ZULÄSSIGER EU-ÜBERGREIFENDER ARBEITNEHMER-DATENTRANSFER IM KONZERNGEFÜGE AM BEISPIEL EINER PERSONAL ERP-EINFÜHRUNG

Dr. Oliver M. Habel, Rechtsanwalt

tecLEGAL Habel Rechtsanwälte
habel@teclegal-habel.de

Zusammenfassung

Die Nutzung der vorhandenen Mitarbeiter-Ressourcen in einem Konzern sind eine wesentliche betriebswirtschaftliche Anforderung für den Erfolg der wirtschaftlichen Tätigkeit der Konzernunternehmen und seiner Mitarbeiter. Die Weitergabe von personenbezogenen Arbeitnehmerdaten zwischen Konzerngesellschaften kann viele Vorteile für beide Seiten bringen, insbesondere bei der Ressourcen-Planung, bei der allgemeinen und individuellen Mitarbeiterentwicklung, aber auch Sorgen im Zusammenhang mit einer Leistungs- und Verhaltenskontrolle verursachen. Die Art der Mitarbeiterdaten sind vielfältig. Insbesondere Leistungs- und Verhaltensdaten berühren den einzelnen Arbeitnehmer unmittelbar in seiner Person. Eine Kontrolle darüber, welche Daten des Arbeitnehmers erhoben, genutzt und ggf. weitergegeben werden, insbesondere wer Zugang hierauf hat, gehört zum Schutz des Kernbereichs des Persönlichkeitsrechts des Arbeitnehmers.

Aus diesem Grund hat sich der Gesetzgeber ausdrücklich dazu entschieden, kein Konzernprivileg in das Bundesdatenschutzgesetz (BDSG) aufzunehmen[1],[2]. Es soll kein Automatismus entstehen, dass die Personaldaten beim Arbeitgeber auch an andere Konzernunternehmungen weitergegeben werden können.

Will eine Konzerngesellschaft Personaldaten für einen bestimmten Zweck zur Datenverarbeitung zu einer anderen Gesellschaft des Konzerns übertragen, kann die Privilegierung einer Auftragsdatenverarbeitung im Sinne von § 11 BDSG als Grundlage für die Datenübertragung in Frage kommen. Werden aber anlässlich der Datenübermittlung auch Funktionen des Arbeitgebers übertragen, insbesondere wenn die Datenverarbeitung beim Datenimporteur auch für seine eigenen Zwecke stattfindet, bedarf es einer anderen gesetzlichen Grundlage aus §§ 32, 28 BSGD oder der vorherigen informierten Einwilligung des einzelnen Arbeitnehmers.

Ganz überwiegend wird das Erfordernis einer Freiwilligkeit der Einwilligung bei Regelung im Arbeitsvertrag selbst oder bei einem nachträglichen Änderungsverlangen des Arbeitgebers verneint, soweit die konkrete Tätigkeit nicht per se bereits einen ausdrücklichen Konzernbezug hat. Als Alternative drängt sich der Abschluss einer Betriebsvereinbarung über die Weitergabe von Arbeitnehmerdaten innerhalb des Konzerns auf, die sowohl die Transparenz und die Überprüfbarkeit der Datenverwendung steigern, insbesondere aber auch dem Betriebsfrieden dienen kann.

Der Beitrag zeigt die rechtlichen Anforderungen an eine Betriebsvereinbarung für eine

[1] Taeger/ Gabel, a. a. O , § 4 b Rn. 15.
[2] Arbeitsbericht, a. a. O, S 7.

rechtmäßige EU-übergreifende Übertragung von Arbeitnehmerdaten anhand eines konkreten Falls auf.

1 Sachverhalt

Steel Deutschland GmbH ist 100 %-ige Tochtergesellschaft der Steel Corporation, Michigan, USA, mit Sitz in München. Rund 100 Arbeitnehmer sind überwiegend am Münchener Standort mit dem Vertrieb von Produkten der Steel Corporation beschäftigt. Die Arbeitsverträge enthalten keine Regelung zu einer Weitergabe von Personaldaten an Konzernunternehmen. In der Regel fallen auch die Aufgabenbeschreibungen in den Arbeitsverträgen so beschränkt aus, dass ein ausdrücklicher Konzernbezug der jeweiligen Beschfäftigung fehlt. Es existiert ein Betriebsrat.

Steel Corporation, USA hat ein Personal-ERP-System am Geschäftssitz der Muttergesellschaft in Michigan, USA installiert. Personaldaten der Mitarbeiter aller Tochtergesellschaften sollen dort erfasst und verarbeitet werden für verschiedene Zwecke der Muttergesellschaft, insbesondere Personalplanung, Verwaltung des Boni-Systems, aber auch der Mitarbeiterentwicklung. Steel Corporation, USA ist Safe Harbor registriert und hat seit 2011eine Data Privacy Policy.

Der Betriebsrat befürchtet, dass die Konzernmutter über das installierte ERP-System insbesondere auch Leistungsdaten der Arbeitnehmer über deren mit IT ausgestatteten Arbeitsplätze auslesen kann, z. B. bei der Lagerhaltung, aber auch in der Verwaltung. Der deutsche Geschäftsführer will Datenschutz-compliant handeln. Das Anschreiben an jeden einzelnen Arbeitnehmer für eine nachträgliche vertragliche Ergänzung der Anstellungsverträge zum Zwecke der Einholung einer individuellen Erlaubnis zur Datenweitergabe an die Konzernmutter möchte er zum Schutz des Betriebsfriedens dringend vermeiden.

2.1 Übersicht über die gesetzlichen Anforderungen an eine Datenübermittlung an Dritte

1.1.1 Der Sachverhalt gibt bereits vor, dass Einwilligungsregelungen zu einer Datenübermittlung an Dritte in den Anstellungsverträgen fehlen und eine nachträgliche Vertragsergänzung, die letztlich rechtlich eine Änderungskündigung wäre, vermieden werden soll. Ort der geplanten Datenverarbeitung bei Steel US ist Michigan, USA, also außerhalb der EU und des EWiR. Für die USA hat die Europäische Kommission auch nicht eine Vergleichbarkeit des Datenschutzniveaus festgestellt. Deshalb muss die Zuläs-

sigkeit der Datenübermittlung im Einzelnen geprüft werden. Die Prüfungsreihenfolge erfolgt in zwei Stufen, zunächst in Gestalt der Suche nach einer Erlaubnisnorm für die Speicherung und Nutzung der Personaldaten bei Steel D. In einem zweiten Schritt folgt die Frage nach der Rechtmäßigkeit einer Datenübermittlung ins Ausland und deren Voraussetzungen.

2.1.2 § 32 Abs. 1 S. 1 BDSG erlaubt spezifisch die Erhebung, Verarbeitung und Nutzung (nachfolgend gemeinsam „Nutzen") von personenbezogenen Daten eines Beschäftigten für die Zwecke des Beschäftigungsverhältnisses und dessen Durchführung oder Beendigung, soweit es erforderlich ist.[3] Im vorliegenden Fall lässt der Sachverhalt nicht erkennen, warum laut Arbeitsverträgen eine Übermittlung von einzelnen Personaldaten an andere Konzerngesellschaften konkret erforderlich sein soll.[4] Die Arbeitsverträge sagen hierzu nichts.

2.1.3 Neben der bereichsspezifischen Regelung in § 32 BDSG kann sich eine gesetzliche Erlaubnis auch aus § 28 Abs. 1 BDSG ergeben.[5] Die Tatbestandsalternative im § 28 Abs. 1 Nr. 1 BDSG ist annähernd gleichlautend mit dem Tatbestand in § 32 Abs. 1 S. 1 BDSG. Zur Erforderlichkeit einer Datenübermittlung ist aber in den Arbeitsverträgen des Beispielfalls nichts geregelt. Deshalb scheidet § 28 1 Nr. 1 BDSG als Erlaubnisnorm aus.

Es bleibt die Alternative in § 28 Abs. 1 Nr. 2 BDSG, die zweierlei voraussetzt:

- Die Wahrung der berechtigten Interessen der Verantwortlichen Stelle ist erforderlich und
- kein schutzwürdiges Interesse des Betroffenen überwiegt.

Für die Feststellung der berechtigten Interessen des Arbeitgebers und der schutzwürdigen Belange des Arbeitnehmers ist nach der Art der Daten und den Zweck der Datenübertragung zu fragen. Der Arbeitgeber muss sich also festlegen, welche Daten er für welche Zwecke an die Muttergesellschaft übermitteln will.

Im vorliegenden Fall sollen dies fiktiv angenommen der Name und die Funktion, das Eintrittsdatum, der Geschäftsbereich und die Abteilungsbezeichnung sein ebenso wie die gleichen Angaben zum Vorgesetzten. Als

[3] Gola/ Schomerus, BDSG, 11. Auflage, 2012, § 32 Rn. 10.
[4] Arbeitsbericht der ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer", a. a. O., S. 5 u. 6.
[5] Gola/ Wronka, a. a. O., § 32, Rn. 32.

Zwecke werden angegeben: Auszahlung, Budgetplanung, Einsatzplanung, Entwicklungsförderung, Benefitauszahlung, Unternehmensorganigramm.

Ich unterstelle, dass die Art der Daten und der Zweck ihrer Übermittlung bei einer Vertriebsgesellschaft wie im vorliegenden Fall der Wahrung berechtigter Interessen des deutschen Arbeitgebers zugeordnet werden kann. Schutzwürdige Belange der Arbeitnehmer könnten entgegen stehen, wenn es sich nicht nur um die vorstehenden, eher technischen Daten zum Arbeitnehmer handelt, sondern auch faktisch über den Zugriff des ERP-Systems auf die IT bei Steel D Verhaltens- und Leistungsdaten des Arbeitnehmers EDV-technisch ausgelesen werden können.

Der Sachverhalt sagt hierzu lediglich, dass der Betriebsrat dieses befürchtet. Folge: Es muss geregelt werden, dass Steel US sich verpflichtet, dies nicht zu tun. Ist dies der Fall, kann man annehmen, dass dem Vorhaben in der konkreten Ausgestaltung bezüglich Art der Daten und des Verwendungszwecks in der Abwägung keine schutzwürdigen Belange des Arbeitnehmers entgegen stehen. § 28 Abs. 1 Nr. 2 BDSG ziehe ich daher als einschlägige Erlaubnisnorm für die Nutzung und mögliche Übermittlung der vorstehend konkretisierten Personaldaten heran.

2.1.4 Alternativ oder auch ergänzend zu der gesetzlichen Erlaubnisnorm kann sich die Zulässigkeit der Datennutzung und Übermittlung auch aus dem Vorliegen einer Einwilligung des Arbeitnehmers im Sinne von § 4 a BDSG ergeben. Bei Arbeitsverträgen ist streitig, ob eine Einwilligungserklärung im Arbeitsvertrag hierfür herangezogen werden kann, da die Freiwilligkeit der Einwilligung ohne Nachteile bei einer Ablehnung unwahrscheinlich ist. Voraussichtlich wird ein Arbeitgeber einen Anstellungsvertrag nicht abschließen, wenn der Arbeitnehmer bereits bei der Einstellung die Einwilligung nicht erteilt.

Auch bei einer nachträglichen Vertragsänderung wird befürchtet, dass der Arbeitnehmer aus Sorge vor Nachteilen unterschreibt, nicht aber aufgrund einer Freiwilligkeit. Deshalb besteht im Beispielsfall beim Geschäftsführer auch die Sorge um den Betriebsfrieden. Die Alternative scheidet vorliegend also auch aus. [6]

[6] Eine Novellierung des Arbeitnehmer-Datenschutzes durch die Bundesregierung mit neuen §§ 32 a bis 32 l BDSG wurde im Februar 2013 von der Bundesregierung zurückgezogen. Deren neugefasster § 32 l hätte zur Einwilligungsfähigkeit erhebliche Einschränkungen vorgesehen. Der Entwurf einer EU-Datenschutzverordnung will in § 7 Abs. 4 nur dann eine Einwilligung anerkennen, wenn zwischen den Vertragsparteien kein wesentliches Ungleichgewicht besteht.

2.1.5 Zur „Übertragung" der Daten an einen Dritten wäre keine Einwilligung des Arbeitnehmers erforderlich, wenn das datenimportierende Konzernunternehmen ausschließlich eine Auftragsdatenverarbeitung für das datenexportierende Konzernunternehmen vornimmt. Das BDSG behandelt fiktiv eine Auftragsdatenverarbeitung seitens der Verantwortlichen Stelle (also dem deutschen Arbeitgeber) nicht als eine Datenübermittlung, sondern privilegiert die Auftragsdatenverarbeitung, indem der Gesetzgeber diese Art der Datenverarbeitung dem Herrschaftsbereich der Verantwortlichen Stelle zuordnet. Kernstück für die Annahme einer Auftragsdatenverarbeitung i. S. v. § 11 BDSG ist die Unterscheidung, ob die zur Verarbeitung übermittelten Daten an den Dritten ausschließlich weiterhin der alleinigen Kontrolle der Verantwortlichen Stelle unterliegen, ohne dass weitere Dritte Zugang zu diesen Daten erhalten können oder eine Funktionsübertragung vorliegt, bei der der Datenimporteur eine Datenverarbeitung nicht nur unter der Kontrolle und bei Wahrung der Voraussetzungen für die Zulässigkeit einer Auftragsdatenverarbeitung in § 11 Abs. 2 BDSG vornimmt, sondern auch einzelne Funktionen der Verantwortlichen Stelle wahrnimmt.[7],[8]

Im vorliegenden Fall soll Steel US Auszahlungen für Steel D veranlassen, bei der Budgetplanung zumindest mitwirken ebenso wie bei der Einsatzplanung. Des Weiteren ist anzunehmen, dass Steel US auch eigene Zwecke verfolgt, wie durch die Zweckbestimmungen „Entwicklungsförderung" und „Benefit-Auszahlung" ersichtlich wird. Damit liegen aber die Voraussetzungen für eine Auftragsdatenverarbeitung nicht vor, so dass die Privilegierung in § 11 BDSG nicht greift.

2.1.6 Losgelöst von der Frage nach einer möglichen Auftragsdatenverarbeitung sind bei einer Datenweitergabe in ein Drittland, § 3 Abs. 8 Satz 2 i. V. m. § 3 Abs. 4 Nr. 3 BDSG, immer, also auch bei einer Auftragsdatenverarbeitung, die Übertragungsvoraussetzungen in §§ 4 b und 4 c BDSG zu erfüllen. [9]

2.2. Datenübertragung an Unternehmen in Drittstaaten

2.2.1 Soweit das datenimportierende Unternehmen seinen Sitz nicht in der EU oder in der erweiterten EWiR hat, bedarf jede Übertragung von Daten der Erfüllung der Voraussetzungen in §§ 4 b,4 c BDSG. Dies gilt auch für Fälle einer privile-

[7] vgl. hierzu Arbeitsbericht, a. a. O., S. 2
[8] vgl. hierzu Arbeitsbericht, a. a. O., S. 7.
[9] Arbeitsbericht, a. a. O., S. 5.

gierten Auftragsdatenverarbeitung, wie sich aus § 3 Abs. 8 S. 2 i. V. m. § 3 Abs. 4 Nr. 3 BDSG ergibt.

2.2.2 Die Voraussetzungen für eine Übermittlung von Daten ins Ausland, das nicht EU und nicht EWiR ist, finden ihre Regelung in § 4 b Abs. 2 S. 1, letzter Teilsatz i. V. m. § 4 b Abs. 2 S. 2 oder § 4 c BDSG. Einerseits muss also eine Erlaubnisnorm für das Nutzen der Daten z. B. nach § 28 Abs. 1 BDSG vorliegen. Andererseits sind die schutzwürdigen Interessen der Betroffenen an dem Ausschluss der Übermittlung zu prüfen, insbesondere wenn im Empfängerland kein angemessenes Datenschutzniveau gewährleistet ist.

Im vorliegenden Fall hat die Empfängerin Steel USA ihren Sitz in Michigan, an dem sie allein die ihr übermittelten Daten verarbeiten will. Für die USA ist seitens der Europäischen Kommission nicht die Gleichheit des Datenschutzniveaus wie beispielweise für die Schweiz oder auch teilweise Kanada festgestellt worden. Stattdessen besteht aber ein zwischen den USA, dort dem US-Bundesministerium für Handel und der Europäischen Kommission abgeschlossenes Safe Harbor Abkommen.

Der datenschutzrechtliche Wert des Safe Harbor Abkommens ist umstritten. Auch sollen sich lediglich rund 300 US-Unternehmen Safe Harbor registriert haben, bei denen aber angenommen wird, dass viele die Registrierungsvoraussetzungen nicht erfüllen. Dies liegt voraussichtlich auch daran, dass sich die Unternehmen, die sich registrieren lassen, selbst zertifizieren und erst dann Gegenstand einer Überprüfung werden können, wenn der Federal Trade Commission als Aufsichtsbehörde Beschwerden vorgelegt werden. Dennoch, dass Safe Harbor Abkommen existiert und ist eine praktikable, da rechtssichere Gestaltungsmöglichkeit für die Schaffung der Voraussetzung einer rechtmäßigen Datenübermittlung aus EU-Europa-Mitgliedsstaaten in die USA[10]. Die Voraussetzungen für eine Registrierung findet man auf der Homepage des amerikanischen Handelsministeriums unter **http://export.gov/safeharbor/**. Eine Registrierung gibt an Informationen zu dem Safe Harbor registrierten Unternehmen:

- vollständiger Name und Gesellschaftsform mit der kompletten Anschrift sowie Telefon, Fax und Internetseite
- Information zu der Kontaktstelle mit Namen und Durchwahl inkl. E-Mail-Adresse der Kontaktperson

[10] Taeger/ Gabel, a. a. O. § 4 b Rn 23.

- Zuständiger „Corporate Officer", also entweder der gesetzliche Vertreter („CEO") oder ein Entscheidungsträger im Unternehmen („Officer")
- Datum der ersten Zertifizierung und der nächsten anstehenden Zertifizierung
- Beschreibung der Art der Daten, der Zweck der Datenübermittlung und der Herkunft der Daten sowie das technische Umfeld der Datenverarbeitung
- Auskunft zur Data Privacy Policy des Unternehmens mit Link zur Internet-Adresse, unter der das Dokument aufgerufen werden kann
- Angabe zur Verifizierung. Besonderheit: Es ist eine Selbstzertifizierung des Anmelders vorgesehen
- Unterwerfung unter eine Streitbelegungsinstanz bei den EU-Europäischen Datenschutzaufsichtsbehörden
- Ausdrückliche Erklärung zur Bereitschaft der Zusammenarbeit mit den EU-Europäischen Datenschutzaufsichtsbehörden
- Benennung der Länder, von denen Daten importiert werden
- Industriesektor des Unternehmens
- Angabe zum Zertifikationsstatus: Lediglich „Current"
- Angabe zum Compliance Status ? In der Regel nicht ausgefüllt, wird aber praktisch so akzeptiert

2.2.3 Die Data Privacy Policy des datenimportierenden Unternehmens bedarf einer konkreten Prüfung[11], ob darin die Safe Harbor Principles und die FAQs = Frequently Asked Questions, die Bestandteil des Safe Harbor Abkommens sind, abgebildet werden, also ob die das datenimportierende Unternehmen selbst bindende Data Privacy Policy die in diesen FAQs genannten Voraussetzungen für sich erfüllt. Datenschutzrechtlich ist es spannend, diese Principles und FAQs zu lesen und Punkt für Punkt mit einer Data Privacy Policy abzuklären. Es kommt auf die Formulierung im Detail an, etwa zu „Opt-out" statt „Opt-in". Dies ist Voraussetzung, um festzustellen, ob die Data Privacy Policy tatsächlich für eine Safe Harbor Registrierung genügt. Da sich die Safe Harbor registrierten Unternehmen selbst zertifizieren, ist es datenschutzrechtlich wohl nicht ausreichend, sich lediglich die Registrierung nachweisen zu lassen. Stattdessen sollte die Verantwortliche Stelle einerseits den genügenden Grad der Selbstverpflichtung in der Data Privacy Policy des Datenimporteurs anhand der Safe Harbor Principles und der FAQs überprüfen. Des Weiteren müssen die vorgesehene Art und der

[11] Siehe hierzu Beschluss der obersten Aufsichtsbehörden für den Datenschutz im nicht öffentlichen Bereich am 28./29.04.2010.

Zweck der Datenübermittlung übereinstimmen mit den betreffenden Angaben hierzu in der Safe Harbor Registrierung. Auch bedarf es der Klärung, ob die Safe Harbor Registrierung aktuell vorliegt und sicherzustellen, dass sich das registrierende Unternehmen verpflichtet, die Registrierung in der Zukunft aufrecht zu erhalten. Schließlich sollte man sich schriftlich erklären lassen müssen, dass das registrierte Unternehmen auch künftig die Voraussetzungen der Zertifizierung erfüllen wird.

Die Vorlage der Safe Harbor Registrierung ist also kein Selbstläufer für die Verantwortliche Stelle, vorliegend Steel D. Stattdessen wird sich Steel D von der Muttergesellschaft Steel USA schriftlich die Erklärungen geben lassen müssen, dass die Zertifizierung auch künftig aufrecht erhalten wird und sie sich verpflichtet, die Voraussetzungen hierfür zu erfüllen.

2.2.4 Der Gesetzgeber hat in § 6 BDSG die Rechte des Betroffenen auf Auskunft, Berichtigung, Löschung oder Sperrung konkretisiert und so gestärkt, dass diese durch Rechtsgeschäfte nicht ausgeschlossen oder beschränkt werden können. Dies hat für eine Betriebsvereinbarung die Notwendigkeit einer Regelung zur Folge, dass die Arbeitnehmer, deren personenbezogene Daten von der Datenübermittlung betroffen sind, einerseits einen direkten Auskunftsanspruch gegenüber der Verantwortlichen Stelle, dem deutschen Arbeitgeber, behalten und andererseits aber auch einen direkten Auskunftsanspruch gegenüber den datenimportierenden Unternehmen besteht. Dies gelingt rechtlich durch eine selbstverpflichtende Übernahme der Betriebsvereinbarung seitens des datenimportierenden Unternehmend.[12]

2.2.5 Liegt eine Safe Harbor Registrierung vor, die die Art und den Zweck der konkreten Daten bzw. die Datenübermittlung abdeckt und gibt das datenimportierende Unternehmen die Erklärungen zur Fortsetzung der Registrierung und Aufrechterhaltung der Registrierungsvoraussetzungen ab, erfüllt die Data Privacy Policy die Voraussetzungen der FAQs und verpflichtet sich der Datenimporteur, den Arbeitnehmern einen direkten Auskunftsanspruch im Umfang von § 6 BDSG zu gewähren, werden die schutzwürdigen Interessen der Betroffenen insbesondere im Hinblick auf für eine Datenübermittlung in die USA aufgrund der Safe Harbor Registrierung und der Data Privacy Policy in Verbindung mit den vorstehenden Selbstverpflichtungen und Erklärungen des datenimportierenden Unter-

[12] Düsseldorfer Kreis, abgestimmte Position der Aufsichtsbehörde der Arbeitsgruppe „Internationaler Datentransfer" v. 12/13.2.2007, II Nr. 1.

nehmens gewahrt sein.

2.2.6 Zur Klärung des Sachverhaltes im Vorfeld bietet es sich an, Auskünfte vom Datenimporteur zu den Fragen einzuholen:

- Art der Personaldaten, die übertragen werden sollen
- Zweck der Datenübertragung an den Datenimporteur
- Liegt eine Auftragsdatenverarbeitung oder eine Funktionsübertragung vor?
- Wer hat Zugang zu den Daten?
- Sollen die Daten an weitere Dritte weiterübermittelt werden?
- Wer hat ggf. die alleinige Entscheidungskompetenz über die Änderung, Löschung und eine Nutzung von einzelnen Personaldaten?
- Ist die Übertragung tatsächlich erforderlich?
- Wäre eine pseudonymisierte Datenübertragung genügend?
- Sollen sensitive Daten im Sinne von § 3 Abs. 9 BDSG ebenfalls übertragen werden?
- Fragen zum Stand der Safe Harbor Registrierung und der Selbstzertifizierung
- Hinweis auf die Zweckbindung bei der Datenübertragung nach § 4 Abs. 6 BDSG

2.3 Ersatz der individuellen Einwilligung durch Betriebsvereinbarung

2.3.1 Durch die Aufgabenzuweisung in § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz, „Einführung und Anwendung technischer Hilfsmittel", wird die erforderliche Kompetenzzuordnung zum Betriebsrat vorgenommen.

Überwiegend wird angenommen, dass eine Betriebsvereinbarung eine „andere Rechtsvorschrift" im Sinne von § 4 BDSG sein kann.[13],[14] § 4 „Zulässigkeit der Datenerhebung, -verarbeitung und –nutzung" BDSG ist eine Erlaubnisnorm in Verbindung mit einer geeigneten anderen Rechtsvorschrift. Deshalb kann der Abschluss einer Betriebsvereinbarung auch eine Alterna-

[13] BAG, BB 1986, S. 2333
[14] Simitis (Hrsg.); BDSG, 7. Auflage, § 4 Rn. 11 und 16.

tive zur individuell erklärte Einwilligung des einzelnen Arbeitnehmers als Erlaubnisnorm sein.

In diesem Zusammenhang: Es bestehen unterschiedliche Auffassungen, ob eine Betriebsvereinbarung unter den Mindeststandard an Datenschutz, den das BDSG sichert, gehen darf. Gabel[15] bejaht dies indirekt, wenn er schreibt, dass eine Vereinbarung zur Datenübertragung zulässig sei, wenn in der Betriebsvereinbarung ausreichende Garantien für die Arbeitnehmer aufgenommen werden und sich das datenimportierende Unternehmen der Betriebsvereinbarung unterwirft. Simitis nimmt an, dass eine Betriebsvereinbarung eine „Rechtsvorschrift" i. S. v. § 4 Abs. 1 BDSG darstellt. Die Regelung müsse dem Recht auf informationelle Selbstbestimmung des Arbeitnehmers selbst genügen. Dies sei Maßstab[16] Das BAG lässt eine Abweichung zu.[17]. Ich möchte hierzu anmerken, dass Abweichungen auch vom BDSG im Einzelfall möglich sein können, wenn die Gesamtschau des Schutzniveaus in einer Betriebsvereinbarung im Wesentlichen dem gesetzgeberischen Datenschutz entspricht.

2.3.2 Die grundsätzlichen Zweifel des Betriebsrates im Beispielsfall sollen an den Anfang gestellt werden, da es nicht zu einer Betriebsvereinbarung kommen wird, wenn diese nicht geklärt werden können. Der Betriebsrat befürchtet technisch wohl begründet, dass auch solche Daten zu einzelnen Arbeitnehmern durch Zugang zu der von den Arbeitnehmern genutzten IT aufgrund des ERP-Systems ausgelesen werden können, die Rückschlüsse auf die Leistung oder auch das Verhalten des einzelnen Arbeitnehmers zulassen, etwa die Geschwindigkeit und Menge der Arbeiten im Lager von den jeweiligen Mitarbeiter, die Verweildauer und ggf. auch der Aufruf von Seiten im Internet, die Dauer der Bearbeitung von Dokumenten etc. Was tun?

Faktisch wird bei Steel US keine Bereitschaft bestehen, die Geeignetheit des ERP-Systems mit seinen verschiedenen Funktionen so zu amputieren, dass nicht nur der Zugang, sondern auch bereits das technische Sammeln solcher Daten nicht möglich ist. Zu dem kommt, dass diese Art von Datenerfassung in den USA völlig unproblematisch möglich ist.

[15] Taeger/ Gabel (Hrsg.), BDSG, 2010, § 4 c Rn. 3.
[16] Simitis (Hrsg.); a. a. O. § 4 Rn. 11 und 16.
[17] BAG, BB 1986, S. 2333.

Es bleibt der Ausweg, sich von dem Datenimporteur, also Steel US, verbindlich erklären zu lassen, dass sie lediglich die in der Betriebsvereinbarung benannten Daten zu den dort ebenfalls benannten Zwecken nutzen wird und keine weiteren Daten von Arbeitnehmern bei Steel D aus dem ERP-System auslesen werde, die zu einer Leistungs- und/oder Verhaltenskontrolle geeignet sind. Dies kann dergestalt geschehen, dass das datenimportierende Unternehmen, Steel US, die Betriebsvereinbarung als auch für sich verbindlich anerkennt.

Allein diese Selbstverpflichtung wird aber noch nicht genügen. Stattdessen wird der Betriebsrat zur Wahrnehmung seiner Schutzpflichten für die Arbeitnehmer ein Kontrollrecht bei dem datenexportierenden Arbeitgeber etablieren wollen.

Wenn diese beiden Pflichten der datenimportierenden Stelle und des Arbeitgebers, also Verpflichtung zur Nichtverwendung von Leistungs- und Verhaltensdaten sowie zu einer Kontrollmöglichkeit des Betriebsrates in der Betriebsvereinbarung geregelt sind, kann dies auch verbindlich für die datenimportierende Unternehmung werden, wenn diese die Betriebsvereinbarung auch für sich rechtlich verbindlich akzeptiert in Gestalt eines entsprechenden Schreibens an das datenexportierende Unternehmen.

2.3.3. Welche Regelungen sind beispielsweise in eine solche Betriebsvereinbarung aufzunehmen?

- Vertragsrubrum mit dem Zweck der Betriebsvereinbarung
- Gegenstand der Betriebsvereinbarung, §§ 80 Abs. 1 Nr. 1, 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz
- Art der Daten (ggf. auf eine Anlage mit den benannten Daten verweisen) und

  Zweck der Datenverarbeitung
- Zugangsberechtigung zu den Arbeitnehmerdaten
- Zweckbindung
- Ausschluss einer Weiterübertragung an Dritte
- Widerrufsrecht des einzelnen Arbeitnehmers
- Verantwortliche Stelle (Hier wäre Steel US aufgrund der Selbstverpflichtung in ihrer eigenen Data Privacy Policy neben dem Arbeit-

geber, Steel D, als weitere Verantwortliche Stelle aufzuführen sowie die Data Privacy Policy selbst zum Bestandteil der Betriebsvereinbarung in einer Anlage zur Betriebsvereinbarung zu machen). Der Arbeitgeber bleibt auf jeden Fall weiterhin Verantwortliche Stelle.

- Aufrechterhaltung der Safe Harbor Registrierung (ein Ausdruck der bestehenden Registrierung sollte als Anlage zur BV genommen werden)
- Selbständiges Auskunftsrecht der Arbeitnehmer des Datenexporteurs direkt auch gegenüber dem Datenimporteur
- Kontrollrecht des Betriebsrates (zumindest beim deutschen Arbeitgeber)
- Information der Arbeitnehmer über die Betriebsvereinbarung (durch beide, den Datenexporteur und –importeur)[18]
  - Kooperation mit den EU-europäischen Datenschutzbehörden seitens des Datenimporteurs, also Steel US
  - Laufzeit der Betriebsvereinbarung
  - Anlagen, z. B.
    - Art der Daten
    - Zweck der Datennutzung
    - Data Privacy Policy des Datenimporteurs
    - Safe Harbor Registrierung des Datenimporteurs
    - Selbstverpflichtung des Datenimporteurs (hierzu unten)

- Die Betriebsvereinbarung selbst sowie auch alle Anlagen sollten jeweils sowohl deutsch- als auch englischsprachig vorliegen. Aus Beratersicht wird der Datenimporteur in der Selbstverpflichtung die Regelung aufnehmen, dass bei sprachlichen Zweifeln die englischsprachige Fassung Vorrang hat.

2.4. Inhalt des Selbstverpflichtungsschreibens des Datenimporteurs

[18] Beschluss der obersten Aufsichtsbehörde für den Datenschutz im nicht öffentlichen Bereich am 28./29.04.2010

2.4.1 In der Unternehmensrealität im internationalen Umfeld ist die Schaffung eines Verständnisses bereits nur für das Anliegen des deutschen und EU-europäischen Datenschutzrechts nicht wirklich gut vermittelbar. In der US-amerikanischen Rechtskultur ist Data Privacy nicht Ausfluss aus dem Persönlichkeitsrecht als Grundrecht, sondern schlicht wettbewerbsrechtliche Grenze in dem Sinn, dass ein unangemessener Umgang mit personenbezogenen Daten wettbewerbswidrig sein kann. Für diese Fälle hat dann aber die Federal Trade Commission (FTC) als Aufsichtsbehörde sehr scharfe Sanktionsmöglichkeiten. Die Kommunikation bedarf also der Geduld und auch eines großen Aufwandes zur Einholung der erforderlichen, insbesondere aber auch dokumentierten Erklärungen zur Selbstverpflichtung des Datenimporteurs.

2.4.2 Eine Selbstverpflichtung des Datenimporteurs ist eine solche schwierige Angelegenheit.[19] Ohne diese Selbstverpflichtung des Datenimporteurs würde man nicht zu einer Betriebsvereinbarung kommen. Auch das Management des deutschen Datenexporteurs wird nicht datenschutz-compliant handeln, wenn diese Erklärungen des Datenimporteurs nicht vorliegen. Ich schlage deshalb zum Vorgehen als Reihenfolge vor:

- Ausarbeitung der Details einer Betriebsvereinbarung inkl. der gewollten Erklärungen und Selbstverpflichtungen des Datenimporteurs
- Abstimmung hierüber zwischen dem Management des Datenexporteurs und dem zuständigen Officer beim Datenimporteur
- Ergänzung oder Abänderung der Data Privacy Policy des Datenimporteurs anhand der Safe Harbor Privacy Principles und der FAQs, soweit dies erforderlich ist
- Zur möglichen eigenen haftungsrechtlichen Absicherung: Anonymisierte Rücksprache mit der Aufsichtsbehörde zum verfolgten Konzept (ausgesprochen positive Erfahrungen beim Bayerischen Landesamt für Datenschutz-aufsicht)
- Aufsetzen der Selbstverpflichtungserklärung zwischen Datenexporteur und –importeur und anschließende Abstimmung mit dem Betriebsrat
- Erforderliche Übersetzungen, damit alle Dokumente zweisprachig vorliegen

[19] Vgl. hierzu Arbeitsbericht, aa. O., S. 9; Taeger/ Gabel, aa. O. § 4 c, Rn. 33.

- Erhalt der finalen Fassung der Selbstverpflichtungserklärung des Datenimporteurs, die in Kopie zur Betriebsvereinbarung genommen wird.
- Unterschrift unter die Betriebsvereinbarung

2.5. Keine Genehmigungspflicht der Aufsichtsbehörden?

Das BDSG verfolgt den Ansatz, dass gem. § 4 b Abs. 5 BDSG auch bei einer Datenweitergabe die Verantwortung bei der Verantwortlichen Stelle bleibt, im Beispielsfall also bei Steel D als Arbeitgeber. [20]

Soweit eine Datenübermittlung ins Ausland nach § 4 b oder § 4 c Abs. 1 BDSG zulässig ist, bedarf die Datenübermittlung nicht der Genehmigung der Aufsichtsbehörde, wie sich aus § 4 c Abs. 2 BDSG im Umkehrschluss ergibt[21]. Ähnlich wie bei der Selbstzertifizierung des Safe Harbor registrierten US-Unternehmens obliegt es also auch nach deutschem Datenschutzrecht der Verantwortlichen Stelle, die Voraussetzungen für eine zulässige Datenübermittlung ins Ausland zu erfüllen. Die Aufsichtsbehörde kann aber das Vorliegen der Voraussetzungen kontrollieren.

Die fehlende Genehmigungspflicht ist ein wesentliches Argument für den Abbau von Widerständen, wie ich sie in der Regel bei US-amerikanischen Inhouse-Anwälten feststelle. Das soll nicht die Chance für eine Umgehung bedeuten. Es entfällt aber auf der amerikanischen Seite der Eindruck eines Kontrolliertwerdens von anderer staatlicher Stelle.

3. Schlussfolgerung

Ohne guten Willen aller Beteiligter geht es nicht. Insbesondere bei einem europäischen Konzernbetriebsrat kann sich der Abstimmungsbedarf vervielfachen.

Auf die Sinnhaftigkeit dieser Schutzvorkehrungen angesprochen, ist mir die beschränkte Chance einer echten Umsetzung des Datenschutzes bekannt. Diese Position nahm im Beispielsfall der Betriebsrat ein. Wenn aber keine Vorkehrungen zum Arbeitnehmerdatenschutz getroffen würden, sondern man es einfach bei der Praxis des Zugriffs auf Arbeitnehmerdaten über das ERP-System

[20] Tager// Gabel, aa. O, § 4 b Rn. 28
[21] Taeger/ Gabel, aa. O; § 4 c Rn. 15.

belassen würde, wäre dies sicherlich ein Bärendienst für den Datenschutz, da der Anspruch auf einen Schutz der Arbeitnehmerdaten aufgegeben würde. Dies kann nicht im Sinne der Arbeitnehmer sein, aber auch nicht in dem eines aufgeklärten Managements, das den Betriebsfrieden auch durch Transparenz sicherstellen will.

München, den 14.07.2013

Dr. Oliver M. Habel

4. Literatur

- *Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Konzerninterner Datentransfer" des Düsseldorfer Kreises (nachfolgend „Arbeitsbericht"), 11.01.2005*
- *Taeger/ Gabel (Hrsg.), Kommentar zum BDSG, Frankfurt am Main 2010*
- *Simitis (Hrsg.), Bundesdatenschutzgesetz, 7. Auflage, Frankfurt am Main 2011*
- *Gola/ Schomerus, BDSG, 11. Auflage, Bonn 2012*