BRUNO SCHIERBAUM

Datenübermittlung ins Ausland – neue Vorgaben im BDSG

Sensibles Thema: Übermittlung von Arbeitnehmerdaten ins Ausland – sei es an die Konzernmutter oder Geschäftspartner. Klar: Die Vorgaben des novellierten Bundesdatenschutzgesetzes sind einzuhalten – auch wenn die Datenübermittlung durch Betriebsvereinbarung geregelt wird! Aber was hat die Novellierung (vielleicht) an Fortschritten oder Klarheit zu diesem Thema gebracht?

Die EG-Datenschutzrichtlinie hat die Novellierung des Bundesdatenschutzgesetzes (BDSG) und auch der Landesdatenschutzgesetze gerade in dem Punkt ›Übermittlung von Daten ins Ausland‹ erforderlich gemacht (zu den alten Regelungen siehe: ›Grenzüberschreitender Datentransfer‹ in cf 8-9/99 ab Seite 36). Das entsprechend angepasste BDSG ist im Mai 2001 in Kraft getreten und ein Teil der Landesdatenschutzgesetze ist ebenfalls novelliert worden.

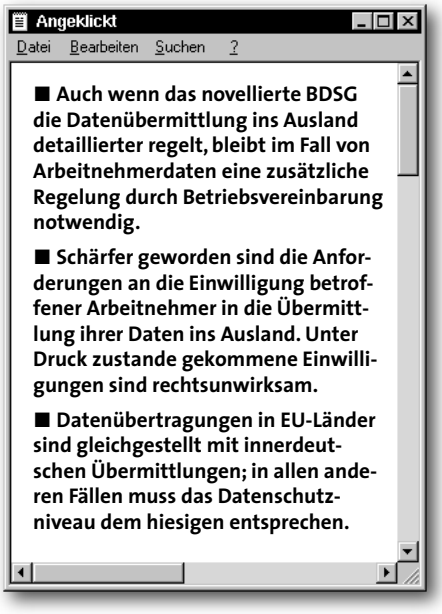
Schon aus der Überschrift der EG-Richtlinie wird deutlich, dass zwei zentrale Anliegen verfolgt werden sollen. Die Datenschutz-Richtlinie ist vom Europäischen Parlament und vom Rat der Europäischen Union als Richtlinie »zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr« erlassen worden. Durch die Vorgabe ›freier Datenverkehr‹ wird die Zielrichtung verfolgt, dass durch ein gleichwertiges Datenschutzniveau innerhalb der Europäischen Union die Datenübermittlung in ein dort ansässiges Unternehmen oder eine Organisation erleichtert werden soll. So enthält das neue BDSG mit den §§ 4 b und c zum ersten Mal für den so genannten *nicht-öffentlichen Bereich* (Privatbetriebe, Vereine, Stiftungen usw.) eine eigenständige Regelung zur Übermittlung personenbezogener Daten ins Ausland. Für den *öffentlichen* Bereich des Bundes gab es bereits im alten BDSG in § 17 eine entsprechende Regelung.

Die Vorgaben der EG-Richtlinie und auch des BDSG zur Datenübermittlung tragen damit einer Entwicklung Rechnung, die sich seit Jahren zeigt: Die fortschreitende Globalisierung und die rasante Entwicklung der Informations- und Kommunikations-Techniken lassen auch den grenzüberschreitenden Datenverkehr selbstverständlich werden.

Die Anzahl multinationaler Konzerne wächst und die weltweiten Datennetze vereinfachen den Datenaustausch. Trotz der Zunahme des globalen Datenverkehrs fehlte es allerdings (und fehlt es noch) am globalen Datenschutz.

Wichtige Neuerungen bei der Übermittlung von Daten sind, dass die ›übermittelnde Stelle‹ (z.B. ein Unternehmen) jetzt gemäß § 4 b Abs. 5 BDSG *die Verantwortung* für die Zulässigkeit und Rechtmäßigkeit der Übermittlung trägt. Dabei hängt die Zulässigkeit einer Übermittlung immer vom Datenschutzniveau *im Empfängerland* ab. Zusätzlich ist die ›Stelle‹, an die Daten übermittelt werden, darauf hinzuweisen, dass die erhaltenen Daten nur *zu dem Zweck* verarbeitet oder genutzt werden dürfen, zu dem sie übermittelt werden.

Trotz dieser gesetzlichen Regelungen bleibt der Abschluss von Betriebsvereinbarungen ein zentrales Regelungsinstrument für die rechtmäßige Übermittlung von Beschäftigten-Daten ins Ausland. Deshalb auch bedarf die Datenübermittlung über die Grenzen der



Bundesrepublik Deutschland hinaus hier einer genaueren Betrachtung – wobei die Materie mit der Novellierung des BDSG keineswegs einfacher geworden ist ...

Zentrale Vorgaben des BDSG

Bei einer Datenübermittlung ins Ausland sind als zentrale Vorgaben der § 4 in Verbindung mit § 28 BDSG zu beachten. Zusätzlich oder auch neben diesen Paragrafen kommen noch § 4 b und § 4 c BDSG zum Tragen. Im § 4 BDSG steht dabei der zentrale und etwas banal klingende Grundsatz, dass die Übermittlung personenbezogener Daten *immer verboten ist – außer sie ist erlaubt*.

Das heißt: Auch für die *Übermittlung* personenbezogener Daten muss es in jedem Fall eine *rechtliche Grundlage* geben, ansonsten dürfen entsprechende Übermittlungen nicht stattfinden. Für eine rechtmäßige Übermittlung personenbezogener Daten sind folgende ›Erlaubnistatbestände‹ denkbar:

- Die Übermittlung erfolgt mit *Einwilligung* des Betroffenen (Beschäftigten); dabei sind die an eine Einwilligung geknüpften Vorgaben (§ 4 a BDSG) zu beachten.
- Die Übermittlung erfolgt im Rahmen der *Zweckbestimmung* des Vertragsverhältnisses (Arbeitsvertragsverhältnisses), wobei die berechtigten Interessen des übermittelnden Unternehmens mit den berechtigten schutzwürdigen Interessen des Betroffenen (Beschäftigten) abzuwägen sind (§ 28 BDSG).
- Die Übermittlung kann auch auf § 4 b und § 4 c BDSG gestützt werden, die verschiedene Möglichkeiten einer Übermittlung gerade bei nicht-angemessenem Datenschutzniveau im so genannten Drittland...[1] vorsehen.
- Die Übermittlung erfolgt auf der Basis einer ›anderen Rechtsvorschrift‹ – auch eine Betriebsvereinbarung kann eine solche Vorschrift sein.

Alle diese genannten Voraussetzungen werfen erhebliche Auslegungsprobleme auf, wobei in der betrieblichen Praxis vor allem dem betrieblichen Datenschutzbeauftragten die Aufgabe zukommt, auf die Rechtmäßigkeit der Übermittlung von Daten hinzuwirken. *Verantwortlich* für die rechtmäßige Übermittlung ist jedoch die übermittelnde Stelle (Arbeitgeber) selbst.

In jedem Fall muss *eine* der hier genannten Voraussetzungen gegeben sein, ehe ein Unternehmen personenbezogene Daten ins Ausland transferieren darf! Kommen wir zu den Einzelheiten:

... Einwilligung des Betroffenen

Mit der Novellierung sind die Anforderungen an eine Einwilligung durch die Betroffenen (z. B. Arbeitnehmer) verschärft und in einem eigenständigen § 4 a BDSG verankert worden. An eine Einwilligungserklärung sind jetzt bestimmte Anforderungen gestellt.

So ist eine Einwilligung nur wirksam, wenn sie auf der *freien Einscheidung* des Betroffenen (Beschäftigten) beruht. Ist sie etwa auf Druck durch den Arbeitgeber hin erteilt worden – zum Beispiel durch Drohung mit Kündigung oder anderen nachteiligen Maßnahmen –, ist sie nicht rechtmäßig erteilt worden.

Zudem ist der Betroffene auf den vorgesehenen *Zweck* der Übermittlung und auch auf die *Folgen einer Einwilligungsverweigerung* hinzuweisen. Eine Einwilligungserklärung muss außerdem ›hinreichend bestimmt‹ sein, das heißt, der Betroffene muss *vorher* wissen, in *was* er einwilligen soll. Dies ist nur dann der Fall, wenn die Erklärung *ausführlich* und *transparent* genug gehalten ist, so dass der Betroffenen die Reichweite seiner Einwilligung genau abschätzen kann.

In einer vorgelegten Einwilligungserklärung muss auch zu erkennen sein, um *welche personenbezogenen Daten* es sich handelt, *wo* und durch *wen* die Daten verarbeitet und ausgewertet werden und es muss ebenfalls deutlich sein, dass sich die Einwilligung auch auf den Transfer der Daten an andere Stellen oder Unternehmen bezieht.

Die Einwilligung bedarf der *Schriftform* und muss eigenhändig vom Einwilligenden unterschrieben werden. Soll sie *zusammen mit anderen* Erklärungen schriftlich (z. B. mit Abschluss des Arbeitsvertrags) abgegeben werden, ist sie besonderes hervorzuheben. Soweit im Rahmen einer Datenübermittlung besonders sensible Daten...[2] weitergegeben werden sollen, muss die Einwilligung sich *ausdrücklich* auch auf diese Daten beziehen.

Bei der Formulierung einer solchen – ja nicht ganz unkomplizierten – Einwilligungserklärung ist in jedem Fall auch der Betriebsrat zu beteiligen, denn es handelt sich dabei um einen mitbestimmungspflichtigen ›Personalfragebogen‹ im Sinne des § 94 BetrVG ...

... BDSG selbst als Rechtsgrundlage

Für die Prüfung, ob das BDSG *selbst* die Grundlage für eine rechtmäßige Datenübermittlung bilden kann, sind § 28 und die §§ 4 b und c BDSG heranzuziehen, wobei – wie gesagt – entscheidend ist, ob im Drittland ein angemessenes Datenschutzniveau besteht oder nicht. Allerdings sind gerade durch die neu eingefügten §§ 4 b und c BDSG eine Fülle an nicht immer nachvollziehbaren *Ausnahmen* geschaffen worden, wonach eine Übermittlung auch bei nicht-angemessenem Datenschutzniveau möglich sein soll ... Zunächst aber:

Datenübermittlung bei angemessenen Schutzniveau

Nach Vorgabe der EG-Datenschutzrichtlinie enthält § 4 b BDSG eine diffe-

1... Der Begriff ›Drittland‹ wird in der EG-Richtlinie für ein Land außerhalb der Europäischen Union verwendet und taucht somit auch in den Vorgaben der EU zum Datenschutz auf. Im BDSG wird dieser Begriff nicht verwandt.

2... Als ›besonders sensible‹ Daten sind gemäß § 3 Abs. 9 BDSG anzusehen: »Besondere Arten personenbezogener Daten sind Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit und Sexualleben.«

renzierte – aber nicht sehr übersichtliche – Regelung für die Übermittlung personenbezogener Daten ins Ausland.

Der Absatz 1 des § 4 b BDSG stellt dabei den *innergemeinschaftlichen* dem *inländischen* Datenverkehr gleich. So ist ein Datentransfer von München nach Paris in Zukunft genauso zu behandeln wie ein Datentransfer von München nach Hamburg. Somit gelten die in § 28 BDSG enthaltenen Zulässigkeitsvoraussetzungen jetzt auch für die Übermittlung von Daten *innerhalb der EU* und in *Staaten des Europäischen Wirtschaftsraums* (Norwegen, Island, Liechtenstein).

Nach § 28 Abs. 1 BDSG ist das Übermitteln personenbezogener Daten als Mittel zur Erfüllung eigener Geschäftszwecke zulässig, ...

1. wenn es der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen (Beschäftigten) dient,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle (Unternehmen) erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an einem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Vertragsverhältnis oder vertragsähnliches Vertrauensverhältnis

Voraussetzung sowohl für die Erhebung, Speicherung, Veränderung, Nutzung als auch für die Übermittlung personenbezogener Daten ist, dass sie *im Rahmen der Zweckbestimmung* eines Vertragsverhältnisses oder eines vertragsähnlichen Vertrauensverhältnisses erfolgen.

Vertragsverhältnisse sind unter anderem Arbeitsverträge. Vertragsähnliche Vertrauensverhältnisse können während der konkreten Anbahnung eines Vertrags (Arbeitsvertrags) im Rahmen von Vorverhandlungen bestehen. Dabei kommt es auf einen später erfolgreichen Vertragsabschluss nicht an.

Auch *nach*-vertragliche Vertrauensverhältnisse, die etwa nach Beendigung eines Arbeitsverhältnisses bestehen können, werden gleichgestellt.

›Im Rahmen der Zweckbestimmung‹ bedeutet: Es dürfen *ausschließlich* die Daten übermittelt werden, die der Erfüllung der Pflichten oder der Wahrung der Rechte aus dem Vertragsverhältnis dienen. Um erkennen zu können, um welche Rechte und Pflichten es bei der Zweckbestimmung gehen kann, muss es als Voraussetzung *übereinstimmende Willenserklärungen* der Vertragsparteien (z. B. Arbeitgeber und Arbeitnehmer) geben. Das bedeutet auch, dass der Anspruch der datenverarbeitenden Stelle auf eine Übermittlung von Daten *gleichwertig* neben dem Anspruch des Betroffenen auf Ausschluss der Übermittlung steht.

Es kommt also bei der Festlegung der Zweckbestimmung nicht etwa einseitig auf die Vorstellungen der verantwortlichen Stelle (des Arbeitgebers, der Daten übermitteln will) an. Hat der Arbeitgeber aus wirtschaftlichen Gründen ein Interesse an der Übermittlung, reicht das allein für die Rechtmäßigkeit nicht aus. Vielmehr müssen gleichzeitig die berechtigten Datenschutz-Interessen des Betroffenen beachtet werden, worauf der nächste Punkt ebenfalls abzielt.

Wahrung berechtigter Interessen

Neben der eng zu fassenden Zweckbestimmung ist zusätzlich zu beachten, dass eine Datenübermittlung immer dann erlaubt ist, wenn sie zur Wahrung berechtigter Interessen der verantwortlichen Stelle (Unternehmen) erforderlich ist *und* wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen (Beschäftigten) am Ausschluss der Übermittlung überwiegt.

Konkret heißt das, dass im Prinzip *vor* jeder Entscheidung über eine Datenübermittlung neben der eng zu fassenden Zweckbestimmung *auch eine Interessenabwägung* vorgenommen werden muss. Wobei eine Übermittlung immer dann zu unterbleiben hätte, wenn das schutzwürdige Interesse des Betroffenen *überwiegt*. Dies wäre zum Beispiel dann der Fall, wenn in dem Empfängerland kein dem deutschen entsprechendes Datenschutzniveau vorhanden wäre.

Wäre das Datenschutzniveau im Empfängerland also niedriger als hierzulande, würde eine Datenübertragung *nicht* durch den § 28 BDSG gedeckt, unabhängig davon, ob sich das Unternehmen auf ein Vertragsverhältnis berufen kann oder nicht.

Allerdings: *Innerhalb der Europäischen Union* ist mit der Umsetzung der EG-Richtlinie in den einzelnen Ländern *immer* ein angemessenes Datenschutzniveau gegeben!

Als Fazit für die Rechtmäßigkeit einer Datenübermittlung *innerhalb* der Europäischen Union kann deshalb Folgendes festgehalten werden: Eine Übermittlung von Beschäftigten-Daten an Unternehmen, die in Staaten innerhalb der EU oder innerhalb des Europäischen Wirtschaftsraums angesiedelt sind, ist nach § 28 BDSG im Rahmen einer *eng ausgelegten* Zweckbestimmung des Arbeitsvertragsverhältnisses *immer* zulässig, da in diesen Staaten ein entsprechendes Datenschutzrecht wie in der Bundesrepublik Deutschland gilt und man somit davon ausgehen kann, dass der Datenschutz gewährleistet ist und dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Übermittlung prinzipiell nicht überwiegt.

Selbstverständlich kommt bei einer entsprechenden Übermittlung von Beschäftigten-Daten zusätzlich das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs. 1 Nr. 6 BetrVG zum Tragen.

Datenübermittlung in Länder außerhalb der EU

Die Datenübermittlung in ein Land außerhalb der Europäischen Union ist – wie gesagt – nur dann zulässig, wenn dieses Land ein angemessenes Datenschutzniveau gewährleistet. Ob nun in dem jeweiligen Land ein angemessenes Datenschutzniveau besteht, kann die Stelle, die Daten übermitteln will, anhand der in § 4 b Abs. 3 BDSG festgelegten Kriterien selber prüfen. Dabei wird

info

Grundsätze für die

Prüfung des angemessenen Datenschutzniveaus

Die ›Artikel-29-Datenschutz-Gruppe‹ (mehr dazu in CF 3/02) hat für die Prüfung des angemessenen Datenschutzniveaus Grundsätze vorgeschlagen, die für Unternehmen, die Daten in ein Drittland übermitteln wollen, wichtige Anhaltspunkte bieten. Diese Grundsätze sind als Mindestanforderungen im Arbeitspapier >WP 4‹ (WP = Working Paper) veröffentlicht worden. Nachfolgend sind die wichtigsten Aspekte für die Prüfung eines angemessenen Datenschutzniveaus aufgelistet:

1. *Grundsatz der Beschränkung der Zweckbestimmung*

Daten sind für einen spezifischen Zweck zu verarbeiten und dementsprechend nur insoweit zu verwenden oder weiter zu übermitteln, als dies mit der Zweckbestimmung der Übermittlung nicht unvereinbar ist.

2. *Der Grundsatz der Datenqualität und -verhältnismäßigkeit*

Daten müssen sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sein. Die Daten müssen angemessen, relevant und im Hinblick auf die Zweckbestimmung, für die sie übertragen oder weiter verarbeitet werden, nicht >ausufernd‹ sein.

3. *Der Grundsatz der Transparenz*

Natürliche Personen müssen Informationen über die Zweckbestimmung der Verarbeitung und die Identität des im Empfängerland für die Verarbeitung Verantwortlichen sowie andere Informationen erhalten, sofern dies aus Billigkeitsgründen erforderlich ist.

4. *Der Grundsatz der Sicherheit*

Der für die Verarbeitung Verantwortliche hat geeignete technische und organisatorische Sicherheitsmaßnahmen für die Risiken der Verarbeitung zu treffen. Alle unter der Verantwortung des für die Verarbeitung Verantwortlichen tätigen Personen, darunter auch Verarbeiter, dürfen Daten nur auf Anweisung des für die Verarbeitung Verantwortlichen verarbeiten.

5. *Die Rechte auf Zugriff, Berichtigung und Widerspruch*

Die betroffene Person muss das Recht haben, eine Kopie aller sie betreffenden Daten erhalten, die verarbeitet werden, sowie das Recht auf Berichtigung dieser Daten, wenn diese sich als unrichtig erweisen. In bestimmten Situationen muss sie auch Widerspruch gegen die Verarbeitung der sie betreffenden Daten einlegen können.

6. *Beschränkung der Weiterübermittlung an andere Länder*

Weitere Übermittlungen personenbezogener Daten vom Bestimmungsland in ein anderes Drittland sind lediglich zulässig, wenn das zweite Drittland (siehe Fußnote 1 auf Seite 24) ebenfalls ein angemessenes Schutzniveau aufweist.

Beispiele weiterer, auf spezifische Arten der Verarbeitung anwendbare Grundsätze:

1. *Sensible Daten*

Sind sensible Kategorien von Daten betroffen (die in Artikel 8 der EG-Datenschutz-Richtlinie aufgelistet sind), so haben zusätzliche Sicherheitsmaßnahmen zu gelten, wie das Erfordernis, dass die betroffene Person ausdrücklich in die Verarbeitung eingewilligt.

2. *Direkt-Marketing*

Werden Daten zum Zwecke des Direkt-Marketings übermittelt, so muss die betroffene Person die Möglichkeit haben, sich jederzeit gegen die Verwendung ihrer Daten für derartige Zwecke zu verwahren.

3. *Automatisierte Einzelentscheidungen*

Erfolgt die Übermittlung mit dem Ziel, eine automatisierte Einzelentscheidung zu treffen, so muss die natürliche Person das Recht haben, die dieser Entscheidung zu Grunde liegende Logik zu erfahren und es müssen andere Maßnahmen getroffen werden, um die berechtigten Interessen der natürlichen Personen zu schützen.

(Etwas gekürzt durch B. Schierbaum)

sie allerdings die Angemessenheit des Datenschutzniveaus unter Berücksichtigung aller Umstände beurteilen müssen, die bei einer Datenübermittlung von Bedeutung sind.

Dafür werden – ohne Anspruch auf Vollständigkeit – im BDSG folgende Beurteilungskriterien genannt:

- die Art der Daten;
- die Dauer der geplanten Verarbeitung;
- das Herkunfts- und das Endbestimmungsland;
- die für die Empfänger geltenden Rechtsnormen sowie
- die für ihn geltenden Standesregeln und Sicherungsmaßnahmen.

Grundsätzlich ist das Schutzniveau in einem Empfängerland immer dann als angemessen anzusehen, wenn der betroffenen Person dort in Bezug auf die Verarbeitung ihrer Daten ein Schutz zuteil wird, der seinem Kern nach den Vorgaben des BDSG (oder der EG-Datenschutz-Richtlinie)…[3] gerecht wird.

Die genannten Kriterien bieten den übermittelnden Unternehmen eine Hilfe, wenn es konkret darum geht, die Angemessenheit des Schutzniveaus zu überprüfen.

Kriterien zur Beurteilung des Datenschutzniveaus

Bei der *›Art der Daten‹* spielen vor allem der Inhalt und auch die Sensibilität (Schutzwürdigkeit) sowie die Möglichkeit der Identifizierung der betroffenen Person eine Rolle.

Bei der *›Dauer der Verarbeitung‹* wird eine kurzzeitige Speicherung anders zu beurteilen sein als eine langfristig geplante Speicherung.

Das *›Herkunfts- und Endbestimmungsland‹* sind die wesentlichen Bezugsgrößen, um die Differenz zwischen den verschiedenen Aspekten des Datenschutzes zu beurteilen, wobei die Vorgabe *›die im Empfängerland geltenden Rechtsnormen‹* dazu verpflichtet, das Datenschutzniveau *generell* zu überprüfen und zu vergleichen.

Geprüft werden muss also, ob es überhaupt vergleichbare Datenschutzgesetze gibt und (in Bezug auf *›geltende Standesregeln‹*) ob es für bestimmte Unternehmen, Branchen, Bereiche oder für bestimmte Formen der Datenverarbeitung (z.B. den Bereich der Telekommunikation) spezielle Regeln gibt.

Von der ›Artikel-29-Datenschutz-Gruppe‹, auf die im zweiten Teil dieses Artikels noch näher eingegangen wird,

3… Zur EG-Datenschutzrichtlinie siehe: ›EG-Datenschutzrichtlinie – die Frist läuft ab!‹ in CF 10/98 ab Seite 24.

sind zusätzlich Mindest-Anforderungen an ein angemessenes Datenschutzniveau formuliert und in einem Arbeitspapier…4 veröffentlicht worden. Wichtige Vorgaben sind im info-Kasten auf Seite 26 zusammengefasst.

Besteht in einem Empfängerland *kein* angemessenes Datenschutzniveau, sieht das BDSG verschiedene Möglichkeiten für eine dennoch mögliche, rechtmäßige Datenübermittlung vor. So gibt es in § 4 c Abs. 1 BDSG einen breit angelegten Ausnahmekatalog. Zudem kann die Aufsichtsbehörde nach § 4 c Abs. 2 BDSG auch im Einzelfall Datenübermittlungen genehmigen. Darüber hinaus kann die EU-Kommission Vorgaben für ein angemessenes Datenschutzniveau entwickeln oder für bestimmte Länder schlicht feststellen, dass ein angemessenes Datenschutzniveau gewährleistet sei (diese Möglichkeiten der EU-Kommission finden sich aber nicht im BDSG, sondern in der EG-Richtlinie).

Ausnahmekatalog nach § 4 c Abs. 1 BDSG

Die Ausnahmen nach § 4 c Abs. 1 BDSG, die eine Datenübermittlung bei *nicht*-angemessenem Datenschutzniveau zulassen, sind fast direkt aus der EG-Datenschutzrichtlinie übernommen. Wobei dieser Ausnahmekatalog vor allem einem Ziel dient: Er soll dem ›freien Datenverkehr‹ Vorrang geben vor dem Datenschutz.

Der Ausnahmekatalog des § 4 c Abs. 1 BDSG soll nachfolgend kurz betrachtet werden, auch wenn er nach Einschätzung des Autors bei Beschäftigten-Daten so nicht zum Tragen kommen dürfte. Denn bei Beschäftigten-Daten wird wohl eine der anderen in diesem zweiteiligen Artikel vorgestellten Varianten für eine Übermittlung Anwendung finden.

Gewährleistet ein Empfängerland *kein* angemessenes Datenschutzniveau, lässt § 4 c BDSG Ausnahmen zu, sofern …

1. der Betroffene seine *Einwilligung* gegeben hat;
2. die Übermittlung für die Erfüllung eines *Vertrags zwischen dem Betroffenen und der verantwortlichen Stelle* oder zur Durchführung von vorvertraglichen Maßnahmen, die auf Veranlassung des Betroffenen getroffen worden sind, erforderlich ist;
3. die Übermittlung zum Abschluss oder zur Erfüllung eines *Vertrags* erforderlich ist, der im Interesse des Betroffenen von der *verantwortlichen Stelle mit einem Dritten* geschlossen wurde oder geschlossen werden soll;
4. die Übermittlung für die *Wahrung lebenswichtiger Interessen* des Betroffenen erforderlich ist oder
5. die *Übermittlung aus einem Register* erfolgt, das zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offen steht, soweit die gesetzlichen Voraussetzungen im Einzelfall gegeben sind.

Für die Datenübertragung in Länder mit schlechterem Datenschutzniveau gibt es eine Fülle von Ausnahmen, die dem ›freien Datenverkehr‹ Vorrang geben vor dem Datenschutz.

Einwilligung

An eine Einwilligung sind die bereits dargestellten Anforderungen geknüpft, wie zum Beispiel die Freiwilligkeit (siehe Seite 24).

Vertrag zwischen Betroffenen und verantwortlicher Stelle

Anwendungsfälle dieser Ausnahme sind zum Beispiel internationale Zahlungsanweisungen, Reisebuchungen und Telefonate mit ›Berührung‹ eines Landes ohne angemessenes Datenschutzniveau.

Kennzeichen dieser Fälle ist es, dass zur Erfüllung eines Vertrags Daten an ein Empfängerland (ohne angemessenes Datenschutzniveau) transferiert werden müssen. Da dieses für den Betroffenen auf der Hand liegt, muss bei dieser Alternative eine gesonderte Einwilligung *nicht* gefordert werden. Die Beteiligung des Betroffenen am Zustandekommen des Vertrags (z. B. eines Kaufvertrags) legitimiert auch die Übertragung der dafür notwendigen Daten.

Vertrag zwischen verantwortlicher Stelle und einem Dritten

Welche Absicht der Gesetzgeber mit dieser Ausnahme verfolgt, ist nur schwer nachzuvollziehen. Anders als bei der vorherigen Ausnahme ist hier nicht die betroffene Person Vertragspartner, wohl aber muss der Vertrag ›in ihrem Interesse‹ liegen. Als sehr abstraktes Beispiel wäre denkbar, dass eine betroffene Person unentgeltlich eine Leistung erhalten soll – etwa wenn im Daten empfangenden Land eine Ware bestellt wird, die von dort unentgeltlich an die Adresse der betroffenen Person geliefert werden soll…5.

Wahrung lebenswichtiger Interessen

Die Datenübermittlung in ein Land mit nicht-angemessenem Datenschutzniveau ist auch dann zulässig, wenn sie für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist. Das BDSG geht davon aus, dass die Wahrung lebenswichtiger Interessen Vorrang vor dem Datenschutz-Interesse hat. Allerdings wird es sich bei der Übermittlung – gerade weil es um lebens-

4… Die Artikel-29-Datenschutz-Gruppe gibt Arbeitspapiere (Working Paper – WP) heraus, die aktuell von WP 1 bis WP 44 über das Internet abgerufen werden können und zwar unter der Adresse: http://europa.eu.int/comm/dg15/de/media/dataprot/wpdocs/index.htm

5… Vergl. Dammann/Simitis: EG-Datenschutzrichtlinie, Art. 26 Anmerkung 7.

wichtige Interessen geht – besonders oft um sensible Daten handeln.

Sensible Daten unterliegen nach dem neuem BDSG normalerweise einem besonderen Schutz, wobei deren Verarbeitung oder Übermittlung immer der Einwilligung bedarf. Hier also die Ausnahme, wobei das BDSG der übermittelnden Stelle einen engen Spielraum vorgibt. Denn von einer Einwilligung in die Übertragung sensibler Daten kann nur abgesehen werden, soweit »dies zum Schutz lebenswichtiger Interessen des Betroffenen oder eines Dritten erforderlich ist, sofern der Betroffene aus physischen oder rechtlichen Gründen außerstande ist, seine Einwilligung zu geben« (§ 28 Abs. 6 Nr. 1 BDSG).

Übermittlung aus einem öffentlichen Register

Die Möglichkeit der Übermittlung aus einem ›öffentlichen Register‹ trägt dem Gedanken Rechnung, dass öffentliche Register einerseits kaum zu schützen sind und dass sie andererseits interessierten Kreisen (auch aus Ländern außerhalb der EU) als verlässliche Informationsquellen zu Verfügung stehen sollen. Öffentliche Register sind beispielsweise Adress-, Telefon- und Branchenbücher, aber auch das Handelsregister oder das Grundbuch.

Zu beachten ist in diesem Zusammenhang jedoch, dass die Übermittlungen aus Registern, zu denen lediglich Personen mit einem ›berechtigten Interesse‹ Zugang haben, nur dann zulässig sind, wenn auch mit dem Datentransfer ein berechtigtes Interesse verfolgt wird. Ein Beispiel hierfür bietet das Fahrzeugregister nach § 31 StVG, dessen Angaben an Privatpersonen nur dann weitergegeben werden dürfen, wenn diese sie zur Verfolgung von Rechtsansprüchen benötigen (§ 39 StVG).

Fazit

Alles in allem besteht die Gefahr, dass durch diese doch sehr weitreichenden Ausnahmeregelungen der Datenschutz bei der Datenübermittlung ins Ausland jedenfalls in Teilbereichen ausgehöhlt wird.

Genehmigung durch die Aufsichtsbehörde

Die Übermittlung personenbezogener Daten in ein Land ohne angemessenes Datenschutzniveau kann nach § 4 c Abs. 2 BDSG schließlich auch durch die Aufsichtsbehörde (z. B. den zuständigen Landesdatenschutzbeauftragten) genehmigt werden und zwar dann, wenn die verantwortliche Stelle ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte vorweist. Diese Garantien können sich insbesondere aus Vertragsklauseln oder verbindlichen Unternehmensregeln ergeben.

Fortsetzung folgt im 2. Teil dieses Artikels in CF 3/02

Bruno Schierbaum, BTQ Niedersachsen, Oldenburg, Telefon 04411-82068, **schierbaum@btq.de**

Literatur zum Thema:

Thomas Barthel: ›Weltweit und (un)kontrollierbar?!‹ in CF 8-9/2000 ab Seite 42

Ulrich Dammann, Spiros Simitis: ›EG-Datenschutzrichtlinie – Kommentar‹, 1997

Wolfgang Däubler: ›Die Übermittlung von Arbeitnehmerdaten ins Ausland‹ in Computer und Recht 1/99 ab Seite 49

Oliver Draf: ›Die Regelung der Übermittlung personenbezogener Daten in Drittländer nach Art. 25, 26 der Datenschutzrichtlinie‹, 1999

Harald Eul, Christoph Godfroid: ›Übermittlung personenbezogener Daten ins Ausland nach Ablauf der Umsetzungsfrist der EG-Datenschutzrichtlinie‹ in Recht der Datenverarbeitung 5/98 ab Seite 185