsbestandteilen bestehen, nicht immer leicht zu beantworten. Dies zeigt sich insbesondere bei umfangreichen IT-Service-Verträgen, die etwa eine Datenverarbeitung im EU-/EWR-Ausland zum Inhalt haben. Solche Verträge bestehen zumeist aus einem Master Services Agreement und haben dann zahlreiche Anhänge, die den Vertragsgegenstand näher definieren, wie z. B. Defined Terms, Statements of Work, Service Level Agreements, Pricing Terms und andere vergleichbare Regelungen.

AUSWIRKUNGEN AUF DIE PRAXIS

Unternehmen sollten auf die veränderte rechtliche Lage reagieren. Es empfiehlt sich, gründlich zu prüfen, ob und wie sie die neuen Standardvertragsklauseln verwenden sollten. Bei bestehenden Vertragsklauseln muss geprüft werden, ob bereits Änderungen an Vertragsteilen, Anhängen oder Zusatzvereinbarungen die Verwendung der neuen Klauseln nötig machen. Hierfür ist in erster Linie maßgeblich, wie umfangreich die vertraglichen Änderungen sind. Versäumnisse können Bußgelder, Schadensersatzansprüche und vor allem erhebliche Rufschädigungen durch negative Presse nach sich ziehen.

[1] *EU-Kommission, Beschluss 2010/87/EU, Erwägungsgrund 4, ABl. EG Nr. L 39 v. 12. Februar 2010, 5(5).*

Safe Harbor: Strengere Anforderungen an den Datentransfer in die USA

Wenn deutsche Unternehmen personenbezogene Daten an Unternehmen außerhalb der EU übermitteln, so müssen sie die strengen Anforderungen des Bundesdatenschutzgesetzes erfüllen. Für einen zulässigen Datentransfer müssen sie dann regelmäßig Maßnahmen treffen, um ein angemessenes Datenschutzniveau beim Empfänger sicherzustellen. Die Verwendung der Safe Harbor-Grundsätze ist eine dieser Maßnahmen.

Die für den Datenschutz zuständigen Aufsichtsbehörden haben nun neue Anforderungen an die Übermittlung personenbezogener Daten auf der Grundlage von Safe Harbor formuliert, die ganz erhebliche Folgen für in Deutschland tätige Unternehmen haben, die Daten in die USA übermitteln. Diese Firmen müssen sich daher darauf einstellen, dass der Datentransfer auf der Grundlage des Safe Harbor-Abkommens nun nur noch unter engeren Voraussetzungen als bislang zulässig ist – und dass die Datenschutz-Aufsichtsbehörden die Einhaltung dieser hohen Anforderungen genau kontrollieren werden.

SAFE HARBOR-ABKOMMEN ALS ERLAUBNIS FÜR DIE DATENÜBERMITTLUNG IN DIE USA

Die USA weisen grundsätzlich kein ausreichendes Schutzniveau für die Verarbeitung und Übermittlung personenbezogener Daten aus Europa auf. Die Übermittlung personenbezogener Daten aus Europa in Drittländer ohne angemessenes Datenschutzniveau ist nur dann erlaubt, wenn sichergestellt wird, dass ein angemessener Schutz der übermittelten Daten gewährleistet ist. Auch das Bereithalten von Daten für einen Abruf aus den USA wird als Datenübermittlung in ein Drittland ohne angemessenes Datenschutzniveau gewertet.

Die EU und die USA haben im Jahr 2000 das sogenannte „Safe Harbor"-Abkommen abgeschlossen, eine Vereinbarung über die Voraussetzungen für einen erlaubten Datentransfer aus EU-Staaten in die USA.[1] Das Safe Harbor-Abkommen ermöglicht es Unternehmen, einen angemessenen Datenschutzstandard dadurch herzustellen, dass sie diesem Abkommen beitreten und sich den Safe Harbor-Grundsätzen verbindlich unterwerfen. Das Verfahren hierzu ist nicht allzu kompliziert; Unternehmen können sich auf der Website des US-amerikanischen Handelsministeriums online registrieren.[2] Auf dieser Seite ist auch die Liste der Unternehmen, die sich den Safe Harbor-Regeln unterworfen haben, abrufbar. Dass dieses Abkommen für viele Unternehmen, die aus Geschäftsgründen international Daten übertragen müssen, eine praktikable Lösung darstellt, belegen die Zahlen: nach einer Pressemitteilung des Bundesbeauftragten für den Datenschutz und der Informationsfreiheit vom 25. Oktober 2006 waren zu diesem Zeitpunkt bereits über 1.000 Unternehmen dem Safe Harbor-Abkommen beigetreten.

NEUE ANFORDERUNGEN DER DATENSCHUTZ-AUFSICHTSBEHÖRDEN

Nun müssen sich Unternehmen auf verschärfte Anforderungen einstellen. Das gemeinsame Abstimmungsgremium der obersten Aufsichtsbehörden für den Datenschutz in der Privatwirtschaft – der sogenannte Düsseldorfer Kreis – hat kürzlich einen wichtigen Beschluss über die Datenübermittlung nach Safe Harbor-Grundsätzen gefasst.[3] Mit diesem Beschluss stellen die Aufsichtsbehörden deutlich höhere Anforderungen als bisher an die grenzüberschreitende Datenübermittlung unter dem Safe Harbor-Abkommen. Die Aufsichtsbehörden auf Landesebene orientieren sich bei ihrem Vorgehen in aller Regel stark an den Vorgaben des Düsseldorfer Kreises – daher sollten Unternehmen den Beschluss beachten und umsetzen.

In Deutschland tätige Unternehmen, die auf der Grundlage von Safe Harbor Daten in die USA übermitteln, sind gut beraten, die Anforderungen der Aufsichtsbehörden für den Datenschutz möglichst zeitnah umzusetzen. Bei Verstößen gegen die Vorschriften des Bundesdatenschutzgesetzes drohen Bußgelder von bis zu 300.000 Euro, die Abschöpfung

[1] Entscheidung 2000/520/EG der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA, ABl. L 215 vom 25.8.2000, abrufbar unter http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:DE:PDF.

[2] Diese Liste ist abrufbar unter https://www.export.gov/safehrbr/list.aspx.

[3] Der Beschluss ist u.a. abrufbar unter: https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2010/Pruefung_der_Selbst-Zertifizierung_des_Datenimporteuers/Beschluss_28_29_04_10.pdf.

von Gewinnen, Schadensersatzklagen und erhebliche Rufschäden. Besonders schwere Verstöße gegen das Bundesdatenschutzgesetz sind strafbar; es droht Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe.

Die einzelnen Kontrollbehörden für den Datenschutz orientieren sich in hohem Maß an den Vorgaben des Düsseldorfer Kreises. Durch dessen Beschluss ist der Datentransfer auf der Grundlage des Safe Harbor-Abkommens künftig nur noch unter engeren Voraussetzungen möglich als bislang. Der Düsseldorfer Kreis hat in seinem Papier die folgenden Voraussetzungen aufgestellt:

- Mehr als sieben Jahre zurückliegende Safe Harbor-Zertifizierungen sollen grundsätzlich nicht mehr als gültig betrachtet werden.

- Das Daten in die USA exportierende Unternehmen soll sich vom Datenempfänger nachweisen lassen, wie das importierende US-Unternehmen seinen Informationspflichten gegenüber den von der Datenverarbeitung Betroffenen nachkommt. Dies sei auch deshalb wichtig, damit der Datenimporteur in den USA diese Information an die von der Übermittlung Betroffenen weitergeben kann.

- Daten exportierende Unternehmen müssen eine Prüfung solcher Mindestkriterien dokumentieren und auf Nachfrage der Aufsichtsbehörden nachweisen können.

FOLGEN DER VERSCHÄRFTEN AUFSICHTSPRAXIS

Im Ergebnis werden deutsche Unternehmen, die auf der Grundlage des Safe Harbor-Abkommens personenbezogene Daten in die USA übermitteln, damit verpflichtet, bei ihren Vertragspartnern die Einhaltung der Safe Harbor-Grundsätze zu überprüfen. Falls eine solche Überprüfung nicht möglich ist, empfehlen die Aufsichtsbehörden, das angemessene Datenschutzniveau auf anderem Wege zu gewährleisten, insbesondere durch die Verwendung von EU-Standardvertragsklauseln zur Datenübermittlung.

EMPFEHLUNGEN FÜR DIE UNTERNEHMENSPRAXIS

Unternehmen, die auf der Grundlage des Safe Harbor-Abkommens personenbezogene Daten an US-Unternehmen übermitteln, müssen der geänderten Praxis der Aufsichtsbehörden zeitnah Rechnung tragen, wenn sie Geldbußen, Rufschäden und mögliche Schadensersatzansprüche Betroffener vermeiden wollen.

1. Nachweise fordern

Deutsche Datenexporteure sollten umgehend auf ihre Vertragspartner zugehen und von diesen die entsprechenden Nachweise verlangen, wie sie die zuständigen Aufsichtsbehörden fordern. Diese Nachweise sollten sorgfältig archiviert werden, um sie auf Nachfrage der Aufsichtsbehörde vorlegen zu können.

2. Verträge gestalten

Bei der Gestaltung künftiger Verträge zur Datenübermittlung auf der Grundlage des Safe Harbor-Abkommens sollten deutsche Datenübermittler noch mehr darauf achten, ihre Vertragspartner in den USA auf die Einhaltung der Safe Harbor-Grundsätze zu verpflichten, z. B. durch Regelungen über Vertragsstrafen bei Verstößen gegen den Datenschutz. Zudem ist es zweckmäßig, auch Kontrollrechte des Datenübermittlers zu vereinbaren.

3. Information Betroffener

Zudem sind Klauseln zweckmäßig, nach denen der US-Vertragspartner während der Vertragslaufzeit regelmäßig aktuelle Zertifizierungsbestätigungen nachweist und kontinuierlich Nachweise vorlegt, wie das US-Unternehmen seinen Informationspflichten gegenüber den von der Datenverarbeitung Betroffenen nachkommt.

Neuer Gesetzesentwurf: Bundesrat fordert Einführung eines „Street View-Gesetzes“ und Änderungen des Bundesdatenschutzgesetzes

Der Bundesrat hat am 9. Juli 2010 einen neuen Gesetzentwurf zur Änderung des Bundesdatenschutzgesetzes (BDSG) eingebracht. Während Innen- und Justizministerium noch über die Einführung des geplanten Beschäftigtendatenschutzgesetzes diskutieren, Gewerkschaften mehr Arbeitnehmerdatenschutz fordern, Transparency International effektive Möglichkeiten zur Korruptionsbekämpfung fordert und Arbeitgeber sich klarere und praxistauglichere Regeln wünschen, will der Bundesrat das Filmen von Straßenzügen und Gebäuden neu regeln. Ein neuer § 30b BDSG soll Bildaufnahmen und andere persönliche Daten der Bürger in Deutschland schützen. Im Rahmen der Übermittlung des Gesetzesentwurfs stellt der Bundesrat einen Katalog von Vorgaben zu weiteren Änderungen des BDSG vor. Falls es zu einer Umsetzung der im Gesetzesentwurf aufgestellten Forderungen des Bundesrats nach einer umfassenden Neuregelung des Datenschutzes kommt, hat dies für Unternehmen weitreichende Folgen. Dieser Überblick fasst das Vorhaben des Bundesrats zusammen und gibt einen Ausblick, welche Veränderungen zu erwarten sind.

HINTERGRUND DER GESETZESINITIATIVE

Ein Anbieter von Online-Diensten war durch das Vorgehen des Unternehmens bei der Erfassung von W-LAN-Daten im Rahmen des Street View-Projekts in die öffentliche Kritik geraten. Datenschützer bemängelten die fehlende Berücksichtigung der Persönlichkeitsrechte Betroffener. Hamburg hatte bereits am 24. April 2010 eine Gesetzesinitiative in den Bundesrat eingebracht, die flächendeckende digitale Aufnahmen von Straßenpanoramen durch private Unternehmen und deren anschließende Veröffentlichung im Internet regeln sollte. Nun hat sich der Bundesrat auf einen Gesetzesentwurf verständigt.

FORDERUNGEN DES BUNDESRATS ZU STREET VIEW UND CO.

Der Bundesrat schlägt in dem Gesetzesentwurf eine besondere datenschutzrechtliche Regelung vor „für den Umgang mit personenbezogenen Daten, die im Zusammenhang mit der georeferenzierten großräumigen Erfassung von Gebäuden, Straßen, Plätzen sowie vergleichbaren Geodaten zum Zweck des Bereithaltens fotografischer oder filmischer Aufnahmen im Internet zum Abruf für jedermann oder zur Übermittlung an jedermann erhoben und gespeichert sowie anschließend an Dritte übermittelt oder über das Internet beispielsweise durch Eingabe einer Anschrift jedermann zugänglich gemacht werden sollen“.

Das soll heißen: Der Bundesrat will Street View und ähnliche Dienste reglementieren. Hierzu soll ein neuer § 30b in das BDSG eingefügt werden:

- Online-Dienste sollen Personen oder Kfz-Kennzeichen unkenntlich machen, bevor diese online gestellt werden.

- Eigentümer, Mieter, Fahrzeughalter und sonstige Betroffene sollen der weiteren Verarbeitung und Nutzung ihrer sonstigen personenbezogenen Daten widersprechen können. Im Falle eines solchen Widerspruchs sind die Daten zu anonymisieren oder zu löschen.

- Spätestens eine Woche vor einer großräumigen Erfassung von Gebäuden, Straßen, Plätzen oder ähnlichen Geodaten soll der Online-Dienst Ort und Zeitpunkt der geplanten Aufnahmen in örtlichen Tageszeitungen und im Internet bekanntgeben.

- Vier Wochen, bevor die Daten ins Internet gestellt oder zum Abruf bereit gehalten werden, muss in Tageszeitungen und im Internet erneut auf das bereits angesprochene Widerspruchsrecht hingewiesen werden.

Auch § 43 BDSG soll geändert werden. Diese Norm regelt die Bußgeldtatbestände bei verbotenem Umgang mit personenbezogenen Daten. Verstöße gegen die geplante Neuregelung zu den Aufnahmen von Geodaten des BDSG sollen mit Geldbußen bis zu 300.000 Euro bestraft werden. Falls ein Unternehmen durch Datenschutzverstöße höhere Beträge erwirtschaftet, so soll das Bußgeld entsprechend erhöht werden.

Offenbar reagiert der Bundesrat mit seinem Vorstoß auf die Presseberichte zum Vorgehen bei Street View und ähnlichen Projekten. Man mag sich fragen, ob nicht auch schon das geltende Datenschutzrecht ein Vorgehen gegen mögliche Persönlichkeitsrechtsverletzungen durch systematisches Aufnehmen von Gebäuden, Straßenzügen, Autos, Personen und so fort hinreichend geregelt hat. Man mag das Vorgehen des Bundesrats auch als Beispiel für die derzeitige Neigung des Gesetzgebers sehen, sich bei seiner Arbeit im Datenschutz an Einzelfällen auszurichten, anstatt das BDSG – wie es dringend nötig wäre – grundlegend zu überarbeiten und an den heutigen Stand der (Informations-)Technik anzupassen. Aber immerhin hat der Bundesrat den generellen Überarbeitungsbedarf des geltenden BDSG erkannt. Er erinnert in seiner Gesetzesinitiative an seinen Beschluss vom 13. Februar 2009, in dem er die Bundesregierung gebeten hatte, einen Diskussionsentwurf für ein grundsätzlich überarbeitetes Datenschutzrecht vorzulegen.

FORDERUNGEN NACH WEITEREN ÄNDERUNGEN DES BDSG

Der Bundesrat hält die Regelung zum Filmen und Verbreiten von Geodaten nur für einen ersten Schritt auf dem Weg zur Schaffung eines modernen und einheitlichen Datenschutzrechts. Darüber hinaus fordert der Bundesrat noch eine Reihe weiterer Regelungen, etwa zu den folgenden Punkten:

Erweiterung von Auskunfts- und Informationspflichten

Der Bundesrat fordert eine Verbesserung der Transparenz der Datenverarbeitung durch erweiterte Auskunfts- und Informationspflichten der Daten verarbeitenden Stellen.

Bereits nach dem geltenden Recht haben Unternehmen, die personenbezogene Daten erheben, verarbeiten oder nutzen, eine Vielzahl von Informationspflichten zu beachten. Allerdings sind diese Regelungen so unstrukturiert und komplex aufgebaut, dass man oft einen Fachmann im Datenschutz braucht, um die eigenen Pflichten zu kennen und ihnen angemessen nachzukommen. Hier sind vor allem klare und praxisgerechte Regeln gefragt.

Grenzen für die Erstellung von Persönlichkeitsprofilen oder zu Personenbewertungen

Der Gesetzesentwurf sieht enge Grenzen für die Bildung von Persönlichkeitsprofilen vor, etwa zu Verbraucherverhalten und Internetnutzung oder für Bewegungsprofile. Zudem sollen Rahmenbedingungen für die Bewertung von Personen im Internet geschaffen werden, etwa von Lehrern oder Professoren durch deren Schüler oder Studenten.

Soziale Netzwerke

Der Bundesrat fordert ferner Regeln für einen verbesserten Schutz des Persönlichkeitsrechts der Nutzer sozialer Netzwerke, wie etwa Facebook oder Xing.

Klarstellung der Anforderungen an wirksame Einwilligungen

Zudem ist eine Präzisierung der bislang recht umstrittenen Anforderungen an die Wirksamkeit von Einwilligungen vorgesehen.

AUSWIRKUNGEN AUF DIE DATENSCHUTZPRAXIS

In der Tat wären bei der Zulässigkeit von Einwilligungen im Rahmen des BDSG einige Klarstellungen des Gesetzgebers dringend notwendig. Derzeit vertreten Fachleute und Aufsichtsbehörden eine Vielzahl unterschiedlicher Auffassungen über die Anforderungen, die an wirksame datenschutzrechtliche Einwilligungen zu stellen sind. Es steht zu hoffen, dass der Gesetzgeber bei der Schaffung einer abschließenden Regelung auch berücksichtigt, dass es durchaus Situationen gibt, in denen Unternehmen im Wirtschaftsleben auf die Verwendung von Einwilligungen angewiesen sind, beispielsweise beim Abschluss von Versicherungsverträgen.

Stärkung der Vorabkontrolle durch den Datenschutzbeauftragten

Vorgesehen ist auch eine Stärkung der innerbetrieblichen Vorabkontrolle bei Datenverarbeitungsverfahren. Eine solche Vorabkontrolle ist nach dem bereits geltenden Recht für Verarbeitungsverfahren vorgeschrieben, die besonders riskant sind für diejenigen, deren Rechte und Freiheiten von der Datenverarbeitung betroffen sind. Allerdings regelt das BDSG nur sehr unklar, in welchen Fällen eine solche Vorabkontrolle durch den betrieblichen Datenschutzbeauftragten vorgeschrieben ist.

Auch im Rahmen der Vorabkontrolle sind klare und verständliche Vorgaben notwendig, unter welchen Voraussetzungen Unternehmen eine solche Vorabkontrolle durchführen müssen. Die derzeitige Unsicherheit erschwert es Unternehmen deutlich, die Anforderungen des Datenschutzes zu erkennen und zu erfüllen. Eine praxisgerechte Regelung zur Durchführung vorgeschriebener Vorabkontrollen würde in der Praxis auch die Stellung des Datenschutzbeauftragten aufwerten – was für die Einhaltung der Vorschriften des Datenschutzes in Unternehmen sicher ein wichtiger Schritt wäre.

Verpflichtung zur Einführung eines innerbetrieblichen Datenschutzkonzepts

Zudem sieht der Gesetzesentwurf eine Verpflichtung der für eine Datenverarbeitung verantwortlichen Stelle(n) vor, ein Datenschutzkonzept zu entwickeln und auf Verlangen der Datenschutzbehörde vorzulegen. Für größere Unternehmen wäre ein solcher Schritt machbar und sicher auch sinnvoll. Hierbei sollte die geplante gesetzliche Regelung sich nicht an abstrakten Schwellenwerten (wie etwa der Beschäftigtenzahl) orientieren, sondern an dem konkreten Gefährdungspotential des jeweiligen Unternehmens. Ein kleiner Adressdatenhändler oder ein kleines Detektivbüro können dringender ein Datenschutzkonzept benötigen als ein großer Handwerksbetrieb, der kaum mit personenbezogenen Daten umgeht. Einen solchen risikobasierten Ansatz sehen aufsichtsrechtliche Vorschriften auch in anderen Bereichen vor, etwa bei für Banken oder Versicherungen vorgeschriebenen Gefährdungsanalysen.

Verbesserung der Eigenkontrolle

Die Selbstkontrolle der für Datenverarbeitungen verantwortlichen Stellen soll gestärkt werden, etwa durch Festlegung von Mindestanforderungen an die Fachkunde des betrieblichen Datenschutzbeauftragten oder die Verpflichtung zur Erbringung geeigneter Nachweise. Zudem sollen Unternehmen den Beauftragten für den Datenschutz bei allen datenschutzrechtlichen Vorgängen zwingend und rechtzeitig beteiligen.

BEWERTUNG/BEURTEILUNG

Dieser Vorstoß ist uneingeschränkt zu begrüßen. Das derzeitige Datenschutzrecht ist ausgesprochen komplex, aber wenig anwenderfreundlich. Bei der aktuellen Gesetzeslage brauchen Unternehmen oftmals spezialisierte Fachleute, um sich gesetzeskonform zu verhalten und das Risiko von Datenschutzverstößen sicher auszuschließen. Sowohl Anforderungen an die Fachkunde von Datenschutzbeauftragten als auch eine Stärkung ihrer Stellung im Unternehmen sind ein Schritt in die richtige Richtung.

WIE GEHT ES WEITER MIT DEM DATENSCHUTZ?

Der Datenschutz in Deutschland ist in Bewegung. Sogenannte Datenskandale bei deutschen Großunternehmen, BDSG-Reform von 2009, der Referentenentwurf vom Mai 2010 zur Einführung eines neuen Beschäftigtendatenschutzes und nun der neue Gesetzentwurf des Bundesrats sind nur einige Eckpunkte, die dies belegen. Doch auch die EU bleibt nicht untätig. Die EU-Kommission hat bereits angekündigt, die dem BDSG zu Grunde liegende Datenschutz-Richtlinie zu überarbeiten. Man braucht kein Fachmann zu sein, um künftige Gesetzesänderungen beim Datenschutz vorherzusagen.

In einem Punkt kann man dem Bundesrat uneingeschränkt zustimmen. Das geltende Datenschutzrecht muss in der Tat gründlich überarbeitet werden. Die derzeitigen Spielregeln sind auch für Fachleute kaum noch verständlich. Wer einen Blick in das Gesetz wirft, sieht sofort, welch chaotische Struktur das ständige Einfügen und Überarbeiten einzelner Regelungen hinterlassen hat. Selbst gut ausgebildete Juristen sind oft nicht ohne Weiteres in der Lage festzustellen, was das BDSG im Einzelnen vorschreibt.

Was ist eigentlich: die Übermittlung von Daten?

Das Bundesdatenschutzgesetz spricht stets von der Erhebung, Verarbeitung, Nutzung und Übermittlung von Daten. Das Weitergeben von Daten an dritte Personen, an andere Geschäftsbereiche innerhalb eines Konzerns oder an andere Unternehmen spielt im Unternehmensalltag eine erhebliche Rolle. Doch ist damit jedes Mal der Tatbestand einer „Übermittlung" erfüllt, wie sie im Gesetz benannt ist und an die zusätzliche Voraussetzungen geknüpft sind?

Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener Daten an einen Dritten. Dritter heißt in diesem Zusammenhang jede Person oder Stelle *außerhalb* der verantwortlichen Stelle. Die verantwortliche Stelle ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Im Wirtschaftsleben sind dies vor allem Unternehmen, die rechtlich selbständig sind. Auch im Konzern verbundene Unternehmen sind jeweils eine eigene verantwortliche Stelle. Denn das BDSG kennt kein sogenanntes Konzernprivileg. Das bedeutet, dass die Weitergabe von Daten von einem Konzernunternehmen an ein anderes eine Datenübermittlung darstellt, die einer Erlaubnisnorm bedarf.

Nicht Dritte sind demnach Personen oder Stellen *innerhalb* der verantwortlichen Stelle. Die Weitergabe von Daten an diese stellt eine Nutzung von Daten, aber keine Übermittlung dar. Werden also Daten vom Einkauf an die Buchhaltung eines Unternehmens weitergegeben, so werden die Daten nur genutzt aber nicht übermittelt. Zwar bedarf auch die Nutzung von Daten einer Erlaubnisnorm, die Anforderungen sind aber de facto geringer, da die Nutzung von Daten innerhalb eines Unternehmens weniger einschneidend für das Persönlichkeitsrecht der Betroffenen als die Übermittlung an Dritte ist.

Eine Übermittlung kann in zwei Formen vorliegen: entweder in dem aktiven Weitergeben von personenbezogenen Daten an einen Dritten oder in dem Bereithalten von Daten zur Einsicht oder zum Abruf durch einen Dritten. Sobald der Dritte die Daten einsieht oder abruft, sind die Daten an den Dritten übermittelt.

Werden die Daten hingegen nur an eine Person oder Unternehmen weitergegeben, die Daten im Auftrag nach § 11 BDSG verarbeitet, so stellt das keine Übermittlung dar. Diese Stelle fungiert dann quasi als „verlängerter Arm" für die verantwortliche Stelle. Diese Verarbeitung ist privilegiert.

About Mayer Brown

Mayer Brown is a leading global law firm with offices in major cities across the Americas, Asia and Europe. We have approximately 875 lawyers in the Americas, 300 in Asia and 425 in Europe. Our presence in the world's leading markets enables us to offer clients access to local market knowledge combined with global reach.

We are noted for our commitment to client service and our ability to assist clients with their most complex and demanding legal and business challenges worldwide. We serve many of the world's largest companies, including a significant proportion of the Fortune 100, FTSE 100, DAX and Hang Seng Index companies and more than half of the world's largest investment banks. We provide legal services in areas such as Supreme Court and appellate; litigation; corporate and securities; finance; real estate; tax; intellectual property; government and global trade; restructuring, bankruptcy and insolvency; and environmental.

OFFICE LOCATIONS

AMERICAS
- Charlotte
- Chicago
- Houston
- Los Angeles
- New York
- Palo Alto
- São Paulo
- Washington

ASIA
- Bangkok
- Beijing
- Guangzhou
- Hanoi
- Ho Chi Minh City
- Hong Kong
- Shanghai

EUROPE
- Berlin
- Brussels
- Cologne
- Frankfurt
- London
- Paris

ALLIANCE LAW FIRMS
- Spain, Ramón & Cajal
- Italy and Eastern Europe, Tonucci & Partners

Please visit www.mayerbrown.com for comprehensive contact information for all Mayer Brown offices.

0810