

Recht und Praxis

Bunte Palette

Zumindest in einem passt alles zusammen: Der unüberschaubaren Vielfalt von Daten schützenden (Daten schützen sollenden) Regelungen steht eine ebensolche Vielfalt praktischer Problemfelder gegenüber. Dass gerade das dafür spricht, Recht und Praxis des Datenschutzes drastisch zu vereinfachen, haben – unter anderem – die bisherigen Artikel dieses Heftes gezeigt.

Im zweiten Abschnitt nun soll es um eine Reihe verschiedener aktueller Einzelfragen gehen. Dazu gehören wichtige und allgemein interessierende Fragen, wie die Problematik des ›grenzüberschreitenden Datenverkehrs‹, ›Biometrie‹ oder ›Datenschutz und Telearbeit‹. Dazu gehören aber auch sehr spezielle und so bisher kaum einmal untersuchte Fragen, wie etwa ›Wenn Arbeitnehmer auch Kunden sind‹ oder ›Datenschutz im Call Center‹. Alles in allem haben wir jedenfalls versucht, die wichtigsten Aspekte unseres Themas (nicht nur, aber vor allem aus Sicht des Arbeitnehmerdatenschutzes) zusammenzutragen.

Wenn hier von ›wir‹ die Rede ist, dann ist damit nicht nur die CF-Redaktion gemeint. Gemeint sind auch und in erster Linie Bruno Schierbaum, Dr. Ulrich Fischer und Dr. Manuel Kiper von der Beratungsstelle für Technologiefolgen und Qualifizierung (BTQ) in Oldenburg. Sie haben nicht nur gleich eine ganze Reihe von Artikeln für dieses Heft verfasst, sie haben die CF-Redaktion auch bei der Gesamtkonzeption in unverzichtbarer Weise unterstützt – dafür herzlichen Dank!

CF-REDAKTION

Grenzüberschreitender Datentransfer

Nicht nur aber vor allem auch für Fragen des Datenschutzes gilt, dass sie sich heute zu Tage wirksam wohl nur international lösen lassen. Dennoch: Auch die Nutzung vorhandener nationaler Regelungen kann einem Missbrauch wirksam den Riegel vorschieben.

DEN SCHUTZ DER Persönlichkeitsrechte bei fortschreitender Globalisierung der Märkte zu gewährleisten, stellt international agierende Unternehmen und Konzerne – im modernen Fachjargon auch ›Global Players‹ genannt – vor große Herausforderungen. Auch für Betriebsräte wird es nicht leichter die Schutzbestimmungen des Bundesdatenschutzgesetzes (BDSG) auf Einhaltung zu kontrollieren und ihre Beteiligungsrechte nach dem Betriebsverfassungsgesetz wahrzunehmen. Denn das BDSG und die Beteiligungsrechte nach dem BetrVG finden an den Grenzen der Bundesrepublik auch *ihre* Grenze – grundsätzlich jedenfalls.

Wenn auch grenzüberschreitender Austausch personenbezogener Daten – von Kunden wie von Beschäftigten – seit Jahren Realität ist, lässt ein weltweit einheitlicher Datenschutzstandard, ein ›globaler Datenschutz‹, noch auf sich warten. Durch die Vorgaben der EG-Datenschutzrichtlinie (siehe CF 10/98 ab Seite 24) jedoch kann eine Entwicklung in Richtung globalem Datenschutz voran getrieben werden. Die DS-Richtlinie enthält in den Artikeln 25 und 26 konkrete Vorgaben für den grenzüberschreitenden Datenverkehr. Bevor darauf jedoch näher eingegangen werden soll, werden die aktuellen Regelungen des

BDSG als zu beachtende Vorgaben bei der Datenverarbeitung und -übermittlung dargestellt:

Vorgaben des Bundesdatenschutzgesetzes

DAS BDSG ENTHÄLT für Privatbetriebe – im BDSG als ›nicht-öffentliche Stellen‹ bezeichnet – keine speziellen Regelungen für den grenzüberschreitenden Datenaustausch.

Grenzüberschreitender Datenaustausch stellt Übermitteln von Daten im Sinne von § 3 Abs. 5 BDSG dar. Dabei ist ›Übermitteln‹ eine von mehreren Phasen der *Verarbeitung* von Daten und ist als »das Bekanntgeben gespeicherter oder durch die Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten (Empfänger)« definiert. Mit dem ›Dritten‹ ist hier jeder außerhalb der speichernden Stelle gemeint (§ 3 Abs. 9 BDSG), so dass ein Unternehmen im Ausland in jedem Fall ›Dritter‹ im Sinne dieser Definition ist.

Auch die Übermittlung personenbezogener Daten unterliegt damit generell einem ›Verbot mit Erlaubnisvorbehalt‹. Das heißt nach § 4 Abs. 1 BDSG: Die Ver-

arbeitung personenbezogener Daten (und damit auch ihre Übermittlung an Dritte) ist nur dann zulässig, wenn:

1. der Betroffene (Beschäftigte) eingewilligt hat oder
2. das BDSG oder
3. eine andere Rechtsvorschrift (das könnte auch eine Betriebsvereinbarung sein) dieses erlaubt oder anordnet.

Will also ein Unternehmen Daten ins Ausland übermitteln, muss *eine* dieser drei Möglichkeiten die rechtliche Basis hierfür bieten. Um es deutlicher zu machen: Wird für den Datentransfer eine Betriebsvereinbarung (als »andere Rechtsvorschrift«) abgeschlossen, muss man sich um die Einwilligung oder die Möglichkeit der Übermittlung auf Basis des BDSG (§ 28 BDSG) nicht mehr weiter kümmern. Nachfolgend sollen deshalb alle drei alternativen Möglichkeiten geprüft werden, inwieweit sie als Grundlage für eine Übermittlung in Betracht kommen.

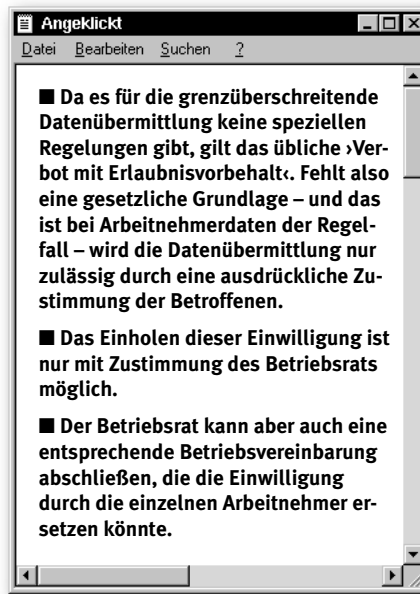
1. Möglichkeit:

Einwilligung des Betroffenen

Will das Unternehmen mit der Möglichkeit der Einwilligung arbeiten, ist gemäß § 4 Abs. 2 BDSG Folgendes zu beachten:

- der Betroffene ist auf den Zweck der Speicherung und einer vorgesehenen Übermittlung sowie auf Verlangen auf die Folgen der Verweigerung der Einwilligung hinzuweisen;
- die Einwilligung bedarf der Schriftform;
- wird die Einwilligungserklärung zusammen mit anderen Erklärungen erteilt, ist sie im äußeren Erscheinungsbild hervorzuheben.

Diese Einwilligung muss *vor der* Übermittlung erfolgen, wobei eine Blanko-einwilligung, die den Umfang der erfassten und verwendeten Daten dem Übermittler überlässt, unwirksam wäre. Zudem muss die Einwilligung freiwillig erfolgen. Ist auch nur eines dieser Kriterien nicht erfüllt, ist eine Einwilligung unwirksam.



Handelt es sich um Beschäftigten-daten, sind diese Voraussetzungen nicht ohne Weiteres durch den Arbeitsvertrag selbst erfüllt. In der Regel wird er nicht ausreichen, da die »Einwilligungserklärung im äußeren Erscheinungsbild der Erklärung« hervorzuheben ist (§ 4 Abs. 2 BDSG). Wenn die Einwilligung den hier genannten Kriterien entspricht, kann der Arbeitgeber damit aber durchaus einen Datentransfer in Ausland legitimieren. Beispiele aus der Praxis für eine entsprechende Einwilligung im Rahmen eines Arbeitsvertrags sind bisher allerdings nicht bekannt.

Zustimmung des Betriebsrats ist nötig

AUSSERDEM GILT: Wenn sich der Arbeitgeber für einen Datentransfer ins Ausland die Einwilligung der Beschäftigten einholen will – in welcher Form auch immer –, könnte er dieses nur mit der Zustimmung des Betriebsrats tun. Die Regelung des § 94 BetrVG zum Einsatz von Personalfragebogen umfasst nämlich auch die Fälle, in denen ein Arbeitnehmer nur nach einer Sache – in diesem Fall wäre das die Zustimmung zur Datenübermittlung – gefragt wird. Der Betriebsrat aber würde in einem solchen Fall seine Zustimmung sicherlich davon abhängig machen, ob der Schutz der Persönlichkeitsrechte gewahrt sein wird. Aber schauen wir noch einmal auf die Details:

2. Möglichkeit: Zulässigkeit der Datenübermittlung nach § 28 BDSG

Der § 28 Abs. 1 BDSG enthält zwei Alternativen für eine Datenübermittlung, die jedoch nicht losgelöst voneinander betrachtet werden können. Demnach ist die Datenübermittlung nur zulässig ...

- im Rahmen der Zweckbestimmung eines Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen;
- soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und
- wenn kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Die Übermittlung personenbezogener Daten (wozu auch die Übermittlung ins Ausland zählt) kann also im Rahmen eines Vertragsverhältnisses prinzipiell zulässig sein (§ 28 Abs. 1 Nr. 1 BDSG).

Beispiel: Wer eine Reise in die Karibik bucht, muss davon ausgehen, dass seine Daten an die Fluggesellschaft, an das Hotel und so weiter übermittelt werden, weil dieses zur Erfüllung des Vertragsverhältnisses erforderlich ist.

Im Arbeitsverhältnis liegen die Dinge jedoch anders, da sich das BDSG (ebenso wie der Arbeitsvertrag) auf jeweils ein einzelnes Unternehmen bezieht. Die Notwendigkeit der Übermittlung von Daten »an Dritte« ergibt sich also nicht »automatisch« aus dem Abschluss eines Arbeitsvertrags (gehört nicht zu seiner »Zweckbestimmung«). Deshalb dürfen auch die Daten von Beschäftigten nicht einmal innerhalb Deutschlands ohne Weiteres an ein anderes Unternehmen etwa des gleichen Konzerns übermittelt werden, viel weniger noch ins Ausland.

Eine Datenübermittlung (grenzüberschreitend oder nicht) kann aber – wie gesagt – auch zulässig sei, »soweit es zur Wahrung berechtigter Interessen der speichernden Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des



Grundsätze:

Was ist ein ›angemessenes Datenschutzniveau‹?

1. Beschränkung auf Zweckbestimmung

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

2. Datenqualität und Verhältnismäßigkeit

Daten müssen sachlich richtig und, wenn nötig, auf dem neuesten Stand sein. Die Daten sollten angemessen, relevant und im Hinblick auf die Zweckbestimmung, für die sie übertragen oder weiterverarbeitet werden, nicht exzessiv sein.

3. Transparenz

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

4. 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 seine Anweisung verarbeiten.

5. Rechte auf Zugriff, Berichtigung und Widerspruch

Die betroffene Person muss das Recht haben, eine Kopie aller sie betreffenden Daten zu 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 in andere Drittländer

Weiterübermittlungen personenbezogener Daten vom Empfänger an Dritte sind nicht zulässig, es sei denn, es werden Mittel gefunden, den betreffenden Dritten vertraglich zu binden und damit den betreffenden Personen die selben Garantien des Datenschutzes zu gewährleisten.

Quelle: Arbeitspapier 12 der Gruppe nach Art. 29 der Datenschutzrichtlinie der EU: Übermittlung personenbezogener Daten an Drittländer; Anwendung von Artikel 25 und 26 Datenschutzrichtlinie der EU (leicht verkürzt durch den Autor B.S.); abgedruckt in: Berliner Datenschutzbeauftragter: Dokumente zum Datenschutz, 1999.

Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt« (§ 28 Abs. 1 Nr. 2 BDSG).

Ein berechtigtes Interesse des Unternehmens an der Übermittlung von Beschäftigtendaten (z.B. zum Zweck einer zentralen Lohn- und Gehaltsabrechnung) wird sich im Regelfall schon aus den wirtschaftlichen Interessen ergeben. Das eigentliche Auslegungsproblem liegt also in der Bewertung des ›schutzwürdigen Interesses‹ des Beschäftigten, das gegen das (wirtschaftliche) Interesse des Unternehmens abgewogen werden muss. Zu den in Frage kommenden ›schutzwürdigen Interessen‹ eines Beschäftigten zählt insbesondere, dass bei der Übermittlung und Verarbeitung sei-

ner personenbezogenen Daten das Grundrecht auf ›informationelle Selbstbestimmung‹ gewährleistet werden muss. Soll also ein Datentransfer in ein Land vorgenommen werden, das im Vergleich zum deutschen Datenschutzrecht ein geringeres Datenschutzniveau (siehe info-Kasten oben) aufweist oder das überhaupt kein Datenschutzgesetz eingeführt hat, muss allein schon wegen der dann schlechter oder ungeschützten Datenverarbeitung in dem ausländischen Unternehmen eine grenzüberschreitende Übermittlung personenbezogener Daten als unzulässig gelten.

3. Möglichkeit: Betriebsvereinbarung als ›andere Rechtsvorschrift‹

Sieht man von der grundsätzlichen Möglichkeit der Einwilligung des Betroffenen ab, scheiden die dargestellten

Möglichkeiten für die Übermittlung von Beschäftigtendaten ins Ausland also aus, so dass als wichtiges Regelungsinstrument der Abschluss einer Betriebsvereinbarung bleibt.

Eine solche Betriebsvereinbarung zum Datenschutz wäre dann eine ›andere Rechtsvorschrift‹ im Sinne des § 4 Abs. 1 BDSG (siehe oben) und könnte damit als Zulässigkeitsvoraussetzung für die Datenübermittlung und -verarbeitung die Zustimmung der einzelnen Arbeitnehmer ersetzen. Beim Abschluss einer Betriebsvereinbarung müssen Arbeitgeber und Betriebsrat allerdings darauf achten, dass die einzelnen Regelungen nicht hinter den Vorgaben des BDSG zurück bleiben. Das Unternehmen wird deshalb mit dem Empfänger der Daten im Ausland eine vertragliche Regelung abschließen müssen, die den Datenempfänger verpflichtet, die Regelungen der Betriebsvereinbarung einzuhalten. So werden der Datenschutz und die Mitbestimmungsrechte des Betriebsrats über die Grenzen der Bundesrepublik ausgeweitet.

Regelungsinhalte sind bekannt

DIE REGELUNGSIHALTE einer solchen Betriebsvereinbarung würden sich dabei nicht grundsätzlich von bekannten und in dieser Zeitschrift auch schon vorgestellten Vereinbarungen zum Arbeitnehmerdatenschutz unterscheiden (z.B. CF 6-7/98 ab Seite 19). Wichtig ist es vor allem, den Rahmen der Datenverarbeitung einzugrenzen, indem eine abschließende Festlegung der eingesetzten Hard- und Software, der personenbezogenen Beschäftigtendaten, der zugriffsberechtigten Personen, der Schnittstellen, Auswertungen und Lösungsfristen erfolgt.

Zusätzlich sollten neben Datenschutz- und Datensicherungsmaßnahmen auch die Rechte der Beschäftigten und Kontrollmöglichkeiten für den Betriebsrat und den betrieblichen Datenschutzbeauftragten entweder in der Betriebs-

vereinbarung, einer Datenschutz-Rahmenvereinbarung oder in dem ergänzenden Vertrag festgelegt werden. Da im Ausland in der Regel bei Datenschutzverletzungen keine Sanktionen vorgesehen sind und es zusätzliche externe Kontrollorgane wie die deutschen Aufsichtsbehörden nicht gibt, sollten auch Strafen bei Vertragsverletzungen vereinbart werden.

EG-Richtlinie und Datentransfer ins Ausland

DER DEUTSCHE GESETZGEBER hätte die EG-Datenschutzrichtlinie (DS-Richtlinie) bis zum 24. 10. 1998 in bundesdeutsches Recht umsetzen müssen. Dieses ist ausgeblieben, wobei ein aktueller Referentenentwurf zum BDSG vorliegt (dieser ist über das Internet abrufbar unter: <http://www.dud.de>).

Eine zentrale Forderung der DS-Richtlinie ist, dass der freie Verkehr auch personenbezogener Daten zwischen den Mitgliedstaaten der EU nicht aus Gründen des Schutzes der Privatsphäre natürlicher Personen beschränkt oder untersagt werden darf (Art. 1 DS-Richtlinie). So wird ein Datentransfer von München nach Paris ebenso zu behandeln sein wie der von München nach Hamburg. Die durch die DS-Richtlinie ausgelösten Angleichungen des Datenschutzrechts in den Mitgliedstaaten der EU sind somit durch die Umsetzung der Vorgaben der DS-Richtlinie als gleichwertig anzusehen.

Beim Datentransfer ins Ausland unterscheidet die DS-Richtlinie allerdings, ob eine Übertragung in einen anderen EU-Mitgliedstaat oder in einen Staat außerhalb der EU erfolgt. Innerhalb der Europäischen Union wird der Datentransfer so zu behandeln sein, als wenn er innerhalb des einzelnen Staates erfolgt. Bei einem Datentransfer in einen Staat außerhalb der Europäischen Union unterscheidet die DS-Richtlinie noch weiter, ob in dem betreffenden Drittland ein

›angemessenes‹ Datenschutzniveau besteht oder nicht. Besteht in dem Drittland unter Berücksichtigung aller Umstände – wie zum Beispiel Art der Daten, geplante Dauer der Verarbeitung, national geltende Datenschutzregelungen – ein angemessenes Schutzniveau, ist die Zulässigkeit des Datentransfers so zu prüfen, als würde eine Übermittlung innerhalb der Bundesrepublik (oder innerhalb der Europäischen Union) erfolgen. Besteht in einem Drittland kein angemessenes Datenschutzniveau, so hat eine Datenübermittlung in diese Länder prinzipiell zu unterbleiben.

Die DS-Richtlinie selbst macht keine Aussagen dazu, was ›angemessenes Schutzniveau‹ konkret bedeutet. Konkrete Ansätze ergeben sich jedoch aus dem Arbeitspapier der nach Art. 29 DS-Richtlinie gebildeten Datenschutzgruppe zum Thema ›Übermittlung personenbezogener Daten an Drittländer: Anwendung von Artikel 25 und 26 der Datenschutzrichtlinie der EU‹. Die aufgestellten Mindestanforderungen (siehe Info-Kasten Seite 38) sollten von den Unternehmen beachtet werden und bei Betriebsvereinbarungen als Regelungen mit einfließen.

Keine Datenschutz-Oasen mehr

›DATEN-OASEN‹ JEDENFALLS – also fast oder gänzlich datenschutzfreie Zonen – dürfte es mit der Umsetzung der DS-Richtlinie durch die Staaten der Europäischen Union innerhalb der europäischen Union, aber auch weltweit nicht mehr geben. Da jedoch die Ausstrahlung der DS-Richtlinie weltweit nicht als realistisch angesehen werden kann, sieht die DS-Richtlinie Ausnahmen vor, wenn Länder außerhalb der Europäischen Union sich mit ihrer Datenschutzgesetzgebung nicht an den Vorgaben der DS-Richtlinie halten.

In der DS-Richtlinie sind zusätzlich Ausnahmen vorgesehen für die Übermittlung in ein Drittland, das kein angemessenes Datenschutzniveau im Sinne der DS-Richtlinie gewährleistet. So kann

eine Übermittlung unter anderem auch dann vorgenommen werden, wenn die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat oder wenn die Übermittlung zur Erfüllung eines Vertrags erforderlich ist. Auch mit der Umsetzung der DS-Richtlinie wird das Regelungsinstrument der Betriebsvereinbarung seine Bedeutung für die Übermittlung von Arbeitnehmerdaten also beibehalten, unterstützt dadurch, dass in Erwägungsgrund 9 zur DS-Richtlinie der Handlungsspielraum der Wirtschafts- und Sozialpartner – also unter anderem von Arbeitgeber und Betriebsrat – hervorgehoben wird.

Bruno Schierbaum,
BTQ Niedersachsen, Donnerschweer Str. 84,
26123 Oldenburg, Telefon 04 41 / 8 20 68,
eMail: schierbaum@btq.de



Weiterführende Literatur:

Harald Eul, Christoph Godefroid: Übermittlung personenbezogener Daten ins Ausland nach Ablauf der Umsetzungsfrist der EG-Datenschutzrichtlinie; in: *Recht der Datenverarbeitung*, Heft 5/1998 ab Seite 185.

Wolfgang Däubler: Grenzüberschreitender Datenschutz – Handlungsmöglichkeiten des Betriebsrats; in: *Recht der Datenverarbeitung*, Heft 3/1998 ab Seite 96.

Wolfgang Däubler: Die Übermittlung von Arbeitnehmerdaten ins Ausland; in: *Computer und Recht*, Heft 1/1999 ab Seite 49.

Bruno Schierbaum: EG-Datenschutzrichtlinie – die Frist läuft ab; in: *CF 10/1998* ab Seite 24.

Peter Wedde: Multidatenschutz per Betriebsvereinbarung; in: *Die Mitbestimmung*, Heft 12/1996 ab Seite 35.