Gutachtliche Stellungnahme

zum

Entwurf

„Betriebsvereinbarung Datenschutz“

für die D. Europe GmbH

von

Prof. Dr. Wolfgang Däubler, Bremen

I. Allgemeine Vorbemerkungen

Die Betriebsvereinbarung hat den Sinn, den Datenschutz der Beschäftigten sicherzustellen und gleichzeitig die Reibungslosigkeit der Arbeitsabläufe nicht zu beeinträchtigen. Beides kommt zugleich den Geschäftspartnern, insbesondere auch den Kunden zugute, die darauf vertrauen können, dass ihre Daten nicht in falsche Hände geraten.

Dies könnte man in einer Präambel zum Ausdruck bringen, die etwa lauten könnte:

„Die folgende Betriebsvereinbarung verfolgt das Ziel, den Datenschutz der Beschäftigten zu gewährleisten und zugleich zur Reibungslosigkeit der Arbeitsabläufe beizutragen. Sie soll eine Atmosphäre der vertrauensvollen Kooperation schaffen, was zugleich auch den Geschäftspartnern zugutekommt."

II. Einzelbestimmungen des Entwurfs

1. Vorgeschlagen ist folgende Formulierung:

„ 1. Geltungsbereich
Diese Betriebsvereinbarung ist für alle Mitarbeiter der D. Europe GmbH gültig. Sie tritt ab dem 01. 03. 2011 in Kraft."

Der Betriebsrat kann nur für die in § 5 Abs.1 BetrVG genannten Arbeitnehmer sprechen. Für leitende Angestellte besitzt er kein Mandat. Dies bringt man üblicherweise in der Weise zum Ausdruck, dass man formuliert:

„Diese Betriebsvereinbarung gilt für alle Mitarbeiter der D. Europe GmbH, die von § 5 Abs.1 BetrVG erfasst werden."

Wenn man dies wünscht, kann man die leitenden Angestellten in Form eines Vertrags zugunsten Dritter begünstigen, indem man etwa formuliert:

„Der Arbeitgeber verpflichtet sich, die Inhalte dieser Betriebsvereinbarung durch entsprechende Gestaltung der Arbeitsverträge auch gegenüber leitenden Angestellten verbindlich zu machen."

Der Zeitpunkt des Inkrafttretens wird in der Regel am Ende einer Betriebsvereinbarung zusammen mit den Kündigungsmöglichkeiten geregelt. Für den Leser hat dies den Sinn, dass er unschwer erkennen kann, welches Gesamtwerk wann beginnt und wann ausläuft. Auch hier sollte so verfahren werden, obwohl es natürlich keinen absolut zwingenden Grund für eine solche Gliederung gibt.

2. Vorgeschlagen wird weiter:

„2. Definitionen
Personenbezogene Daten: Sämtliche personenbezogenen Daten über einzelne Mitarbeiter oder Datenzusammenfassungen, aus denen personenbezogene Daten abgeleitet werden können.
Private Daten: Unter privaten Daten werden sämtliche Daten verstanden, die nicht in einem direkten Zusammenhang mit dem Dienstverhältnis stehen.
Dienstliche Daten: Sämtliche Daten, die der Mitarbeiter der DE-STA-CO Europe GmbH gegenüber schriftlich oder mündlich erklärt, und alle Daten, die in der Personalakte vermerkt sind."

Viele Betriebsvereinbarungen kommen ohne solche Definitionen aus, was dazu führt, dass die Begrifflichkeiten des BDSG Anwendung finden. Die Zuordnung zum privaten und zum dienstlichen Bereich ist dort zwar nicht geregelt, erweist sich jedoch meist als unproblematisch. In Einzelfällen können sich gleichwohl Zweifel ergeben. So ist beispielsweise ein Anruf zu Hause, man komme heute später, da man Überstunden machen müsse, einerseits privat, andererseits aber dienstlich veranlasst. Was die Nutzung des Telefons angeht, werden in solchen Fällen üblicherweise dieselben Grundsätze wie bei einem Dienstgespräch angewandt. Eine Definition hat überdies den Nachteil, dass sie nicht mehr Klarheit bringt; wann lässt sich ein „unmittelbarer", wann ein nur mittelbarer Zusammenhang mit dem Arbeitsverhältnis feststellen? In erster Linie wird daher vorgeschlagen, keine Regelung zu treffen oder auf das BDSG zu verweisen („Die hier verwendeten Begriffe entsprechen denen des BDSG").

Legen die Betriebsparteien gleichwohl Wert auf eigene Definitionen, so könnte man wie folgt formulieren:

„Personenbezogene Daten: Sämtliche Daten, die sich auf einen Mitarbeiter/eine Mitarbeiterin beziehen oder die auf einen Mitarbeiter/eine Mitarbeiterin bezogen werden können."

Die personenbeziehbaren Daten erfassen auch die „Datenzusammenfassungen" (etwa Daten über Gruppen von Beschäftigten), aus denen personenbezogene Daten einzelner Mitarbeiter abgeleitet werden können.

„Private Daten: Personenbezogene Daten, die nicht in einem direkten Zusammenhang mit dem Arbeitsverhältnis stehen (z. B. Freizeitaktivitäten)."

Man kann an die als erstes definierten personenbezogenen Daten anknüpfen und trotz aller Unschärfe einen „direkten" Zusammenhang mit dem Arbeitsverhältnis verlangen. Der Begriff „Dienstverhältnis" wird üblicherweise nur im Beamtenrecht gebraucht.

„Dienstliche Daten: Personenbezogene Daten, die in einem unmittelbaren Zusammenhang mit dem Arbeitsverhältnis stehen (z. B. Daten aus der Zeiterfassung oder der Lohnabrechnung)"

Auf die Erklärung gegenüber dem Arbeitgeber und auf die Einbeziehung in die Personalakte abzustellen, ist demgegenüber zu eng. Kommens- und Gehenszeiten würden beispielsweise nicht erfasst, obwohl sie unzweifelhaft mit dem Arbeitsverhältnis engstens verbunden sind.

3. Weiter wird vorgeschlagen:

„**3. Verpflichtung auf das Datengeheimnis**
Soweit Mitarbeiter im Rahmen ihrer beruflichen Tätigkeit auch nur gelegentlich mit der Bearbeitung von geschützten Daten zu tun haben, kann D Europe GmbH verlangen, dass sie sich ausdrücklich schriftlich gemäß den gesetzlichen Bestimmungen auf das

Datengeheimnis verpflichten. Diese Verpflichtung erstreckt sich auch auf die Zeit nach Beendigung der datenverarbeitenden Tätigkeit oder die Zeit nach dem Ausscheiden aus dem Unternehmen."

Der Begriff „geschützte Daten" ist nicht erläutert; es dürfte sich um alle personenbezogenen Daten im Sinne des BDSG bzw. der Definition unter 2. handeln. Bezieht man auch den Fall ein, dass ein Mitarbeiter nur „gelegentlich" mit solchen Daten zu tun hat, so muss man bei realistischer Betrachtung alle Mitarbeiter auf das Datengeheimnis verpflichten. Dies geht etwas zu weit. Sinnvoll wäre es, einfach zu formulieren:

„Die Verpflichtung auf das Datengeheimnis richtet sich nach § 5 BDSG. Dabei ist die Schriftform zu wahren."

Damit ist die gesetzliche Regelung übernommen; sie hat bisher zu keinen Unzuträglichkeiten geführt. Die Schriftform dient der Rechtssicherheit und entspricht einer verbreiteten Praxis.

4. Weiter wird vorgeschlagen:

„4. Meldepflicht für Datenschutzmängel
Es liegt im Interesse der D. Europe GmbH und ihrer Mitarbeiter, dass Mängel im Datenschutz, in der Datensicherung sowie der Ordnungsmäßigkeit und erkennbarer Verstöße gegen das Datengeheimnis unverzüglich dem zuständigen Vorgesetzten oder dem Datenschutzbeauftragten zur Kenntnis gebracht werden."

Die Vorschrift ist nicht ganz eindeutig, da die Überschrift *für* eine Verpflichtung, der Wortlaut jedoch *dagegen* spricht, dass der einzelne Arbeitnehmer zu einer Anzeige verpflichtet sein soll. Entsprechende „Hinweispflichten" haben im Zusammenhang mit Ethik-Kodizes eine große Rolle gespielt, wobei häufig der Vorwurf einer Pflicht zur Denunziation erhoben wurde.

Grundlegend in der Rechtsprechung BAG Beschl. v. 22. Juli 2008 – 1 ABR 40/07 – NZA 2008, 1248. Aus der Literatur s. Dzida NZA 2008, 1265; Deinert/Kolle AuR 2006, 177; Däubler, dbr 9/2005 S. 25

Dies sollte man nach Möglichkeit vermeiden. Auf der anderen Seite sind natürlich alle Beteiligten daran interessiert, dass Mängel rechtzeitig aufgedeckt und behoben werden. Beides könnte dafür sprechen, lediglich den betrieblichen Datenschutzbeauftragten einzuschalten, wobei er ggf. dem Anzeigeerstatter Vertraulichkeit zusichern kann.

Seit September 2009 gilt außerdem die Vorschrift des § 42a BDSG, die bei „Datenpannen" bestimmte Maßnahmen einschließlich einer Information der Betroffenen vorsieht. Dies sollte nicht unerwähnt bleiben.

Auf dieser Grundlage könnte man sich folgende Formulierung vorstellen:

„4. Meldung von Datenschutzmängeln
Wird gegen Regeln des Datenschutzes oder der Datensicherung verstoßen, so sollte unverzüglich der betriebliche Datenschutzbeauftragte informiert werden. Dieser ergreift die erforderlichen Schritte, um für Abhilfe zu sorgen; dem Informanten kann er Vertraulichkeit zusagen. § 42a BDSG bleibt unberührt."

5. Als nächstes wird vorgeschlagen:

„**5. Datenschutzbeauftragter**
Bestellung und Abberufung eines Datenschutzbeauftragten bedürfen der vorherigen Unterrichtung des Betriebsrats. Der betriebliche Datenschutzbeauftragte ist verpflichtet und ermächtigt, dem Betriebsrat alle Informationen zugänglich zu machen, welche dieser benötigt, um seine Aufgabe nach dieser Betriebsvereinbarung wahrzunehmen."

Was die Bestellung des betrieblichen Datenschutzbeauftragten betrifft, so besitzt der Betriebsrat in vielen Fällen ein Zustimmungsverweigerungsrecht nach § 99 BetrVG. Auch steht es den Betriebsparteien nach der Rechtsprechung frei, insoweit ein Mitbestimmungsrecht des Betriebsrats einzuführen.

LAG Düsseldorf RDV 1989, 34. Ebenso in der Literatur Tinnefeld/Ehmann/Gerling, Einführung in das Datenschutzrecht, 4. Aufl. 2005, S. 453; Simitis in: Simitis (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 6. Aufl. 2006, § 4f Rn 68; Däubler, Gläserne Belegschaften? Datenschutz in Betrieb und Dienststelle, 5. Aufl. 2010, Rn 597

Eine Verpflichtung in dieser Richtung besteht allerdings nicht.

Die vorliegende Betriebsvereinbarung müsste zumindest auf § 99 BetrVG verweisen, da sie sonst als Regelung interpretiert werden könnte, die vom BetrVG zu Lasten des Betriebsrats abweicht (was sicherlich nicht dem Willen der Beteiligten entspricht und auch keine Wirksamkeit entfalten könnte).

Nach Satz 1 wäre daher einzufügen:

„§ 99 BetrVG und andere gesetzliche Rechte des Betriebsrats bleiben unberührt."

Gegen den (bisherigen) zweiten Satz bestehen für den Regelfall im Ergebnis keine Bedenken. Soweit es sich bei dem betrieblichen Datenschutzbeauftragten um einen Arbeitnehmer des Betriebes handelt, können seine gesetzlichen Pflichten durch Betriebsvereinbarung konkretisiert werden. Soweit es sich allerdings um einen Externen handelt, wäre eine solche Regelung problematisch, weil der Betriebsrat ihm gegenüber nicht zum (Mit-)Erlass verbindlicher Regeln berechtigt ist. Im Folgenden wird daher unterstellt, dass es einen „internen" betrieblichen Datenschutzbeauftragten gibt.

III. Datenübermittlung an andere Unternehmen im In- und Ausland, insbesondere an die Konzernspitze

1. Der Vorschlag

„6. Ausnahmen bei konzerninterner Datenübermittlung
Personenbezogene Daten dürfen nur zu dienstlichen Zwecken weitergegeben werden. Dieses schließt Mitarbeiter der Dover Corporation, 3005 Highland Parkway, Downers Grove, IL 60515 und D Industries, 1025 Doris Road, Auburn Hills, Michigan 48326 ein.

Die Dover Corporation und D Industries haben verbindliche Unternehmensrichtlinien geschaffen, welche die internationale Weitergabe von personenbezogenen Daten innerhalb des Konzerns regeln und die Datenschutzgrundsätze für den Umgang mit personenbezogenen Daten festlegen. Der in den Unternehmensrichtlinien geregelte Datenschutz entspricht im Wesentlichen den Kernprinzipien der Europäischen Datenschutzrichtlinie. Dover Corporation hat zusätzlich die Safe-Harbor-Zertifizierung beantragt. Vor diesem Hintergrund wird für den Datentransfer in die USA zu Mitarbeitern der Konzernunternehmen Dover Corporation und D Industries folgendes vereinbart:

Werden aus den USA von Dover Corporation oder D Industries personenbezogene Daten angefordert, so können diese an folgende Personen weitergegeben werden:

- President,
- Vice President Finance,
- Vice President Human Resources
- oder eine von diesen beauftragte und/oder bevollmächtigte Person.

Personenbezogene Daten sind bei der Datenübermittlung soweit als möglich als gesicherter Dateianhang zu versenden. Der Anhang ist mit einem Passwort zu versehen."

In unmittelbarem inhaltlichem Zusammenhang damit steht die Vorschrift nach Ziff. 7, die die Weitergabe von Daten regelt. Sie soll bestimmen:

„**7. Genehmigung**
Die Genehmigung zur Weitergabe personenbezogener Daten erfolgt bei privaten Daten ausschließlich über den Mitarbeiter. Die Genehmigung zur Weitergabe personenbezogener Daten kann bei dienstlichen Daten vom Personalleiter oder der Geschäftsführung erfolgen."

2. Reihenfolge der Regelung

Es liegt nahe, zunächst die in Nr. 7 enthaltenen allgemeinen Regeln zur Übermittlung von Arbeitnehmerdaten anzusprechen, die alle Drittunternehmen gelten. Dabei ist zwischen dem Inland bzw. dem EU-Gebiet und Drittstaaten zu unterscheiden. Für die konzernweite Praxis besonders bedeutsam ist die Übermittlung in die USA, die einige Sonderprobleme aufweist.

3. Übermittlung an andere Unternehmen im Inland und innerhalb der EU

Die Übermittlung von personenbezogenen Daten von Arbeitnehmern an ein anderes Unternehmen muss nach § 32 Abs.1 Satz 1 BDSG für die Begründung, die Durchführung oder die Beendigung des Arbeitsverhältnisses erforderlich sein. Dies gilt nach § 4b Abs.1 BDSG in gleicher Weise, wenn der Datenempfänger in der EU ansässig ist. Juristisch spielt es dabei keine Rolle, ob das Unternehmen dem Konzern angehört oder ob es ein außenstehendes Unternehmen ist. Bei ersterem wird lediglich häufiger der Fall eintreten, dass Daten übermittelt werden und dass hierfür eine Rechtsgrundlage erforderlich ist.

Was im Einzelfall für die Durchführung des Arbeitsverhältnisses „erforderlich“ ist, lässt sich nicht im Einzelnen vorausbestimmen. Dass es sich dabei nur um „dienstliche“ Daten handeln wird, liegt auf der Hand. Der Entwurf beschränkt sich verständlicherweise darauf, nur die Kompetenz für die Übermittlung zu regeln und den Personalleiter und die Geschäftsführung für zuständig zu erklären. Ob sich diese von anderen Personen vertreten lassen können, ist anders als im dritten Abschnitt von Ziff. 6 nicht angesprochen. In der Praxis dürfte es kaum durchführbar sein, allein die konkreten Personen des Personalleiters bzw. der Geschäftsführer zu einer Übermittlung zu ermächtigen. Wird beispielsweise im Wege der Funktionsübertragung die Lohnabrechnung an eine Drittfirma vergeben, so müssen auch Mitarbeiter der Personalabteilung befugt sein, der Drittfirma die nötigen Informationen zukommen zu lassen.

Die Vorschrift des § 32 Abs.1 Satz 1 BDSG gilt selbstredend auch im vorliegenden Fall, doch wäre es der Übersichtlichkeit wegen wünschenswert, dies auch in der Betriebsvereinbarung zum Ausdruck zu bringen. Andernfalls besteht die Gefahr, dass irrtümlich davon ausgegangen wird, „grünes Licht“ durch die zuständigen Personen genüge für eine Übermittlung an Drittunternehmen. Als Formulierung käme in Betracht:

„6. Datenübermittlung an andere Unternehmen

Personenbezogene Daten von Mitarbeitern dürfen an andere Unternehmen nur übermittelt werden, wenn dies zur Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist. Eine Übermittlung ist nur durch den Personalleiter oder einen Geschäftsführer möglich. Sie können dieses Recht auf nachgeordnete Personen delegieren."

Was private Daten betrifft, so stehen sie außerhalb des Arbeitsverhältnisses; eine Weitergabe an andere Unternehmen kommt daher im Regelfall nicht in Betracht. Es gelten die allgemeinen Grundsätze des BDSG. Beispielsweise können Arbeitnehmer Kunden sein und in dieser Eigenschaft Einkäufe tätigen, die über ein anderes Konzernunternehmen abgewickelt werden. Eine Regelung hierzu ist überflüssig. Wenn sie gleichwohl gewünscht wird, müsste man formulieren:

„Private Daten von Arbeitnehmern unterliegen den allgemeinen Regeln des BDSG. Eine Übermittlung an Dritte ist nur auf der Grundlage besonderer Verträge oder einer Einwilligung des Arbeitnehmers zulässig. Die Einwilligung muss freiwillig erteilt sein. Ihre Verweigerung darf keine Benachteiligung im Arbeitsverhältnis möglich erscheinen lassen."

Eine reale Freiwilligkeit soll dadurch sichergestellt sein, dass schon die (abstrakte) Möglichkeit einer Benachteiligung im Arbeitsverhältnis die Freiwilligkeit ausschließt.

4. Übermittlung an Unternehmen in Drittstaaten

Aus den vorliegenden Papieren wird nicht deutlich, dass eine Übermittlung an Unternehmen in Drittstaaten außerhalb der USA von wesentlicher praktischer Bedeutung wäre. Gleichwohl kann sie nicht ausgeschlossen werden. Entsprechende Vorgänge können sich durch geschäftliche Kontakte ergeben, deren Abwicklung auch die Mitteilung von Arbeitnehmerdaten verlangt. Zum zweiten ist es aber auch denkbar, dass Aufgaben der Personalverwaltung, insbesondere der Personalabrechnung aus Gründen der Kostenersparnis in ein Drittland wie z. B. Indien ausgelagert werden. Insoweit müsste ggf. eine Regelung aufgenommen werden. Grundlage ist die gesetzliche Regelung.

Nach § 4b Abs.2 Satz 2 BDSG muss die Übermittlung unterbleiben, „soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn… ein angemessenes Datenschutzniveau nicht gewährleistet ist." Die „Angemessenheit" beurteilt sich nach § 4b Abs.3 BDSG unter Berücksichtigung aller Umstände, die bei einer Datenübermittlung oder einer Kategorie von Datenübermittlungen von Bedeutung sind. Dabei können „insbesondere die Art der Daten, die Zweckbestimmung, die Dauer der geplanten Verarbeitung, das Herkunfts- und das Endbestimmungsland, die für den betreffenden Empfänger geltenden Rechtsnormen sowie die für ihn geltenden Standesregeln und Sicherheitsmaßnahmen herangezogen werden." Ist ein angemessenes Niveau gegeben, werden Empfänger in dem fraglichen Land wie Empfänger in der EU behandelt.

Die Beurteilung, ob in einem anderen Land ein angemessenes Niveau besteht, ist an sich nach Abs.5 Sache der übermittelnden Stelle. Angesichts der genannten Kriterien würde dies meist auf eine Überforderung hinauslaufen. Obwohl das BDSG keinen entsprechenden Hinweis enthält, orientiert man sich deshalb an Feststellungen der EU-Kommission, die auf der Grundlage von Art. 31 Abs.2 der EG-Datenschutzrichtlinie das Datenschutzniveau bestimmter Länder als „angemessen" bezeichnet. Dies gilt etwa für Argentinien (ABlEG v. 5. 7. 2003, Nr. L 168/19), Kanada (ABlEG v. 4. 1. 2000, Nr. L 215/1), die Schweiz (ABlEG 25. 8. 2000, Nr. L 215/1) sowie die Inseln Guernsey (ABlEG v. 25. 11. 2003, Nr. L 308/27) und Isle of Man (ABlEG v. 30. 4. 2004, Nr. 151/51, berichtigt in ABlEG v. 10. 6. 2004, Nr. L 208/47).
Der jeweilige aktuelle Stand ist über das Internet abrufbar (www.europa.eu.int/comm/justice_home/fsj/privacy/thirdcountries/index_de.htm).

Ist im Einzelfall *kein angemessenes Datenschutzniveau* gewährleistet, ist eine *Übermittlung* personenbezogener Daten *keineswegs generell ausgeschlossen*. Vielmehr sieht § 4c BDSG eine Reihe von Voraussetzungen vor, unter denen gleichwohl eine Übermittlung stattfinden kann. Der wichtigste Fall ist in § 4c Abs.2 Satz 1 BDSG genannt, wonach die Aufsichtsbehörde die Übermittlung genehmigen kann, wenn durch privatautonome Vereinbarungen ausreichende Garantien hinsichtlich des Schutzes des Persönlichkeitsrechts und der Ausübung der damit verbundenen Rechte geschaffen sind.

In der Praxis orientiert man sich an Standardvertragsklauseln der EU-Kommission, die als „ausreichend“ betrachtet werden und die die Genehmigung zur Formalie werden oder ganz entfallen lassen. Dabei muss man zwischen den Standardvertragsklauseln für die Übermittlung (Entscheidung der Kommission vom 15. 6. 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten in Drittländer nach der Richtlinie 95/46/EG, ABlEG v. 4. 7. 2001, Nr. L 181/19) und solchen für die Auftragsdatenverarbeitung unterscheiden, die in solchen Fällen eine „Übermittlung“ im Rechtssinne darstellt (Entscheidung der Kommission v. 27. 12. 2001 hinsichtlich Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Auftragsverarbeiter in Drittländern nach der Richtlinie 95/46/EG, ABlEG v. 10. 1. 2002, Nr. L 6/52). Für die eigentliche Übermittlung gibt es einen weiteren Standardvertrag aus dem Jahre 2004, der jedoch nach Auffassung der Aufsichtsbehörden für Arbeitnehmerdaten nicht geeignet ist, da die im Mustervertrag von 2001 enthaltenen Individualrechte der Betroffenen auf Auskunft, Berichtigung, Löschung und Schadensersatz nicht enthalten sind (dazu Schmidl DuD 2008, 258 ff.).

Bei multinationalen Konzernen und bei kooperierenden Unternehmen steht ein zweiter Weg zur Verfügung, um den notwendigen Persönlichkeitsschutz sicherzustellen. An die Stelle eines Vertrages treten hier „verbindliche Unternehmensregelungen“, die einen vergleichbaren Schutz sicherstellen. Allerdings existiert kein „Musterkodex“ analog den Standardvertragsklauseln, so dass die staatliche Genehmigung weiterhin erforderlich bleibt.

Ebenso Achim Büllesbach, Transnationalität und Datenschutz. Die Verbindlichkeit von Unternehmensregelungen, 2008, S. 176 ff.; Räther DuD 2005, 462, 464; ähnlich Scheja, Datenschutzrechtliche Zulässigkeit einer weltweiten Kundendatenbank, 2006, S. 261 ff.

Im Rahmen einer Betriebsvereinbarung, die den Arbeitnehmerdatenschutz auch im Verhältnis zu ausländischen Unternehmen regelt, kann man bewusst auf die gesetzliche Regelung verweisen. Dies hat allerdings den Nachteil, dass der Betriebsrat seine Informations- und Kontrollrechte nicht den ausländischen Unternehmen (Datenempfänger, Auftragnehmer) gegenüber ausüben kann, da die Standardvertragsklauseln lediglich Rechte für den Betroffenen, nicht aber solche des Betriebsrats ansprechen. Im Rahmen des Mitbestimmungsverfahrens kann aber sehr wohl

über die Standardverträge hinaus vereinbart werden, dass sich der Betriebsrat in gleicher Weise wie ein Betroffener an die ausländische Stelle mit der Bitte um Auskunft wenden kann. Dies lässt sich unschwer mit der Erwägung rechtfertigen, dass die Einschaltung Dritter nicht zu einer Verschlechterung seiner Position führen darf: Auch wenn diese einbezogen sind, muss es ihm möglich sein, die Einhaltung datenschutzrechtlicher Bestimmungen zu überwachen, soweit die von ihm vertretenen Arbeitnehmer betroffen sind.

Man könnte daher den Grundsatz formulieren:

„Personenbezogene Daten von Arbeitnehmern können im Rahmen der allgemeinen Voraussetzungen an ausländische Unternehmen übermittelt werden, wenn diese in einem Mitgliedstaat der EU oder des Europäischen Wirtschaftsraums belegen sind. Gleichgestellt sind Unternehmen aus Ländern, die nach den Erklärungen der EU-Kommission ein angemessenes Datenschutzniveau besitzen.

Sollen Daten in Länder ohne angemessenes Datenschutzniveau übermittelt werden, so ist die Genehmigung der Aufsichtsbehörde einzuholen oder ein von der EU-Kommission und den Aufsichtsbehörden empfohlener Standardvertrag zugrunde zu legen. Soweit danach einzelne Betroffene Rechte gegenüber dem Datenempfänger haben, gilt dies auch für den Betriebsrat. Diesem steht insbesondere das Recht zu, die Einhaltung des Datenschutzrechts einschließlich der zu seiner Realisierung geschlossenen Verträge zu überwachen und die dafür erforderlichen Informationen vom Datenempfänger zu erhalten.“

5. Übermittlung in die USA

a) Safe Harbor Grundsätze

In vielen Bereichen, etwa auch im Arbeitsrecht, weisen die USA kein Datenschutzniveau auf, das man nach europäischen Maßstäben als angemessen ansehen kann.

S. etwa Buchner, Informationelle Selbstbestimmung im Privatrecht, 2006, S. 7 ff.; Wilske CR 1993, 297 ff.; Däubler CR 1999, 53

Um den Datenverkehr nicht unnötig zu belasten, ist zwischen der EU-Kommission und dem US-Handelsministerium eine Abmachung getroffen worden. Danach sind Unternehmen aus den USA dann taugliche Datenempfänger, wenn sie sich den Grundsätzen über den sicheren Hafen (safe harbor principles) angeschlossen haben, deren Einhaltung von der Federal Trade Commission auf Beschwerde hin kontrolliert wird.

Einzelheiten bei Klug RDV 2000, 212; Weniger, Grenzüberschreitende Datenübermittlungen international tätiger Unternehmen, 2005, S. 425 ff.

Unternehmen, die nicht von der Federal Trade Commission überprüft werden können, kommen für die Safe-Harbor-Grundsätze nicht in Betracht.

Schließt sich ein US-Unternehmen diesen Prinzipien an, so ist zu fragen, auf welche konzernangehörigen Unternehmen sich dies bezieht und welche Art von Daten erfasst ist.

So Regierungspräsidium Darmstadt, Tätigkeitsbericht 2007, RDV 2009, 42

Nach Auffassung der EU-Kommission sichern die Safe-Harbor-Grundsätze ein „angemessenes Datenschutzniveau“, so dass die Übermittlung von Arbeitnehmerdaten auch ohne staatliche Genehmigung zulässig ist. Damit ist allerdings lediglich das Hindernis aus dem Weg geräumt, dass in den USA nicht generell ein „angemessenes“ Datenschutzniveau besteht. Die übrigen Voraussetzungen für die Datenübermittlung, wie sie auch im Inland oder gegenüber Unternehmen aus anderen EU-Mitgliedstaaten erfüllt sein müssen, bleiben jedoch bestehen. Aus diesem Grund bedürfen die Formulierungen in Ziff. 6 einiger Klarstellungen.

b) Zwecke der Übermittlung

Die Übermittlung von Arbeitnehmerdaten an die Konzernunternehmen in den USA bedarf einer Rechtsgrundlage, die auch in einer Betriebsvereinbarung liegen kann. Dies ist für die konzerninterne Übermittlung mittlerweile weithin anerkannt,

Dazu Däubler, Gläserne Belegschaften? Rn 453 im Anschluss an BAG DB 1996, 1985

kann jedoch auch im vorliegenden Zusammenhang gelten. Die hier getroffene Regelung ist daher zugleich die maßgebende Rechtsgrundlage für die Übermittlung. Dabei darf die Betriebsvereinbarung jedoch nicht in übermäßigem Umfang in das informationelle Selbstbestimmungsrecht eingreifen und muss deshalb die Zwecke bestimmen, denen die Übermittlung dienen soll.

Ziff. 6 des vorliegenden Entwurfs ordnet in seinem Eingangssatz an, dass personenbezogene Daten nur zu „dienstlichen Zwecken“ weitergegeben werden dürfen. Dies wäre als solches viel zu pauschal; dienstlichen Zwecken würde beispielsweise auch ein (von niemandem beabsichtigtes) System totaler Überwachung unter Einsatz neuester Technik dienen. Die Dover Corporation Datenschutz-Richtlinien, auf die im zweiten Absatz von Ziff. 6 verwiesen wird, enthalten deshalb mit Recht in Nr. 4 sehr viel konkretere Zwecke. Diese ermöglichen allerdings eine weitgehende Überwachung der in Deutschland tätigen Mitarbeiter, was in den Begriffen „Leistungs- und Fortbildungsmanagement“ und „Verarbeitung und Überprüfung von Berichten im Rahmen des Dover Compliance-Programms“ zum Ausdruck kommt. Ob man dies im Grundsatz akzeptieren oder die Verweisung in der Betriebsvereinbarung insoweit einschränken will, ist eine betriebspolitisch zu entscheidende Frage.

c) Mitbestimmung des Betriebsrats

Wenn nur eine Übernahme der Richtlinien in Betracht kommt, sollte man jedenfalls dafür sorgen, dass das Mitbestimmungsrecht des Betriebsrats bei Leistungs- und Verhaltenskontrollen nach § 87 Abs.1 Nr. 6 BetrVG gewahrt bleibt: Dieses greift auch dann Platz, wenn die Auswertung der Mitarbeiterdaten im Ausland erfolgt. Insoweit kann nichts anderes gelten als bei Befragungen von in Deutschland tätigen Beschäftigten, die von der ausländischen Konzernspitze direkt mit Hilfe von E-Mails durchgeführt werden.

Zu diesem Fall HessLAG 5. 7. 2001, AuR 2002, 33 und U. Fischer AuR 2002, 7

Es würde sich daher empfehlen, dies im Text der Betriebsvereinbarung zu verdeutlichen und etwa zu formulieren:

„Das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs.1 Nr. 6 BetrVG bleibt auch dann unberührt, wenn Datenverarbeitungen, die geeignet sind, Verhalten und Leistung der Arbeitnehmer zu überwachen, ganz oder teilweise im Ausland erfolgen."

d) Zugriffsberechtigungen

Datenschutzrechtlich ergibt sich weiter das Problem, dass Nr. 4 der Richtlinien die Zugriffsberechtigung auf Mitarbeiter der Personal- und der IT-Abteilung sowie auf Führungskräfte in den USA beschränkt, während der 3. Absatz von Ziff. 6 alle Personen einbezieht, die vom Präsidenten (CEO), vom Vizepräsidenten Finanzen und vom Vizepräsidenten Human Resources benannt wurden. Hier wäre zumindest eine Klarstellung in der Richtung angebracht, dass nur Mitarbeiter der Personal- und der IT-Abteilung sowie Führungskräfte beauftragt oder bevollmächtigt werden können.

e) Übermittlung an Dritte durch US-Unternehmen

Sonderprobleme ergeben sich dann, wenn die in ein US-Konzernunternehmen übermittelten Daten an Dritte weitergegeben werden sollen. Insoweit ist darauf zu achten, dass die Betriebsvereinbarung nicht implizite von den Safe Harbor Principles abweicht und dadurch ggf. erhebliche Schwierigkeiten für alle Beteiligten provoziert.

Nach den „Safe Harbor Privacy Principles" (abgerufen am 11.6.2011 unter http://www.export.gov/safeharbor/eu/eg_main_018475.asp) gelten beim „Onward Transfer" die Notice and Choice Principles, sofern es sich nicht um einen Fall von Auftragsdatenverarbeitung handelt. „Notice" bedeutet Information des Betroffenen, „Choice" meint u. a. das Recht, der Übermittlung an Dritte zu widersprechen und diese so unmöglich zu machen. Die vorliegenden Regelungen zur Übermittlung könnten den Eindruck erwecken, dass man dieses Verfahren nicht praktiziert. Dies sollte im Rahmen des irgend Möglichen verhindert werden, in dem man ausdrücklich formuliert:

„Die Weiterübermittlung von Arbeitnehmerdaten ist nur zulässig, wenn sie vorher den betroffenen Arbeitnehmern mitgeteilt und diesen das Recht eingeräumt wird, innerhalb einer Woche nach Eingang der Miteilung der Übermittlung zu widersprechen. Während des Urlaubs und einer krankheitsbedingten Arbeitsunfähigkeit ist der Lauf der Frist

gehemmt. Die Auftragsdatenverarbeitung richtet sich nach dem Grundsatz „Onward Transfer“ der „Safe Harbor Privacy Principles“ in ihrer jeweiligen Fassung.“

f) Informations- und Kontrollrechte des Betriebsrats

Ein weiteres Problem betrifft die Informations- und Kontrollrechte des Betriebsrats. Die Richtlinien enthalten unter Ziff. 7 eine sinnvolle Regelung über die Rechte der Betroffenen auf Auskunft, Überprüfung, Löschung und Berichtigung, die sich in ähnlicher Weise in dem Grundsatz „Access“ der Safe Harbor Principles wiederfindet. Dass auch der Betriebsrat aufgrund seiner Aufgaben einen erheblichen Informationsbedarf hat, ist ähnlich wie in den EU-Musterverträgen nicht erwähnt. Insoweit empfiehlt es sich, hier eine entsprechende Ergänzung vorzunehmen und beispielsweise zu formulieren:

„Soweit einzelne Betroffene Rechte auf Auskunft gegenüber Unternehmen in den USA haben, gilt dies auch für den Betriebsrat. Diesem steht insbesondere die Befugnis zu, die Einhaltung des Datenschutzrechts einschließlich der zu seiner Realisierung geschlossenen Verträge und der Safe Harbor Principles zu überwachen und die dafür erforderlichen Informationen vom Datenempfänger zu erhalten. Er kann dabei dieselben Wege wie ein einzelner Beschäftigter benutzen.“

Der Schlusssatz soll insbesondere die Möglichkeit eröffnen, sich an die Kontaktstelle für den Datenschutz zu wenden, die in Ziff. 10 der Richtlinien erwähnt ist.

IV. Weitere Vorschriften

1. Sanktionen

Nr. 8 des vorliegenden Entwurfs bestimmt:

„Verstöße gegen das Datengeheimnis können gemäß § 43 BDSG und andere einschlägige Vorschriften mit Freiheits- oder Geldstrafen geahndet werden. Davon unbeschadet können bei Verletzungen arbeitsvertragliche Sanktionen von einer Abmahnung bis hin zur außerordentlichen Kündigung verhängt werden.“

Dass Verstöße gegen datenschutzrechtliche Grundsätze zu Bußgeldern und Strafen nach §§ 43, 44 BDSG führen und außerdem arbeitsrechtliche Konsequenzen bis hin zur fristlosen Kündigung haben können, ist allgemein anerkannt. Insofern fragt es sich, ob die Betriebsvereinbarung dies ausdrücklich hervorheben soll. Wird dies aus irgendwelchen Gründen von beiden Seiten gewünscht, so wäre Folgendes zu beachten:

§ 43 BDSG betrifft ausschließlich Ordnungswidrigkeiten; die Tatbestände in Abs.1 unterscheiden sich dabei durch den niedrigeren Bußgeldrahmen von denen des Abs.2. Die Strafvorschriften sind in § 44 BDSG enthalten, wobei – soweit ersichtlich – noch nie Freiheitsstrafen verhängt wurden. Der Hinweis auf die arbeitsrechtlichen Sanktionen leidet ein wenig daran, dass der Leser nicht erkennen kann, wann die Nebenpflicht zur Wahrung datenschutzrechtlicher Grundsätze verletzt ist.

Zur bestehenden Rechtsprechung s. KR-Fischermeier, Gemeinschaftskommentar zum Kündigungsschutzgesetz und zu sonstigen kündigungsschutzrechtlichen Vorschriften, 9. Aufl. 2009, § 626 BGB Rn 418; Kittner/Däubler/Zwanziger-Däubler, Kündigungsschutzrecht, 8. Aufl. 2011, § 626 BGB Rn 126

Man sollte deshalb zumindest klarstellen, dass arbeitsrechtliche Sanktionen nur bei Verletzung arbeitsvertraglicher Pflichten in Betracht kommen. Als Formulierung wäre (notfalls) zu erwägen:

„Verstöße gegen das Datengeheimnis und andere datenschutzrechtliche Bestimmungen können nach §§ 43, 44 BDSG zu Geldbußen, in bestimmten Fällen auch zu einer Geld- oder Freiheitsstrafe führen. Soweit arbeitsvertragliche Nebenpflichten verletzt werden, sind Sanktionen möglich, die von der Abmahnung bis zur außerordentlichen Kündigung reichen können."

2. Inkrafttreten und Kündigung

Insoweit könnte man formulieren:

„Die vorliegende Betriebsvereinbarung tritt mit Unterzeichnung durch die Betriebsparteien in Kraft. Sie kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden. Eine Nachwirkung ist ausgeschlossen; nach dem Wirksamwerden der Kündigung gelten die gesetzlichen Bestimmungen."

Die Laufzeit einer Betriebsvereinbarung hängt entscheidend davon ab, ob beide Seiten in ihr eine dauerhafte Lösung sehen oder ob die Arbeitgeberseite eine inhaltliche Konzession gemacht hat und nunmehr für einige Jahre an dieser Front Ruhe haben möchte. Insoweit lässt sich von außen schwer beurteilen, ob eine längerfristige Bindung in Betracht kommt oder nicht. Nach der vorliegenden Fassung ist eine relativ schnelle Änderung möglich. Dazu trägt such die Tatsache bei, dass die Nachwirkung ausgeschlossen wird. Dies ist zwar zulässig, wird aber regelmäßig nur bei Übergangsregelungen praktiziert. Würde man sich für eine Nachwirkung entscheiden, könnte dies der Vereinbarung zusätzliche Stabilität verleihen, da es immer geraume Zeit dauert, bis eine Neuregelung ausverhandelt ist.

3. Salvatorische Klausel

Die vorgeschlagene Betriebsvereinbarung bestimmt insoweit:

„10. Salvatorische Klausel
Sollten einzelne Bestimmungen dieser Vereinbarung einschließlich dieser Regelung ganz oder teilweise unwirksam sein oder werden, oder sollte der Vertrag eine Regelungslücke enthalten, bleibt die Wirksamkeit der übrigen Bestimmungen oder Teile solcher Bestimmungen unberührt. Anstelle der unwirksamen oder fehlenden Bestimmungen gelten die jeweils gesetzlichen Regelungen. Beide Parteien verpflichten sich unverzüglich, für den unwirksam gewordenen Teil der Vereinbarung eine dem ursprünglichen Sinn und der verfolgten Absicht entsprechende Vereinbarung zu treffen, die der aktuellen Rechtslage entspricht."

Salvatorische Klauseln sind eine sinnvolle Einrichtung und deshalb weit verbreitet. Unproblematisch ist der Satz 1, wonach die Gültigkeit der übrigen Abmachungen unberührt bleibt, wenn eine Bestimmung unwirksam ist (oder wird) oder wenn ein

wesentlicher Punkt vergessen wurde und man deshalb entsprechend § 155 BGB Zweifel an der Wirksamkeit der gesamten Abmachung haben könnte.

Wie man die von Anfang an bestehende oder später entstehende Lücke schließt, ist schwieriger zu entscheiden. Der Verweis auf das Gesetz ist überall dort sinnvoll, wo es eine gesetzliche Regelung gibt. Fehlt sie, kann man entweder eine Ergänzung aus dem Sinn und Zweck des Vertragswerks heraus oder – wie hier – eine Verhandlungspflicht vorsehen, die aber durch einen Konfliktlösungsmechanismus ergänzt werden muss, weil Verhandlungen nicht immer zu einem Ergebnis führen. Möglich wäre die folgende Formulierung:

„Sollten einzelne Bestimmungen dieser Vereinbarung einschließlich dieser Regelung ganz oder teilweise unwirksam sein oder werden, oder sollte der Vertrag einen wesentlichen Punkt nicht geregelt haben, so bleibt die Wirksamkeit der übrigen Bestimmungen bzw. der nicht betroffenen Teile solcher Bestimmungen unberührt. Die entstandene Lücke ist im Rahmen des Möglichen durch Rückgriff auf gesetzliche Regelungen zu schließen.

Die Betriebsparteien verpflichten sich, unverzüglich Verhandlungen aufzunehmen, um die Lücke durch eine dem Sinn und Zweck der Vereinbarung entsprechende Regelung zu schließen. Bleiben die Verhandlungen ergebnislos, entscheidet die Einigungsstelle.“

V. Ergänzende Vorschriften

Der vorliegende Entwurf greift eine Reihe von Fragen nicht auf, die in der Praxis vieler Unternehmen eine Rolle spielen. Gerade angesichts der „Verlagerung“ wichtiger Teile der Personaldatenverarbeitung in die USA erscheint das Gebot der Datentransparenz besonders dringend. Dabei reicht es nicht, dieses schlicht als Ziel festzuschreiben. Vielmehr geht es um konkrete Konsequenzen. Dazu gehört etwa die Trennung von Datenbeständen je nach dem Zweck, der der Erhebung der Daten zugrunde lag. Dies wird auch von § 28 Abs.1 Satz 2 BDSG gefordert, doch erscheint es sinnvoll, insoweit eine klarstellende Bestimmung aufzunehmen. Dies setzt wiederum voraus, dass der Zweck vor der Erhebung eindeutig festgelegt wurde. Weiter sollte man auch eine mögliche Zweckänderung ins Auge fassen und an relativ enge Voraussetzungen binden; nur so kann dem informationellen Selbstbestimmungsrecht ausreichend Rechnung getragen werden.

Die Festlegung datenschutzrechtlicher Regeln ist nur dann von praktischer Bedeutung, wenn auch eine effektive Kontrolle stattfinden kann. Diese sollte Sache des Betriebsrats sein, dem man das Recht einräumen kann, in bestimmte Dateien selbst Einblick zu nehmen. Auch wäre es nützlich, könnte er durch Befragung von Beschäftigten an ihren Arbeitsplätzen klären, inwieweit die Zugriffsrechte eingehalten sind oder nicht.

Die folgenden Formulierungen kämen in Betracht:

8. Datentransparenz

(1) Alle verwendeten Systeme müssen für die Betroffenen transparent sowie abschließend und vollständig dokumentiert sein.

(2) Vor der Erhebung personenbezogener Daten ist der mit ihr verbundene Zweck verbindlich festzulegen und den betroffenen Arbeitnehmern wie dem Betriebsrat mitzuteilen.

(3) Personenbezogene Daten der Arbeitnehmer sind ihrem jeweiligen Zweck entsprechend getrennt von Daten zu speichern, die zu anderen Zwecken erhoben worden sind. Eine zweckübergreifende Verarbeitung und Nutzung ist nur unter den Voraussetzungen einer Zweckänderung zulässig.

(4) Eine Zweckänderung gespeicherter Arbeitnehmerdaten ist nur zulässig, wenn die Voraussetzungen des § 28 Abs.2 BDSG erfüllt sind, der Betroffene vorher informiert wurde und der Betriebsrat zustimmt.

9. Kontrollrechte des Betriebsrats

(1) Der Betriebsrat kann nach § 80 Abs.2 BetrVG alle Informationen verlangen, die er für die Ausübung seiner Befugnisse und zur Durchführung dieser Betriebsvereinbarung benötigt. Er hat außerdem das Recht, die mit Datenverarbeitung befassten Arbeitnehmer über die Einhaltung der bestehenden datenschutzrechtlichen Regeln und dieser Betriebsvereinbarung zu befragen. Sie müssen ggf. bestimmte Anwendungen zu

Prüfzwecken durchführen, soweit dies der Betriebsrat verlangt. Der Vorgesetzte ist vorher zu informieren.

(2) Der Betriebsrat kann Einsicht in die Nutzungs- und Zugriffsberechtigungen aller Mitarbeiter einschließlich leitender Angestellter, der Geschäftsführung und der in USA tätigen Führungskräfte nehmen. Soweit vorhanden, sind ihm Protokolle und die Programmdokumentation des jeweiligen IuK-Systems zugänglich zu machen. Die Einsichtnahme erfolgt in Anwesenheit des betrieblichen Datenschutzbeauftragten; ist dieser verhindert, hat er einen Vertreter zu entsenden.

(3) Dem Betriebsrat wird ein Online-Leserecht auf folgende Datenarten eingeräumt:

- Anwesenheitszeiten der Arbeitnehmer
- …

(4) Finden bei der Einführung eines neuen IuK-Systems Qualifizierungsmaßnahmen statt, so können daran zwei Betriebsratsmitglieder teilnehmen; § 37 Abs.6 und 7 BetrVG bleibt unberührt.

VI. Vorschlag für eine Betriebsvereinbarung (zugleich Zusammenfassung der gemachten Vorschläge)

Betriebsvereinbarung Datenschutz

Zwischen

D Europe GmbH
vertreten durch:

und

Betriebsrat der D Europe GmbH
vertreten durch:

wird Folgendes vereinbart:

Die hier niedergelegte Betriebsvereinbarung verfolgt das Ziel, den Datenschutz der Beschäftigten zu gewährleisten und zugleich zur Reibungslosigkeit der Arbeitsabläufe beizutragen. Sie soll eine Atmosphäre der vertrauensvollen Kooperation schaffen, was zugleich auch den Geschäftspartnern zugutekommt.

1. Geltungsbereich

Diese Betriebsvereinbarung gilt für alle Mitarbeiter der D GmbH, die von § 5 Abs.1 BetrVG erfasst werden.
Der Arbeitgeber verpflichtet sich, die Inhalte dieser Betriebsvereinbarung durch entsprechende Gestaltung der Arbeitsverträge auch gegenüber leitenden Angestellten verbindlich zu machen. (Satz 2 optional)

2. Definitionen (optional)

Personenbezogene Daten: Sämtliche Daten, die sich auf einen Mitarbeiter/eine Mitarbeiterin beziehen oder die auf einen Mitarbeiter/eine Mitarbeiterin bezogen werden können.
Dienstliche Daten: Personenbezogene Daten, die in einem unmittelbaren Zusammenhang mit dem Arbeitsverhältnis stehen (z. B. Daten aus der Zeiterfassung oder der Lohnabrechnung)
Private Daten: Personenbezogene Daten, die nicht in einem direkten Zusammenhang mit dem Arbeitsverhältnis stehen (z. B. Freizeitaktivitäten).

3. Datengeheimnis

Die Verpflichtung auf das Datengeheimnis richtet sich nach § 5 BDSG. Dabei ist die Schriftform zu wahren.

4. Meldung von Datenschutzmängeln

Wird gegen Regeln des Datenschutzes oder der Datensicherung verstoßen, so sollte unverzüglich der betriebliche Datenschutzbeauftragte informiert werden. Dieser ergreift die erforderlichen Schritte, um für Abhilfe zu sorgen; dem Informanten kann er Vertraulichkeit zusagen. § 42a BDSG bleibt unberührt.

5. Betrieblicher Datenschutzbeauftragter

Bestellung und Abberufung eines Datenschutzbeauftragten bedürfen der vorherigen Unterrichtung des Betriebsrats. § 99 BetrVG und andere gesetzliche Rechte des Betriebsrats bleiben unberührt.

Der betriebliche Datenschutzbeauftragte ist verpflichtet und ermächtigt, dem Betriebsrat alle Informationen zugänglich zu machen, welche dieser benötigt, um seine Aufgabe nach dieser Betriebsvereinbarung zu erfüllen.

6. Datenübermittlung an andere Unternehmen

(1) Personenbezogene Daten von Mitarbeitern dürfen an andere Unternehmen nur übermittelt werden, wenn dies zur Begründung, Durchführung oder Beendigung des Arbeitsverhältnisses erforderlich ist. Eine Übermittlung ist nur durch den Personalleiter oder einen Geschäftsführer möglich. Sie können dieses Recht auf nachgeordnete Personen delegieren.

(2) – Optional - Private Daten von Arbeitnehmern unterliegen den allgemeinen Regeln des BDSG. Eine Übermittlung an Dritte ist nur auf der Grundlage besonderer Verträge oder einer Einwilligung des Arbeitnehmers zulässig. Die Einwilligung muss freiwillig erteilt sein. Ihre Verweigerung darf keine Benachteiligung im Arbeitsverhältnis möglich erscheinen lassen.

7. Datenübermittlung ins Ausland, insbesondere in die USA

(1) Personenbezogene Daten von Arbeitnehmern können im Rahmen der allgemeinen Voraussetzungen an ausländische Unternehmen übermittelt werden, wenn diese in einem Mitgliedstaat der EU oder des Europäischen Wirtschaftsraums belegen sind. Gleichgestellt sind Unternehmen aus Ländern, die nach den Erklärungen der EU-Kommission ein angemessenes Datenschutzniveau besitzen.

(2) Sollen Daten in Länder ohne angemessenes Datenschutzniveau übermittelt werden, so ist die Genehmigung der Aufsichtsbehörde einzuholen oder ein von der EU-Kommission und den Aufsichtsbehörden empfohlener Standardvertrag zugrunde zu legen. Soweit danach einzelne Betroffene Rechte gegenüber dem Datenempfänger haben, gilt dies auch für den Betriebsrat. Diesem steht insbesondere das Recht zu, die Einhaltung des Datenschutzrechts einschließlich der zu seiner Realisierung geschlossenen Verträge zu überwachen und die dafür erforderlichen Informationen vom Datenempfänger zu erhalten.

(3) Die Dover Corporation und die D Industries haben verbindliche Unternehmensrichtlinien geschaffen, welche die internationale Weitergabe von personenbezogenen Daten innerhalb des Konzerns regeln und die dabei zu beachtenden datenschutzrechtlichen Grundsätze festlegen. Dover Corporation wird sich zusätzlich der Safe-Harbor-Zertifizierung unterziehen.

Personenbezogene Daten dürfen nur zu dienstlichen Zwecken im Sinne der Ziff. 4 der Datenschutzrichtlinien der Dover Corporation in die USA übermittelt werden. Eine Anforderung kann allein durch den Präsidenten, den Vizepräsidenten Finanzen und den Vizepräsidenten Human Resources erfolgen, die diese Möglichkeit nur auf Mitarbeiter der Personal- und der IT-Abteilung sowie auf Führungskräfte delegieren können.

Die Weiterübermittlung von Arbeitnehmerdaten durch US-Unternehmen ist nur zulässig, wenn sie vorher den betroffenen Arbeitnehmern mitgeteilt und diesen das Recht eingeräumt wird, innerhalb einer Woche nach Eingang der Mitteilung der Übermittlung zu widersprechen. Während des Urlaubs und einer krankheitsbedingten Arbeitsunfähigkeit ist der Lauf der Frist gehemmt. Die Auftragsdatenverarbeitung richtet sich nach dem Grundsatz „Onward Transfer" der „Safe Harbor Privacy Principles" in ihrer jeweiligen Fassung.

Soweit einzelne Betroffene Rechte auf Auskunft gegenüber Unternehmen in den USA haben, gilt dies auch für den Betriebsrat. Diesem steht insbesondere die Befugnis zu, die Einhaltung des Datenschutzrechts einschließlich der zu seiner Realisierung geschlossenen Verträge und der Safe Harbor Principles zu überwachen und die dafür erforderlichen Informationen vom Datenempfänger zu erhalten. Er kann dabei dieselben Wege wie ein einzelner Beschäftigter benutzen.

(4) Personenbezogene Daten sind bei der Übermittlung ins Ausland soweit als möglich als gesicherter Datenanhang zu versenden. Der Anhang ist mit einem Passwort zu versehen.

(5) Das Mitbestimmungsrecht des Betriebsrats nach § 87 Abs.1 Nr. 6 BetrVG bleibt auch dann unberührt, wenn Datenverarbeitungen, die geeignet sind, Verhalten und Leistung der Arbeitnehmer zu überwachen, ganz oder teilweise im Ausland erfolgen.

8. Datentransparenz (optional)

(1) Alle verwendeten Systeme müssen für die Betroffenen transparent sowie abschließend und vollständig dokumentiert sein.

(2) Vor der Erhebung personenbezogener Daten ist der mit ihr verbundene Zweck verbindlich festzulegen und den betroffenen Arbeitnehmern wie dem Betriebsrat mitzuteilen.

(3) Personenbezogene Daten der Arbeitnehmer sind ihrem jeweiligen Zweck entsprechend getrennt von Daten zu speichern, die zu anderen Zwecken erhoben worden sind. Eine zweckübergreifende Verarbeitung und Nutzung ist nur unter den Voraussetzungen einer Zweckänderung zulässig.

(4) Eine Zweckänderung gespeicherter Arbeitnehmerdaten ist nur zulässig, wenn die Voraussetzungen des § 28 Abs.2 BDSG erfüllt sind, der Betroffene vorher informiert wurde und der Betriebsrat zustimmt.

9. Kontrollrechte des Betriebsrats (optional)

(1) Der Betriebsrat kann nach § 80 Abs.2 BetrVG alle Informationen verlangen, die er für die Ausübung seiner Befugnisse und zur Durchführung dieser Betriebsvereinbarung benötigt. Er hat außerdem das Recht, die mit Datenverarbeitung befassten Arbeitnehmer über die Einhaltung der bestehenden datenschutzrechtlichen Regeln und dieser Betriebsvereinbarung zu befragen. Sie müssen ggf. bestimmte Anwendungen zu Prüfzwecken durchführen, soweit dies der Betriebsrat verlangt. Der Vorgesetzte ist vorher zu informieren.
(2) Der Betriebsrat kann Einsicht in die Nutzungs- und Zugriffsberechtigungen aller Mitarbeiter einschließlich leitender Angestellter, der Geschäftsführung und der in USA tätigen Führungskräfte nehmen. Soweit vorhanden, sind ihm Protokolle und die Programmdokumentation des jeweiligen IuK-Systems zugänglich zu machen. Die Einsichtnahme erfolgt in Anwesenheit des betrieblichen Datenschutzbeauftragten; ist dieser verhindert, hat er einen Vertreter zu entsenden.
(3) Dem Betriebsrat wird ein Online-Leserecht auf folgende Datenarten eingeräumt:

- Anwesenheitszeiten der Arbeitnehmer
- …

(4) Finden bei der Einführung eines neuen IuK-Systems Qualifizierungsmaßnahmen statt, so können daran zwei Betriebsratsmitglieder teilnehmen; § 37 Abs.6 und 7 BetrVG bleibt unberührt.

10. (bisher 8.) Sanktionen bei Zuwiderhandlungen (optional)

Verstöße gegen das Datengeheimnis und andere datenschutzrechtliche Bestimmungen können nach §§ 43, 44 BDSG zu Geldbußen, in bestimmten Fällen auch zu einer Geld- oder Freiheitsstrafe führen. Soweit arbeitsvertragliche Nebenpflichten verletzt werden, sind Sanktionen möglich, die von der Abmahnung bis zur außerordentlichen Kündigung reichen können.

11. (bisher 9.) Inkrafttreten und Auslaufen

Die vorliegende Betriebsvereinbarung tritt mit Unterzeichnung durch die Betriebsparteien in Kraft. Sie kann mit einer Frist von drei Monaten zum Quartalsende gekündigt werden. Eine Nachwirkung ist ausgeschlossen; nach dem Wirksamwerden der Kündigung gelten die gesetzlichen Bestimmungen.

12. (bisher 10.) Salvatorische Klausel

Sollten einzelne Bestimmungen dieser Vereinbarung einschließlich dieser Regelung ganz oder teilweise unwirksam sein oder werden oder sollte der Vertrag einen wesentlichen Punkt nicht geregelt haben, so bleibt die Wirksamkeit der übrigen Bestimmungen bzw. der nicht betroffenen Teile solcher Bestimmungen unberührt. Die entstandene Lücke ist im Rahmen des Möglichen durch Rückgriff auf gesetzliche Regelungen zu schließen.

Die Betriebsparteien verpflichten sich, unverzüglich Verhandlungen aufzunehmen, um die Lücke durch eine dem Sinn und Zweck der Vereinbarung entsprechende Regelung zu schließen. Bleiben die Verhandlungen ergebnislos, entscheidet die Einigungsstelle.