Arbeitnehmerdatenschutz vor der Reform – Fehlanzeige?

Von Dr. **Michael Schmidl**, München

„Siemens lässt sensible Personaldaten künftig von einem US-Unternehmen verwalten." So ist in der Online-Ausgabe der Süddeutschen Zeitung vom 18.9.2009[1] im Hinblick auf die Einführung einer konzernweiten HR-Datenbank des amerikanischen Anbieters „Success Factors" zu lesen. Im gleichen Beitrag wird die Arbeitnehmervertretung von Siemens mit den Worten zitiert: „Die Folgen eines solchen Schritts sind schwer zu überschauen." Derartige Berichte verstellen den Blick darauf, dass die Einführung internationaler HR-Systeme grundsätzlich datenschutzrechtlich zulässig gestaltet werden kann. Betriebliche Datenschutzbeauftragte und Betriebsräte versuchen, wohl veranlasst durch die gegenwärtige Diskussion über die angeblich eklatanten Schutzdefizite für Arbeitnehmerdaten, die Übermittlung von Arbeitnehmerdaten ins Ausland mit datenschutzrechtlichen Argumenten zu verhindern. Der nachfolgende Beitrag richtet sich an Studierende aller Fakultäten und Semester. Er erläutert einige Grundprinzipien des Arbeitnehmerdatenschutzes und zeigt damit zugleich, dass die allgegenwärtige Diskussion über die Schutzdefizite für Arbeitnehmerdaten nicht uneingeschränkt berechtigt ist.

I. Einleitung

Aus datenschutzrechtlicher Sicht geht es den deutschen Arbeitnehmerinnen und Arbeitnehmern schlecht. Dieser Eindruck könnte zumindest entstehen, wenn man die seit Jahren und in den letzten Monaten mit besonderer Intensität geführte Diskussion zum Arbeitnehmerdatenschutz betrachtet. Auf der Homepage des Bundesbeauftragten für den Datenschutz ist unter anderem zu lesen, dass Arbeitnehmer und Arbeitgeber im Wesentlichen darauf angewiesen sind, sich „wegen fehlender gesetzlicher Regelungen zum Arbeitnehmerdatenschutz" an der einschlägigen, notwendigerweise lückenhaften und für die Betroffenen nur schwer erschließbaren Rechtsprechung zu orientieren.[2] Mit der am 1.9.2009 in Kraft getretenen Vorschrift des § 32 BDSG (Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses) dürfte sich dieser Zustand kaum geändert haben. § 32 BDSG soll lediglich eine Zusammenfassung bisheriger Prinzipien zum Arbeitnehmerdatenschutz enthalten:[3]

> „§ 32 enthält eine allgemeine Regelung zum Schutz personenbezogener Daten von Beschäftigten, die die von der Rechtsprechung erarbeiteten Grundsätze des Datenschutzes im Beschäftigungsverhältnis nicht ändern, sondern lediglich zusammenfassen und ein Arbeitnehmerdatenschutzgesetz weder entbehrlich machen noch inhaltlich präjudizieren soll."

Auch wenn die Notwendigkeit spezieller Regelungen (in Gestalt eines Arbeitnehmerdatenschutzgesetzes) zum Arbeitnehmerdatenschutz[4] kaum noch[5] bestritten wird, darf durch die einschlägige Diskussion nicht der Eindruck entstehen, die aktuelle gesetzliche Regelung sei völlig unzureichend. Die „Datenschutzskandale" der vergangenen Jahre haben gemeinsam, dass sie mehrheitlich nicht auf fehlende gesetzliche Vorschriften zurückgeführt werden können. Im Hinblick auf das geltende Recht kann allerdings von einem gewissen Defizit in der Anwendung gesprochen werden.[6] Dieses Defizit schlägt sich beispielsweise in der Bußgeldpraxis der Behörden nieder. Spektakuläre Bußgeldentscheidungen sind im Bereich des Datenschutzrechts eher einer Seltenheit,[7] auch wenn im Jahr 2008 wegen der Verletzung datenschutzrechtlicher Vorschriften, unter anderem zum Nachteil der eigenen Arbeitnehmer, gegen verschiedene Vertriebsgesellschaften der Lebensmittelkette Lidl Bußgelder von insgesamt ca. EUR 1,5 Millionen verhängt und diesen verschiedene Auflagen gemacht wurden.[8] Die „Sanktionswirkung" von Verletzungen des Datenschutzrechts geht derzeit eher von der öffentlichen Meinung aus, wie unter anderem der Fall von Hartmut Mehdorn zeigt.[9]

Ungeachtet der aktuellen Diskussion um Schutzlücken für Arbeitnehmerdaten ist auch das derzeit geltende Datenschutzrecht bei konsequenter Anwendung und unter Berücksichtigung der zahlreichen Vorgaben der Aufsichtsbehörden geeignet, einen angemessenen Schutz von personenbezogenen Daten von Arbeitnehmern zu bewirken. Dies lässt sich am Beispiel der datenschutzrechtlichen Anforderungen an die Übermittlung von Arbeitnehmerdaten im Konzern verdeutlichen. Beispiele für die Übermittlung von Arbeitnehmerdaten im Konzern gibt es zuhauf. Für eine amerikanische Muttergesellschaft mit deutscher Tochtergesellschaft beispielsweise ist

---

[1] http://www.sueddeutsche.de/wirtschaft/870/482333/text/

[2] Vgl. http://www.bfdi.bund.de/nn_530440/DE/Themen/Arbeit/Arbeitnehmerdatenschutz/Artikel/Arbeitnehmerdatenschutzgesetz.html (abgerufen am 23.9.2009).

[3] BT-Drs. 16/13657, S. 35.

[4] Für die Schaffung einer speziellen gesetzlichen Regelung haben sich ausgesprochen: Peter Schaar (Bundesbeauftragter für den Datenschutz) und der Deutsche Gewerkschaftsbund, vgl. becklink 281510 unter http://beck-online.beck.de/?VPATH=bibdata%2Freddok%2Fhp.10%2F281510.htm (abgerufen am 23.9.2009).

[5] Stimmen gegen ein Arbeitnehmerdatenschutzgesetz vgl. becklink 281510 unter http://beck-online.beck.de/?VPATH=bibdata%2Freddok%2Fhp.10%2F281510.htm (abgerufen am 23.9.2009).

[6] Siehe http://www.compliancemagazin.de/plaintext/gesetzestandards/ deutschland/bundestagbundesregierung/deutschebundesregierung050608.html (abgerufen am 23.9.2009).

[7] Zur Höhe von Bußgeldern kritisch *Simitis*, Das Parlament (8.12.2008), unter http://www.bundestag.de/presse/pressemitteilungen/2008/pm_0812051.html (abgerufen am 23.9.2009).

[8] Vgl. dazu Pressemitteilung des Innenministeriums Baden-Württemberg vom 11.9.2008, http://www.innenministerium.baden-wuerttemberg.de/fm7/2028/Lidl%20%20Bu%DFgeldverfahren%20abgeschlossen.470204.pdf (abgerufen am 23.9.2009).

[9] Zur Bahnaffäre vgl. *Diller*, BB 2009, 438 und Erwiderung *Steinkühler*, BB 2009, 1294.

die Zugriffsmöglichkeit auf folgende Auswahl von Personaldaten deutscher Mitarbeiter absolut typisch: Vorname und Nachname, Personalnummer, Geburtsdatum, Geschlecht, Privatadresse, Telefonnummern (Privat- und Mobilnummer), Notfallkontakt, Lebenslauf mit elektronischen Kopien von Zeugnissen, Qualifikationen (Ausbildung, Sprachen, Berufserfahrung etc.), Abteilung, Name des direkten Vorgesetzten, Arbeitszeit pro Woche (Vollzeit, Teilzeit), Gehalt und sonstige Vergünstigungen, Historie der Gehaltserhöhungen, Steuernummer, Beginn des Beschäftigungsverhältnisses, Anzahl genommener Urlaubstage, Leistungsbeurteilungen, Disziplinarmaßnahmen, Kommentare von Vorgesetzten zu besonderen Fähigkeiten.

Die wichtigsten Gründe für diese umfassende Datenhaltung bei einer bestimmten Hauptgesellschaft (häufig bei der Muttergesellschaft) liegen in der Organisationsstruktur moderner internationaler Konzerne. Diese ist dadurch geprägt, dass bestimmte zentrale Funktionen bei einer oder mehreren Konzerngesellschaften gebündelt und zugleich bei den anderen Konzerngesellschaften abgeschafft oder auf einen minimalen Umfang beschränkt werden. Die Bündelung bestimmter Funktionen führt zu Synergieeffekten. Dies lässt sich am Beispiel der konzerneinheitlichen Vergütungsstruktur verdeutlichen. Gehälter und Zulagen werden zentral und einheitlich, zugleich aber unter Berücksichtigung bestimmter lokaler Besonderheiten, anhand eines Bewertungsschemas bestimmt. Auf diese Weise werden konzernweite Transparenz und Nachvollziehbarkeit erreicht. Die Erreichung der gleichen Transparenz und Nachvollziehbarkeit durch ein entsprechendes Tätigwerden der jeweiligen Tochtergesellschaften wäre ungleich aufwendiger. Ein weiteres Beispiel ist die Zusammenstellung von Teams mit bestimmten Kompetenzen, um besonderen Herausforderungen (z.B. die Durchführung eines komplexen internationalen Projekts für einen wichtigen Kunden) gerecht werden zu können. Nur aus der übergeordneten Perspektive derjenigen Gesellschaft, bei der alle wesentlichen Personaldaten vorhanden sind, kann eine solche Aufgabe sinnvoll bewältigt werden. Selbst wenn sich über komplexe Abstimmungsprozesse auch bei diesem Beispiel noch eine Erledigung auf der Ebene der Tochtergesellschaften denkbar wäre, so lässt sich zumindest nicht leugnen, dass der zu betreibende Aufwand und die damit einhergehenden Kosten ungleich höher wären. Schließlich bringt es die Funktionskonsolidierung mit sich, dass es häufig Vorgesetzte in einer Konzerngesellschaft gibt, die für Mitarbeiter in verschiedenen anderen Konzerngesellschaften die Personal- und Führungsverantwortung haben. Für einen Konzern, innerhalb dessen die Führungsfunktionen in der beschriebenen Weise verteilt sind, hat sich die Bezeichnung „Matrixorganisation“[10] eingebürgert. Bisweilen wird der Vorgesetzte, der die Personal- und Führungsverantwortung für Mitarbeiter aus unterschiedlichen Konzerngesellschaften trägt, auch als „Matrixvorgesetzter“ bezeichnet.

Die „Matrix“ als immer mehr zur Regel werdende Organisationsform von Konzernen geht mit zahlreichen Datenübermittlungen von der den Arbeitsvertrag schließenden Gesellschaft an andere Konzerngesellschaften einher und soll im vorliegenden Beitrag als Testfall für das geltende Arbeitnehmerdatenschutzrecht dienen (II.). Im Ergebnis wird zu zeigen sein, dass sich aus dem geltenden Recht, konkretisiert durch Vorgaben der Aufsichtsbehörden zur Übermittlung von Arbeitnehmerdaten im Konzern,[11] auch ohne ein spezielles Arbeitnehmerdatenschutzgesetz ein geschlossenes Schutzsystem für Arbeitnehmerdaten ergibt (III.). Im Anschluss an eine Zusammenfassung (IV.) wird die aktuelle Diskussion zu den für ein Arbeitnehmerdatenschutzgesetz geforderten Inhalten in Form eines Ausblicks kommentiert (V.).

II. Datenschutz im Konzern und Matrixorganisationen

Die Übermittlung von personenbezogenen Daten zwischen Konzerngesellschaften wird vom deutschen Datenschutzrecht grundsätzlich nicht anders behandelt als sonstige Datenübermittlungen. Datenschutz im Konzern ist zu einem wesentlichen Teil von diesem Grundsatz geprägt, der unter anderem in der Verneinung des so genannten Konzernprivilegs (1.) zum Ausdruck kommt. Wie bereits in der Einleitung beschrieben, sind international präsente Konzerne ungeachtet des fehlenden Konzernprivilegs heute mehrheitlich in Form einer Matrix organisiert. Charakteristisch für diese Organisationsform ist unter anderem der Austausch von Mitarbeiterdaten zwischen Muttergesellschaft und Tochtergesellschaften sowie zwischen den Tochtergesellschaften untereinander (2.).

1. Kein Konzernprivileg

Das bis zur Schaffung eines Spezialgesetzes zum Arbeitnehmerdatenschutz in vielen Fragen[12] maßgebliche Bundesdatenschutzgesetz ist nicht auf die Datenverarbeitung im Konzern zugeschnitten.[13] Der Gesetzgeber hat sich sogar ausdrücklich gegen ein „Konzernprivileg“ entschieden.[14] Dies wird im Hinblick auf die Definition der Datenübermittlung gemäß §§ 3 Abs. 4 S. 2 Nr. 3 i.V.m. Abs. 8 S. 2 BDSG deutlich:

[10] Zum Begriff der „Matrixorganisation“ vgl. *Picot/Dietl/Franck*, Organisation, 5. Aufl. 2008, S. 255.

[11] Vgl. dazu u.a. Hinweise zum Datenschutz Nr. 39 des Innenministeriums Baden-Württemberg (http://www.innenministerium.baden-wuert-temberg.de/fm/1227/him_39.pdf (abgerufen am 23.9.2009).

[12] Bereichsspezifische Regelungen enthalten z.B. § 11 ff. TMG; vgl. dazu *Spindler/Schuster*, Recht der elektronischen Medien, 2008, § 11 TMG und *BITKOM*, Leitfaden: Die Nutzung von E-Mail und Internet im Unternehmen, 2004 unter http://www.bitkom.org/files/documents/BITKOM_Leitfaden_Email_u._Internet_im_Unternehmen_Version_1_3(1).pdf (abgerufen am 23.9.2009).

[13] Vgl. *Simitis*, in: Simitis, Kommentar zum BDSG, 2006, § 2 Rn. 143.

[14] Vgl. dazu auch *Ruppmann*, Der konzerninterne Austausch personenbezogener Daten: Risiken und Chancen für den Datenschutz, 2002.

§ 3 Abs. 4 S. 2 Nr. 3:
„[…] (4) Verarbeiten ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im Einzelnen ist, ungeachtet der dabei angewendeten Verfahren: […] 3. Übermitteln das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass a) die Daten an den Dritten weitergegeben werden oder b) der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft […]"

§ 3 Abs. 8 S. 2:
„[…] Dritter ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. […]"

Auf Grundlage dieser Definition ändert die Zugehörigkeit zum gleichen Konzern nichts am Vorliegen einer Übermittlung, wenn Arbeitnehmerdaten zwischen Konzernunternehmen ausgetauscht werden. Lediglich die Weitergabe von Arbeitnehmerdaten an Auftragsdatenverarbeiter innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums ist keine Übermittlung gemäß § 3 Abs. 4 S. 2 Nr. 3 BDSG, weil solche Auftragsdatenverarbeiter gemäß § 3 Abs. 8 S. 3 BDSG[15] nicht Dritte sind.[16] Hintergrund dieser Regelung ist, dass der Auftraggeber gemäß § 11 Abs. 1 S. 1 BDSG[17] für die Einhaltung der Vorschriften des BDSG und anderer Vorschriften über den Datenschutz verantwortlich bleibt. Der Auftraggeber hat den Auftragsdatenverarbeiter unter besonderer Berücksichtigung der Eignung der von ihm getroffenen technischen und organisatorischen Maßnahmen auszuwählen und sich von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Der Auftrag ist gemäß § 11 Abs. 2 S. 2 BDSG zwingend schriftlich zu erteilen und hat bestimmte Regelungen zu beinhalten.[18] Diese Gestaltung wäre auch im Konzern denkbar, indem beispielsweise die nicht-europäische Muttergesellschaft als Auftragsdatenverarbeiterin ihrer weltweiten Tochtergesellschaften agiert. In der Praxis ist diese Vorgehensweise allerdings nicht leicht umsetzbar. Häufig ist es beispielsweise nicht mit dem Selbstverständnis und den Zielen der Muttergesellschaft zu vereinbaren, ausschließlich nach Maßgabe der Weisungen ihrer Tochtergesellschaften und zur Erreichung von deren Zwecken zu handeln. Im Lichte dessen, dass die in § 3 Abs. 8 S. 3 BDSG angelegte Privilegierung, wie beschrieben, auf in der Europäischen Union oder dem Europäischen Wirtschaftsraum ansässige Auftragsdatenverarbeiter beschränkt ist,[19] müssen zudem auch für die Weitergabe der Daten an die nicht-europäische Muttergesellschaft als Auftragsdatenverarbeiterin die Voraussetzungen einer zulässigen Übermittlung[20] vorliegen.

Die Vornahme einer Übermittlung löst gemäß § 4 Abs. 1 BDSG[21] wiederum das Erfordernis eines Erlaubnistatbestandes aus. Die zentralen Erlaubnistatbestände für Arbeitnehmerdaten sind § 32 Abs. 1 S. 1 BDSG (Erforderlichkeit für die Durchführung des Beschäftigungsverhältnisses) und § 28 Abs. 1 S. 1 Nr. 2 BDSG (Erforderlichkeit zur Erreichung eines berechtigen Interesses des Arbeitgebers und keine überwiegenden schutzwürdigen Interessen der Arbeitnehmer). Die am 1.9.2009 in Kraft getretene Vorschrift des § 32 Abs. 1 S. 1 BDSG[22] hat folgenden Wortlaut:

---

[15] § 3 Abs. 8 S. 3 BDSG lautet: „Dritte sind nicht der Betroffene sowie Personen und Stellen, die im Inland, in einem anderen Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum personenbezogene Daten im Auftrag erheben, verarbeiten oder nutzen."

[16] Hierzu *Dammann*, in: Simitis, Kommentar zum BDSG, 2006, § 3 Rn. 244.

[17] § 11 Abs. 1 S. 1 BDSG lautet: „Werden personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt, ist der Auftraggeber für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz verantwortlich."

[18] Gemäß § 11 Abs. 2 S. 2 BDSG sind im insbesondere im Einzelnen festzulegen: 1. der Gegenstand und die Dauer des Auftrags, 2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen, 3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen, 4. die Berichtigung, Löschung und Sperrung von Daten, 5. die nach Abs. 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen, 6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen, 7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers, 8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen, 9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält, 10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags."

[19] Vgl. *Gola/Schomerus,* Kommentar zum BDSG, 2007, § 11 Rn. 16.

[20] Dazu auch *Räther/Seitz*, MMR 2002, 425.

[21] § 4 Abs. 1 BDSG lautet: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind nur zulässig, soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat."

[22] Zu beachten ist, dass § 32 Abs. 1 S. 1 BDSG im Beschäftigungsverhältnis an die Stelle von § 28 Abs. 1 S. 1 Nr. 1 BDSG tritt. Die Gesetzesbegründung (BT-Drs. 16/13657, S. 34 f.) dazu lautet: „In einem neuen § 32 wird § 28 Absatz 1 Satz 1 Nummer 1 im Hinblick auf Beschäftigungsverhältnisse konkretisiert und insoweit verdrängt. Ebenfalls durch § 32 verdrängt wird § 28 Absatz 1 Satz 2: § 32 regelt, zu welchen Zwecken und unter welchen Voraussetzungen personenbezogene Daten vor, im und nach dem Beschäftigungsverhältnis erhoben, verarbeitet und genutzt werden dürfen. Einer weiteren konkreten Festlegung der Zwecke nach § 28 Absatz 1 Satz 2 durch Arbeitgeber bedarf es daher nicht mehr. Die übrigen einschlägigen allgemeinen und be-

> „§ 32. Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses. (1) Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist."

Der neben § 32 BDSG anwendbare[23] § 28 Abs. 1 S. 1 Nr. 2 BDSG lautet wie folgt:

> „§ 28. Datenerhebung und -speicherung für eigene Geschäftszwecke. (1) Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig, […] 2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt […]."

Häufig wird man zu dem Ergebnis kommen, dass die Übermittlung von Personaldaten im Konzern nicht zwingend für die Durchführung des Beschäftigungsverhältnisses erforderlich ist, d.h. dem Maßstab des § 32 Abs. 1 S. 1 BDSG nicht gerecht wird. Dies gilt insbesondere für Fälle, in denen sich die Matrixstruktur erst nach Begründung des Beschäftigungsverhältnisses ergeben hat – etwa durch einen Unternehmenskauf –, weil die bisherige Durchführung des Beschäftigungsverhältnisses dann als (im Hinblick auf die Wandelbarkeit einer Erforderlichkeitsbetrachtung nicht vollständig überzeugender) Beweis für die fehlende Erforderlichkeit der internationalen Datenübermittlungen herangezogen werden kann. In solchen Fällen kann auf § 28 Abs. 1 S. 1 Nr. 2 BDSG zurückgegriffen werden. Bei der Prüfung der Tatbestandsvoraussetzungen kann sich die Konzernzugehörigkeit des gewünschten Empfängers zwar in der Interessensabwägung gemäß § 28 Abs. 1 S. 1 Nr. 2 BDSG mittelbar positiv auswirken,[24] etwa wegen im Konzern bestehender einheitlicher technischer Schutz- und Verarbeitungsstandards. Im Grunde genommen, muss die Datenübermittlung im Konzern aber an den gleichen Maßstäben gemessen werden, wie die Übermittlung an beliebige Dritte.[25] Soll die Übermittlung zur Erfüllung bestimmter Interessen der Muttergesellschaft erfolgen, beispielsweise weil diese eine zentrale HR-Datenbank einführen will, so ist dies gemäß § 28 Abs. 2 Nr. 2 a) BDSG[26] nur dann zulässig, wenn kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat.[27]

Im Vergleich zu § 28 Abs. 1 S. 1 Nr. 2 BDSG, der den Ausgleich zwischen berechtigten Interessen der verantwortlichen Stelle und schutzwürdigen Interessen des Betroffenen im Wege der Interessenabwägung („[…]das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung *überwiegt*[…]") zulässt, ist der in § 28 Abs. 2 Nr. 2 a) BDSG enthaltene Maßstab schwieriger zu erfüllen. Bereits die Existenz eines entgegenstehenden Interesses steht der Rechtfertigung einer Maßnahme auf Grundlage von § 28 Abs. 2 Nr. 2 a) BDSG entgegen. Durch diesen unterschiedlichen Maßstab ist sichergestellt, dass Drittinteressen die durch das Schuldverhältnis gesteckten Verarbeitungsgrenzen nur in engen Grenzen verlagern können. Dies gilt jedenfalls dann, wenn sich ein Interesse der Muttergesellschaft nicht zugleich als Interesse der Tochtergesellschaft darstellt, so dass ungeachtet der interessensmäßigen Betroffenheit der Muttergesellschaft § 28 Abs. 1 S. 1 Nr. 2 BDSG zur Anwendung kommen kann. Für das Arbeitsverhältnis trägt die in § 28 Abs. 1 S. 1 Nr. 2 und Abs. 2 Nr. 2 a) BDSG angelegte Unterscheidung und die daraus folgende Nachrangigkeit von Interessen der Muttergesellschaft dem Umstand Rechnung, dass zwischen dem Dritten (z.B. der Muttergesellschaft) und dem Betroffenen (z.B. dem Arbeitnehmer) kein Vertragsverhältnis besteht.[28]

Aus datenschutzrechtlicher Sicht sind „herkömmliche" Unternehmensstrukturen, die durch verschiedene innerhalb eines Unternehmens gebündelte Führungsebenen gekennzeichnet sind, in der Folge leichter abzubilden, als die dezentral organisierten Matrixorganisationen.[29] Die sogenannten „herkömmlichen" Unternehmensstrukturen sind durch verschiedene bereichsspezifische Pyramidenstrukturen sowie eine bereichsübergreifende Gesamthierarchie innerhalb eines Rechtsträgers geprägt. Bereichsspezifische Pyramidenstrukturen kommen beispielsweise für die Unternehmensfunktionen Produktmanagement, Einkauf, Produktion, Qualitätskontrolle, Marketing, Vertrieb, Public Relations, IT, Buchhaltung, Controlling, Recht und Compliance in Betracht. Die entsprechenden Abteilungen unterstehen, abhängig von der Größe des Unternehmens, einer Abteilungsleitung, die neben unmittelbaren Aufgaben die fachliche Überwachung einer gewissen Anzahl berichtspflichtiger Funktionsträger sicherzustellen hat. Die Funktionsträger in der Abteilungsleitung sehen sich ihrerseits im Rahmen der Gesamthierarchie des Rechtsträgers gewissen der Kontrolle dienenden Berichtspflichten ausgesetzt. Anders als in den zuvor beschriebenen Matrixorganisationen erfordert die Erfüllung der genannten

reichsspezifischen Datenschutzvorschriften, die eine Datenerhebung, -verarbeitung oder -nutzung erlauben oder anordnen, werden durch § 32 nicht verdrängt."

[23] BT-Drs. 16/13657, S. 35.

[24] Dazu auch *Räther/Seitz*, MMR 2002, 425.

[25] Vgl. *Kilian/Heussen*, Computerrechtshandbuch, 2008, 1.7.VI, Rn. 180.

[26] § 28 Abs. 2 Nr. 2 a BDSG lautet: „Die Übermittlung oder Nutzung für einen anderen Zweck ist zulässig: […] 2. soweit es erforderlich ist a) zur Wahrung berechtigter Interessen eines Dritten […] und kein Grund zu der Annahme besteht, dass der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung oder Nutzung hat […]."

[27] Vgl. *Simitis* (Fn. 12), § 28 Rn. 216.

[28] Vgl. auch *Wank*, in: Erfurter Kommentar zum Arbeitsrecht, 2009, § 28 BDSG Rn. 4, 27 ff.

[29] Vgl. dazu auch *Simitis* (Fn. 12), § 4c Rn. 10 ff.

Aufgaben und Berichtspflichten in der Regel lediglich die Erhebung und Nutzung von personenbezogenen Daten der einzelnen Beschäftigten, aber keine Datenübermittlungen an Dritte.

2. Ausgewählte Charakteristika von Matrixorganisationen

Anders als die zuvor erwähnten „herkömmlichen" Unternehmensstrukturen zeichnen sich Matrixorganisationen durch die Zuordnung von Aufgaben und Verantwortlichkeiten hauptsächlich und ausschließlich auf Basis der Geeignetheit für die Erledigung einer Aufgabe aus.[30] Alleine die Geeignetheit für die Erfüllung einer Aufgabe führt zur Zuweisung einer bestimmten Aufgabe an den entsprechenden Arbeitnehmer. Es kommt dabei nicht darauf an, bei welcher Konzerngesellschaft dieser Arbeitnehmer angestellt ist und wo diese ihren Sitz hat. Häufig, wenn auch nicht zwangsläufig, umfassen Matrixorganisationen auch Konzerngesellschaften (z.B. die Muttergesellschaft) in Ländern, die nicht Mitgliedstaaten der Europäischen Union oder des Europäischen Wirtschaftsraums sind. Aus Sicht des BDSG, vgl. § 4b Abs. 2 S. 2 BDSG, hat die Übermittlung in solche Länder grundsätzlich zu unterbleiben, wenn diese nicht über ein angemessenes Datenschutzniveau verfügen und keine Ausnahmeregelung eingreift:

> „§ 4b. Übermittlung personenbezogener Daten ins Ausland sowie an über- oder zwischenstaatliche Stellen. […] (2) […] Die Übermittlung unterbleibt, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den in Satz 1 genannten Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. […]"

Einer der Grundpfeiler von Matrixorganisationen liegt darin, den gesamten Konzern als eine funktionale Einheit anzusehen;[31] die jeweiligen Parteien der arbeitsvertraglichen Beziehungen der einzelnen Mitarbeiter haben aus dieser Perspektive keine Bedeutung. Die von den Konzerngesellschaften als verantwortlichen Stellen (d.h. aus der Perspektive der Mitarbeiter von den Arbeitgebern) verfolgten Zwecke für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten sind daher vom Gedanken der Funktionseinheit geprägt und somit in der Regel vielfältig. Neben den auch für das Arbeitsverhältnis ohne Matrixdimension existierenden, am Ziel der Durchführung des Arbeitsverhältnisses ausgerichteten Zwecken, gibt es für Matrixorganisationen typische Zwecke.[32] Hier sind etwa die weltweite Personalverwaltung und Nachfolgeplanung[33], die Erleichterung der weltweiten (d.h. die Grenzen von Rechtsträgern überschreitende) Zusammenarbeit, insbesondere durch die Bildung von Projektteams aus Mitarbeitern verschiedener Konzerngesellschaften,[34] die konzernweite Herstellung von Lohngerechtigkeit oder die gezielte konzernweite Förderung von Talenten zu nennen.[35] Im Hinblick darauf, dass sich derartige Zwecke nur auf der Basis eines vollständigen Überblicks über die aktuelle Situation in allen Konzerngesellschaften verfolgen lassen, können sie als Konzernzwecke und ihre Erreichung als Konzernfunktion bezeichnet werden. Konzernzwecke sind typischerweise (auch oder ausschließlich) eigene Zwecke der Muttergesellschaft, so dass die erforderlichen Datenübermittlungen von den einzelnen Konzerngesellschaften an die Muttergesellschaft als Übermittlungen zwischen verantwortlichen Stellen einzustufen sind[36] und ihre Erreichung eigene Entscheidungen der Muttergesellschaft erfordern. Weisungen der Tochtergesellschaften an die Muttergesellschaft sind damit unvereinbar. Die Organisationsform der Auftragsdatenverarbeitung (siehe oben) kommt neben der im Konzern häufig schwer vermittelbaren Weisungsunterworfenheit der Muttergesellschaft auch aufgrund der Erforderlichkeit eigener Entscheidungen der Muttergesellschaft nicht in Betracht.

Für Mitarbeiter von Unternehmen, die zu einer Matrixorganisation gehören, ist das Arbeitsumfeld durch eine Vielzahl von Vorgesetzten geprägt. Die Vorgesetzten sind ihrerseits wieder in unterschiedlichen Konzerngesellschaften angestellt und werden häufig als „Matrixvorgesetzte" bezeichnet; sie erhalten die erforderlichen Informationen standortunabhängig über die elektronische Personalakte[37] ihrer jeweiligen Mitarbeiter. Die Existenz von Matrixvorgesetzten in unterschiedlichen Tochtergesellschaften ist dabei logische Folge der konsequent kompetenzorientierten Bildung von Teams und deren jeweiliger Leiter.

Das so entstehende Beziehungsgeflecht wird nicht selten über den Austausch von E-Mails und die Durchführung von Telefon- oder Videokonferenzen aufrechterhalten. Persönliche Treffen, Teambesprechungen oder Feedbackrunden sind in der Regel zwar ein wichtiger Bestandteil solcher virtueller Teams. Es lässt sich andererseits feststellen, dass Unternehmen die damit einhergehenden Kosten, insbesondere Reisekosten, gerade in wirtschaftlich schwierigen Zeiten, zu vermeiden suchen.

Wie noch zu zeigen sein wird, macht es aus Sicht der betroffenen Arbeitnehmer einen Unterschied, ob ihr Arbeitsver-

---

[30] Siehe *Picot/Dietl/Franck* (Fn. 9), S. 256.

[31] Zur Matrixorganisation vgl. *Brickley/Smith/Zimmerman*, Managerial Economics and Organizational Architecture, 3. Aufl. 2004, S. 344 ff.

[32] Vgl. *Schmidl*, WDPR 2009, 17.

[33] Unter Nachfolgeplanung ist die konzernweite und meist langfristig angelegte Analyse eines gewissen Mitarbeiterkreises zu verstehen, um aus diesem Kreis auf Grundlage eines differenzierten Systems von den Betroffenen bekannten und nicht bekannten Bewertungskriterien den aktuellen und künftigen konzernweiten Bedarf an Führungspersonal zu decken. Die Aufnahme in die Nachfolgeplanung wird von den Betroffenen als Chance verstanden und erfolgt in aller Regel – nicht zuletzt wegen der mit gesetzlichen Erlaubnistatbeständen schwer zu rechtfertigenden Fülle der erhobenen Daten – auf Grundlage einer Einwilligungserklärung.

[34] Dazu *v. Sponeck*, CR 1991, 600.

[35] Vgl. dazu auch *Simitis* (Fn. 12), § 28 Rn. 22 ff.

[36] Siehe dazu *Kilian/Heussen* (Fn. 24), 1.7.VI., Rn. 180.

[37] Zu den Eckpunkten der datenschutzrechtlichen Prüfung bei einer elektronischen Personalakte siehe *Bergmann/Möhrle/Herb*, Kommentar zum BDSG, 35. EL 2007, § 28 Rn. 40b.

hältnis bereits anfänglich eine derartige Matrixdimension hatte oder ob sich diese erst nachträglich ergeben hat.[38] Lag eine Matrixdimension bereits bei Abschluss des Arbeitsvertrages vor, so könnte von einem Arbeitsverhältnis mit primärem Konzernbezug gesprochen werden. Ergibt sich eine Matrixdimension erst nach Abschluss des Arbeitsvertrages, so liegt ein Fall des sekundären Konzernbezugs vor.[39]

Vereinfacht lässt sich eine Matrixorganisation[40] wie in *Graphik 1* (siehe unten S. 464) dargestellt skizzieren.

III. Arbeitnehmerdatenschutz in Matrixorganisationen

Vor dem Hintergrund des fehlenden Konzernprivilegs[41] muss die Rechtmäßigkeit für alle in Matrixorganisationen erforderlichen Übermittlungen von Mitarbeiterdaten gesondert geprüft werden.[42] Für die Überprüfung der Rechtmäßigkeit der Übermittlung von personenbezogenen Daten ist gemäß §§ 4 Abs. 1, 4b, 4c, 28, 32 BDSG in zwei Schritten vorzugehen - in der Regel ist daher vom Zwei-Stufen-Test[43] die Rede. Die erste Stufe betrifft die Frage, ob die Übermittlung an sich rechtmäßig ist;[44] hier ist zu prüfen, ob die im BDSG für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten enthaltenen Rechtmäßigkeitsvoraussetzungen eingehalten sind (1.). Auf der zweiten Stufe wird geprüft, ob beim Empfänger der übermittelten Daten ein angemessenes Datenschutzniveau besteht (2.).[45] Die Arbeitnehmereinwilligung könnte auf beiden Stufen wirken,[46] ist allerdings aus verschiedenen Gründen nicht zu empfehlen (3.).[47]

1. Prüfung der Rechtmäßigkeit der geplanten Maßnahme

Auf der ersten Stufe der Überprüfung einer internationalen Datenübermittlung ist zu ermitteln, ob die im BDSG für die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten enthaltenen Rechtmäßigkeitsvoraussetzungen eingehalten sind.[48] Für die Prüfung auf der ersten Stufe bleibt die Frage der Angemessenheit des beim Empfänger bestehenden Datenschutzniveaus grundsätzlich außer Betracht - geprüft wird lediglich, ob die Voraussetzungen eines Erlaubnistatbestands gemäß § 4 Abs. 1 BDSG vorliegen.[49] Für die konzerninterne Übermittlung von Arbeitnehmerdaten kommt § 32 Abs. 1 S. 1 BDSG in Betracht, wenn das Arbeitsverhältnis primären Konzernbezug[50] aufweist und die Übermittlungen daher für dessen Durchführung notwendig sind.[51] Liegt ein Fall sekundären Konzernbezugs vor, so ist regelmäßig auf § 28 Abs. 1 S. 1 Nr. 2 oder auf § 28 Abs. 2 Nr. 2 a) BDSG abzustellen.[52] Für die Zulässigkeit ist in diesen Fällen (§ 28 Abs. 1 S. 1 Nr. 2 BDSG) ein berechtigtes Interesse des Arbeitgebers erforderlich und es dürfen keine überwiegenden Interessen der Arbeitnehmer am Unterbleiben der Übermittlung bestehen. Dient die Übermittlung dem berechtigten Interesse eines Dritten (z.B. der Muttergesellschaft), so darf kein Grund zur Annahme bestehen, dass ein Betroffener ein entgegenstehendes schutzwürdiges Interesse hat (§ 28 Abs. 2 Nr. 2 a) BDSG).[53]

Für die Anwendung dieser gesetzlichen Erlaubnistatbestände spielen die vom Düsseldorfer Kreis (einem Gremium aus den obersten Datenschutzaufsichtsbehörden der Länder für den nicht-öffentlichen Bereich, die zum Zweck der einheitlichen Anwendung des BDSG in Deutschland Entschließungen fassen) formulierten besonderen Schutzanforderungen eine entscheidende Rolle.[54] Der Düsseldorfer Kreis geht von der Prämisse aus, dass das allgemeine Interesse an einer arbeitsteiligen Zusammenarbeit der Konzernunternehmen nicht per se höher zu bewerten ist, als das Interesse der betroffenen Arbeitnehmer am Verbleib ihrer Daten beim Arbeitgeber. Demnach müssen die für Fälle sekundären Konzernbezugs einschlägigen Erlaubnistatbestände § 28 Abs. 1 S. 1 Nr. 2 und § 28 Abs. 2 Nr. 2 a) BDSG unter Berücksichtigung der grundlegenden Entscheidungen eines jeden Individualarbeitsvertrages und der Kernverpflichtungen der Arbeit-

[38] Vgl. *Gola/Schomerus* (Fn. 18), § 28 Rn. 10.
[39] Vgl. *Gola/Schomerus* (Fn. 18), § 4c Rn. 6.
[40] Zur Strukturierung von Matrixorganisationen nach Objekt- und Verrichtungsprinzip sowie der resultierenden Mehrfachunterstellung siehe *Picot/Dietl/Franck* (Fn. 9), S. 255 f.
[41] Siehe oben Ziff. II. 1.
[42] Vgl. zur Inexistenz eines Konzernprivilegs auch *Simitis* (Fn. 12), § 2 Rn. 159.
[43] Zur Begrifflichkeit siehe Positionspapier des Düsseldorfer Kreises vom 19./20. April 2007, I.5., unter https://www.ldi.nrw.de/mainmenu_Service/submenu_Entschliessungsarchiv/Inhalt/Beschluesse_Duesseldorfer_Kreis/Inhalt/2007/20070419_Internationaler_Datenverkehr/Positionspapier.pdf (abgerufen am 23.9.2009).
[44] Vgl. Art. 25 Abs. 1 EG-Datenschutzrichtlinie (95/46/EG), http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html (abgerufen am 23.9.2009).
[45] Siehe zum angemessenen Schutzniveau http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm (abgerufen am 23.9.2009).
[46] Vgl. *Simitis* (Fn. 12), § 4a Rn. 83.
[47] Vgl. *Schmidl*, DuD 2007, 756; zur strukturellen Schwäche der Einwilligung im Arbeitsverhältnis vgl. Arbeitspapier Nr. 114 der Art. 29-Gruppe unter http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_de.pdf (abgerufen am 23.9.2009), S. 13.
[48] Siehe dazu *Simitis* (Fn. 12), § 4 Rn. 15.
[49] Vgl. hierzu *Gola/Schomerus* (Fn. 18), § 4 Rn. 5.
[50] Zu den Begriffen des primären und sekundären Konzernbezugs siehe oben Ziff. II. 2.
[51] Vgl. *Simitis* (Fn. 12), § 28 Rn. 211.
[52] Siehe Positionspapier „Abgestimmte Positionen der Aufsichtsbehörden in der AG Internationaler Datenverkehr'" (12./13.2.2007) unter http://www.lfd.m-v.de/dschutz/ddk/int-daten.html (abgerufen am 23.9.2009).
[53] Siehe auch Art. 26 Richtlinie 95/46/EG unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html.
[54] Die veröffentlichten Entschließungen des Düsseldorfer Kreises sind zu finden unter http://www.bfdi.bund.de/cln_118/DE/Entschlie%C3%9Fungen/DuesseldorferKreis/DKreis_node.html (abgerufen am 23.9.2009).

gebers angewandt werden, da diese Normen keine willkürliche Erweiterung des Verarbeitungsumfangs zulassen, wie er in den Zwecken des Arbeitsvertrages gefasst ist. Die Übermittlung darf nicht darauf hinauslaufen, dass eine Konzerngesellschaft größere Befugnisse erhält, als dies beim Arbeitgeber der Fall ist; es darf kein frei zugänglicher Datenpool entstehen. In der Interessensabwägung gemäß § 28 Abs. 1 S. 1 Nr. 2 BDSG oder der Prüfung von § 28 Abs. 2 Nr. 2 a) BDSG ist zu berücksichtigen und positiv zu gewichten, ob es konzernweite Standards für die Schaffung, Erhaltung und Durchsetzung der Datenschutzrechte des Betroffenen gibt. Die Kernaussage des Düsseldorfer Kreises ist, dass die durch eine Übermittlung von Daten herbeigeführte Diversifizierung der Verantwortlichkeiten kompensiert werden muss. Dies soll dadurch erreicht werden, dass der Arbeitgeber kraft vertraglicher Vereinbarungen mit Wirkung zugunsten Dritter, einer Betriebsvereinbarung[55] oder einer Direktzusage gegenüber den Arbeitnehmern umfassender Ansprechpartner für den Arbeitnehmer bleibt und zudem auch für die Erfüllung der Rechte des Arbeitnehmers auf Auskunft, Löschung, Berichtigung, Sperrung und (grundsätzlich auch) Schadensersatz einstehen muss und zwar zusätzlich zu denjenigen Unternehmen, an welche die Daten übermittelt wurden. Die vertragliche Vereinbarung, häufig auch „Datenschutzkonzept" genannt, mit Wirkung zugunsten Dritter (d.h. der Arbeitnehmer) sollte Regelungen zu folgenden Themen enthalten: Zweckbindung, Datenqualität und Verhältnismäßigkeit, Information der Betroffenen, Sicherheit und Geheimhaltung, Recht auf Auskunft, Berichtigung, Löschung und Widerspruch und zur Handhabung sensibler Daten. Schließlich sind die Arbeitnehmer in nachvollziehbarer Weise zu unterrichten, um eine transparente Gesamtstruktur zu schaffen.[56]

Der Düsseldorfer Kreis hat in einer nicht veröffentlichten Entscheidung aus dem Jahre 2009 von dem Erfordernis eines Datenschutzkonzepts für den Fall Abstand genommen, dass zwischen Arbeitgeber und Drittem zur Absicherung der Übermittlung von Arbeitnehmerdaten ein Standardvertrag 2004/915/EG abgeschlossen wurde; in dieser Konstellation sollen im Hinblick auf die bereits in Anhang A zu diesem Standardvertrag enthaltenen Grundsätze gesonderte vertragliche Absprachen zwischen Arbeitgeber und Drittem zur Absicherung der Arbeitnehmerrechte entbehrlich sein. Erforderlich bleibe allerdings auch in dieser Konstellation die Sicherstellung der datenschutzrechtlichen Ansprüche der Arbeitnehmer auf Auskunft, Berichtigung und Löschung sowie gegebenenfalls Schadensatz gegen den Arbeitgeber. Die beschriebene Entscheidung macht deutlich, dass sich die Trennung zwischen 1. und 2. Prüfungsstufe nicht lückenlos durchhalten lässt. Vielmehr können die zur Rechtfertigung auf der 2. Stufe eingesetzten Mittel sich auf das Prüfungsergebnis auf der 1. Stufe positiv auswirken.[57]

[55] Vgl. *Trittin/Fischer*, NZA 2009, 343.

[56] Siehe Anhang A, 3. der Entscheidung 2004/915/EG (Standardvertrag Set II), unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004D0915:EN:NOT (abgerufen am 23.9.2009).

[57] Vgl. dazu *Rittweger/Schmidl*, DuD 2004, 617 ff.

2. Angemessenheit des Schutzniveaus beim Empfänger

Auf der zweiten Stufe wird geprüft, ob beim Empfänger der übermittelten Daten ein angemessenes Datenschutzniveau besteht. Wie oben beschrieben lässt sich dieses Erfordernis aus § 4b Abs. 2 BDSG ableiten, wonach die Übermittlung personenbezogener Daten zu unterbleiben hat, soweit der Betroffene ein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat, insbesondere wenn bei den empfangenden Stellen ein angemessenes Datenschutzniveau nicht gewährleistet ist. Ein angemessenes Datenschutzniveau liegt bei den EU-Mitgliedstaaten und den EWR-Mitgliedstaaten (Norwegen, Liechtenstein und Island) vor.[58] Auf Grundlage von Entscheidungen der Europäischen Kommission gemäß Art. 25 Abs. 6 Richtlinie 95/46/EG gilt dies auch für die Schweiz, Kanada, Argentinien, Guernsey und die Isle of Man.[59] Ein angemessenes Datenschutzniveau kann sich auch durch eine Safe-Harbor-Zertifizierung[60] eines US-Empfängers,[61] durch den Abschluss geeigneter Standardverträge zwischen den Parteien,[62] oder durch die Einführung

[58] Vgl. dazu http://ec.europa.eu/justice_home/fsj/privacy/thridcountries/index_de.htm (abgerufen am 23.9.2009).

[59] Vgl. *Gola/Schomerus* (Fn. 18), § 4b Rn. 14.

[60] Das Safe-Harbor-Regelwerk besteht aus verschiedenen Grundsätzen zum Datenschutz und hebt die US-Gesellschaften, die sich dementsprechend zertifizieren, in den Status von Empfängern, bei denen das (auf der 2. Stufe zu prüfende) angemessene Datenschutzniveau besteht; vgl. dazu die Entscheidung 2000/520/EG der Kommission vom 26.7.2000 (ABl. 2000 L 215, S. 7 ff.). Safe Harbor soll die Übermittlung personenbezogener Daten von der EU an Unternehmen in den USA ermöglichen und zwar ungeachtet dessen, dass in den USA insgesamt aus Sicht der EU kein angemessenes Datenschutzniveau besteht. Anhang 1 der Kommissionsentscheidung stellt dazu fest: „Die umfassende Rechtsvorschrift der Europäischen Union zum Schutz personenbezogener Daten, die Datenschutzrichtlinie […] legt fest, dass personenbezogene Daten nur in Nicht-EU-Länder übermittelt werden können, die einen ‚angemessenen' Schutz der Privatsphäre gewährleisten. Die Vereinigten Staaten und die Europäische Union haben beide das Ziel, den Datenschutz für ihre Staatsbürger zu verstärken, wobei die Vereinigten Staaten jedoch einen anderen Ansatz verfolgen als die Europäische Gemeinschaft. Die USA verwenden einen sektoralen Ansatz, der auf einer Mischung von Rechtsvorschriften, Verordnungen und Selbstregulierung basiert. Angesichts dieser Unterschiede fühlen sich viele US-Organisationen verunsichert bezüglich der Auswirkung des seitens der EU geforderten ‚Angemessenheits-Standards' für die Übermittlung personenbezogener Daten aus der Europäischen Union in die Vereinigten Staaten."

[61] Das Safe-Harbor-Regelwerk ist allerdings nicht auf Banken und Versicherungen anwendbar, vgl. dazu Hinweise Nr. 39, 3.1.2 des Innenministeriums Baden-Württemberg, siehe www.staatsanzeiger-bw.de/info_bekannt/Datenschutz.pdf (abgerufen am 23.9.2009).

[62] Vgl. *Räther/Seitz*, MMR 2002, 425.

verbindlicher Unternehmensregelungen[63] (so genannte Binding Corporate Rules) im Konzern ergeben.

Der schnellste Weg zur Herstellung eines angemessenen Datenschutzniveaus beim Empfänger liegt im Abschluss eines Standardvertrags. Es gibt derzeit 3 verschiedene Standardverträge,[64] die den Unternehmen mit Sitz in EU-Mitgliedstaaten über Entscheidungen der Kommission als Instrumente vorgegeben sind, ein angemessenes Datenschutzniveau beim Empfänger zu schaffen. Der Text der Standardverträge darf von den Parteien grundsätzlich nicht verändert werden.[65] Für die Betroffenen günstige Abweichungen von den Standardverträgen sollen aber zulässig sein. In der Praxis empfiehlt es sich, eine von den Parteien gewünschte Privilegierung der Betroffenen schon aus Gründen der Erhaltung der Standardisierung und der leichteren Erkennbarkeit außerhalb der Standardvertragsklauseln zu regeln. Zudem dürften die Meinungen der Parteien über die Frage, was für die Betroffenen günstige Änderungen sind, nicht immer einheitlich sein. Mangelnde Rechtssicherheit über die Entfaltung der Wirkung des Standardvertrags, ein angemessenes Datenschutzniveau herzustellen, ist die Folge.

Vereinfacht lässt sich die Wirkung der genannten Mechanismen (Standardverträge, Safe Harbor, verbindliche Unternehmensregelungen) in Ländern mit einem unangemessenen Datenschutzniveau am Beispiel der USA anhand *Graphik 2* (siehe unten S. 464) verdeutlichen.

Erläuterung zur Graphik 2: In Deutschland (karierte Fläche) herrscht (auch) aufgrund der Umsetzung der EG-Datenschutzrichtlinie (Richtlinie 95/46/EG) ein angemessenes Datenschutzniveau. Aus europäischer Sicht ist dies für die USA (schraffierte Fläche) nicht der Fall. Für die Übermittlungen von Arbeitnehmerdaten von der deutschen Tochtergesellschaft an die amerikanische Muttergesellschaft ist (wegen der auf der zweiten Stufe zu erfüllenden Anforderungen) bei dieser ein angemessenes Datenschutzniveau herzustellen. Für einen Empfänger in den USA kommt zusätzlich zum Abschluss eines Standardvertrags und der Einführung von Binding Corporate Rules im Konzern die Selbstzertifizierung der Amerikanischen Muttergesellschaft nach den Safe Harbor-Grundsätzen in Betracht. In der Folge herrscht zwischen den beteiligten Gesellschaften (ovale und weiße Fläche) ein angemessenes Datenschutzniveau. Bei diesem Datenschutzniveau handelt es sich zwar um ein angemessenes. Mit dem in Deutschland ist es indes nicht identisch. Vielmehr werden die Verarbeitungsgrundsätze jeweils durch die Regelungen des Instruments (Standardverträge,[66] Binding Corporate Rules,[67] Safe Harbor[68]) bestimmt, mit dem das angemessene Datenschutzniveau hergestellt wurde.

3. Sonderproblem Arbeitnehmereinwilligung

Nach Maßgabe des Wortlauts von § 4 Abs. 1 BDSG, wonach die

> „[…] Erhebung, Verarbeitung und Nutzung personenbezogener Daten […] nur zulässig [ist], soweit dieses Gesetz oder eine andere Rechtsvorschrift dies erlaubt oder anordnet oder der Betroffene eingewilligt hat“

scheint auch die Einwilligung ein geeigneter Erlaubnistatbestand für die internationale Übermittlung und anschließende Verarbeitung von Arbeitnehmerdaten zu sein. Gemäß § 4c Abs. 1 S. 1 Nr. 1 BDSG („[…] sofern 1. der Betroffene seine Einwilligung gegeben hat“) gilt dies auch für die zweite Stufe. Die Einwilligung kann mithin grundsätzlich das Fehlen eines angemessenen Datenschutzniveaus beim Empfänger ausgleichen.[69]

Für das Arbeitverhältnis ist die Einwilligung allerdings schlecht geeignet. Gemäß § 4a Abs. 1 S. 1 BDSG ist die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht.[70] Die ganz herrschende Meinung in Deutschland geht davon aus, dass der Arbeitnehmer nicht freiwillig einwilligen kann.[71] Auch auf europäischer Ebene sind die Aufsichtsbehörden der Mitgliedstaaten im Rahmen der so genannten Artikel-29-Gruppe[72] entsprechend übereingekommen. Am 13. September 2001 verabschiedete die Artikel-29-Gruppe ein Arbeitspapier (Stellungnahme

[63] Verbindliche Unternehmensregelungen dienen dazu, bei allen Unternehmen (d.h. auch solchen in Staaten außerhalb von EU/EWR) innerhalb eines Konzerns ein (auf der 2. Stufe zu prüfendes) angemessenes Datenschutzniveau herzustellen; vgl. dazu *Rittweger/Weiße*, CR 2003, 142; *Schröder*, DuD 2004, 462.

[64] Zu finden unter http://ec.europa.eu/justice_home/fsj/privacy/modelcontracts/index_de.htm (abgerufen am 23.9.2009).

[65] Siehe z.B. Art. 11 der Entscheidung 2001/497/EG unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32001D0497:DE:NOT (abgerufen am 23.9.2009).

[66] Vgl. z.B. die „Grundsätze für die Datenverarbeitung“ in Anhang A der Entscheidung 2004/915/EG (Standardvertrag Set II) unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?u-ri=CELEX:32004D0915:EN:NOT (abgerufen am 23.9.2009).

[67] Die Binding Corporate Rules, d.h. verbindlichen Unternehmensregelungen, unterliegen einer gewissen Gestaltungsfreiheit des betroffenen Konzerns, wobei gewissen Gestaltungsgrundsätze zu beachten sind; vgl. z.B. „Rahmen für verbindliche unternehmensinterne Datenschutzregelungen (Binding Corporate Rules – BCR)“ unter http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2008/wp154_de.pdf (abgerufen am 23.9.2009).

[68] Vgl. z.B. die „Grundsätze des Sicheren Hafens zum Datenschutz“ in Anhang 1 der Entscheidung 2000/520/EG unter http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:215:0007:0047:EN:PDF (abgerufen am 23.9.2009).

[69] Vgl. *Simitis* (Fn. 12), § 4c Rn. 8.

[70] Zu den Grundvoraussetzungen einer wirksamen Einwilligung siehe *Bergmann/Möhrle/Herb* (Fn. 36) , § 4a Rn. 3a ff.

[71] Vgl. *Wank* (Fn. 27), § 4a BDSG Rn. 2.

[72] Die Datenschutzgruppe ist gemäß Artikel 29 der Richtlinie 95/46/EG eingesetzt worden. Sie ist ein unabhängiges europäisches Beratungsgremium in Datenschutzfragen. Ihre Aufgaben sind in Artikel 30 der Richtlinie 95/46/EG sowie in Artikel 14 der Richtlinie 97/66/EG festgelegt.

8/2001) zur Verarbeitung personenbezogener Daten von Beschäftigten (Arbeitspapier Nr. 48).[73] Am 25. November 2005 verabschiedete die Artikel 29 Gruppe ein Arbeitspapier über eine gemeinsame Auslegung des Artikel 26 Abs. 1 der Richtlinie 95/46/EG vom 24. Oktober 1995[74] (Arbeitspapier Nr. 114).[75] Arbeitspapiere sind zwar nicht verbindlich, sie werden jedoch von den Datenschutzaufsichtsbehörden der Mitgliedstaaten der europäischen Union (weitestgehend[76]) beachtet und geben daher in verlässlicher Weise Aufschluss darüber, was von den jeweiligen nationalen Behörden zu erwarten ist. Einige der Aussagen im Arbeitspapier Nr. 114 betreffen die Zweifel an der Möglichkeit der freiwilligen Arbeitnehmereinwilligung[77] und die strukturelle Schwäche der Einwilligung als Basis von Maßnahmen der Datenverarbeitung („Die Datenschutzgruppe ist aufgrund ihrer Erfahrungen außerdem der Meinung, dass die Einwilligung in Fällen der wiederholten oder gar routinemäßigen Übermittlung von Daten zu deren Verarbeitung wahrscheinlich langfristig keinen angemessenen Rechtsrahmen für die Verantwortlichen für die Verarbeitung bietet.").[78] Die Arbeitnehmereinwilligung eignet sich daher nicht als Grundlage der Verarbeitung von Arbeitnehmerdaten im Konzern. Auch die jederzeitige Widerruflichkeit[79] der Einwilligung spricht gegen sie als Grundlage der Übermittlung von Arbeitnehmerdaten.[80] Das Arbeitspapier Nr. 48 stellt unter anderem klar, dass Arbeitgeber die Einwilligung ihrer Mitarbeiter nicht für Maßnahmen einholen sollten, die für die Erfüllung des Arbeitsvertrages erforderlich und daher bereits als solche zulässig sind.[81]Die Aufforderung zur Einwilligung wird in solchen Fällen im Einklang mit Arbeitspapier Nr. 48 als irreführend und daher unzulässig angesehen, weil bei den Beschäftigten auf diese Weise der Eindruck erweckt wird, ohne ihre Einwilligung könne das Beschäftigungsverhältnis nicht durchgeführt werden.

[73] Vgl. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/ 2001/wp48de.pdf (abgerufen am 23.9.2009).

[74] Art. 26 Abs. 1 der Richtlinie 95/46/EG (ABl. 1995 L 281, S. 31 ff.) hat folgenden Wortlaut: „Artikel 26. Ausnahmen. (1) Abweichend von Artikel 25 sehen die Mitgliedstaaten vorbehaltlich entgegenstehender Regelungen für bestimmte Fälle im innerstaatlichen Recht vor, daß eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland, das kein angemessenes Schutzniveau im Sinne des Artikels 25 Absatz 2 gewährleistet, vorgenommen werden kann, sofern a) die betroffene Person ohne jeden Zweifel ihre Einwilligung gegeben hat oder b) die Übermittlung für die Erfüllung eines Vertrags zwischen der betroffenen Person und dem für die Verarbeitung Verantwortlichen oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person erforderlich ist oder c) die Übermittlung zum Abschluß oder zur Erfüllung eines Vertrags erforderlich ist, der im Interesse der betroffenen Person vom für die Verarbeitung Verantwortlichen mit einem Dritten geschlossen wurde oder geschlossen werden soll, oder d) die Übermittlung entweder für die Wahrung eines wichtigen öffentlichen Interesses oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor Gericht erforderlich oder gesetzlich vorgeschrieben ist oder e) die Übermittlung für die Wahrung lebenswichtiger Interessen der betroffenen Person erforderlich ist oder f) die Übermittlung aus einem Register erfolgt, das gemäß den Rechts- oder Verwaltungsvorschriften zur Information der Öffentlichkeit bestimmt ist und entweder der gesamten Öffentlichkeit oder allen Personen, die ein berechtigtes Interesse nachweisen können, zur Einsichtnahme offensteht, soweit die gesetzlichen Voraussetzungen für die Einsichtnahme im Einzelfall gegeben sind."

[75] Vgl. http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2005/wp114_de.pdf (abgerufen am 23.9.2009).

[76] In einigen Mitgliedstaaten, z.B. Spanien, wird die Arbeitnehmereinwilligung als zulässig angesehen.

[77] Arbeitspapier Nr. 114, S. 13, Ziff. 2.1 zu „Einwilligung muss ohne Zwang gegeben werden"; vgl. dazu auch *Büllesbach*, in: Roßnagel, Handbuch des Datenschutzrechts, 2003, § 6.1 Rn. 14; *Gola/Schomerus* (Fn. 18), mit dem Hinweis auf die Gefahr der Entmündigung des Arbeitnehmers, § 4a Rn. 6 und 9.

[78] Arbeitspapier Nr. 114, S. 13, Ziff. 2.1.

[79] Vgl. *Gola/Schomerus* (Fn. 18), § 20 Rn. 21-24.

[80] Vgl. *Schmidl*, DuD 2007, 756 ff.

[81] Arbeitspapier Nr. 48, S. 27, Ziff 10. Einwilligung.

[82] Zum Entwurf eines Arbeitnehmerdatenschutzgesetzes siehe http://www.bmas.de/coremedia/generator/37290/2009_09_04_diskussionsentwurf_datenschutz.html (abgerufen am 23.9.2009).

IV. Zusammenfassung

Aus Sicht international präsenter Konzerne mag es noch so sinnvoll sein, den Austausch von Arbeitnehmerdaten jedweder Art zwischen Konzerngesellschaften grundsätzlich zu gestatten. Das europäische und in der Folge das deutsche Datenschutzrecht sehen gleichwohl kein Privileg für derartige Datenübermittlungen vor. Vielmehr werden Übermittlungen im Konzern wie solche zwischen Dritten behandelt – ein Konzernprivileg gibt es nicht. Ungeachtet dessen, sind zahlreiche internationale Konzerne in fein unterteilte Funktionsbereiche gegliedert, denen auch die Mitarbeiter der jeweiligen Konzerngesellschaften zugeordnet werden und zwar ohne Ansehung der Frage, mit welcher Konzerngesellschaft der eigentliche Arbeitsvertrag abgeschlossen wurde. In derartigen Matrixorganisationen sind zahlreiche Datenübermittlungen zwischen der Muttergesellschaft und den Tochtergesellschaften einerseits und den Tochtergesellschaften untereinander andererseits erforderlich und an der Tagesordnung.

Das deutsche Datenschutzrecht ist jedenfalls in der von den deutschen Aufsichtsbehörden konkretisierten Form und den besonderen Anforderungen an den Schutz von Arbeitnehmerdaten geeignet, diesen komplexen Strukturen internationaler Konzerne gerecht zu werden. Am Beispiel der Anforderungen an die Übermittlung von Arbeitnehmerdaten im Konzern wird deutlich, dass effektiver Arbeitnehmerdatenschutz bereits jetzt, d.h. auch ohne Arbeitnehmerdatenschutzgesetz,[82] Realität ist. Bereits die Unterscheidung danach, ob ein Arbeitsverhältnis mit primärem (d.h. anfänglich vorhandenem) oder sekundärem (d.h. nachträglich entstehenden)

Konzernbezug vorliegt und die in Abhängigkeit davon anzuwendende gesetzliche Grundlage für die Übermittlung von Daten, trägt den Arbeitnehmerinteressen Rechnung. Auf Grundlage der speziellen Anforderungen des Düsseldorfer Kreises an die Rechtmäßigkeit der Übermittlung von Arbeitnehmerdaten im Konzern können die Arbeitnehmer Ansprüche auf Auskunft, Löschung, Berichtigung, Sperrung und gegebenenfalls Schadensersatz stets gegen ihren Arbeitgeber geltend machen und zwar ungeachtet dessen, wo sich ihre Daten tatsächlich befinden oder, im Falle des Schadensersatzes, wer einen Schaden verursacht hat. Auch die von den Aufsichtsbehörden formulierten Grenzen für die Arbeitnehmereinwilligung tragen dazu bei,[83] dass Arbeitnehmer im Konzern nicht rechtlos gestellt werden, indem sie zur Erteilung universeller Einwilligungen veranlasst werden.

Auch wenn ein in sich geschlossenes Arbeitnehmerdatenschutzgesetz in der vergangenen Legislaturperiode nicht Realität wurde, ist das allgemeine Datenschutzrecht in der durch Rechtsprechung und Vorgaben der Aufsichtsbehörden konkretisierten Form, in vielen Bereichen geeignet, angemessenen Arbeitnehmerdatenschutz zu erreichen. Was in diesem Beitrag am Beispiel der Übermittlung von Arbeitnehmerdaten im Konzern verdeutlicht wurde, gilt gleichermaßen für den Schutz der Privatsphäre von Arbeitnehmern im Fall der privaten E-Mail-Nutzung.[84] Auch für die vom Arbeitgeber organisierte Überwachung von Mitarbeitern durch Mitarbeiter, beispielsweise in den so genannten Whistleblowing-Systemen, haben die Aufsichtsbehörden strenge Vorgaben entwickelt.[85] So hat der Arbeitgeber unter anderem sicherzustellen, dass nur bestimmte Ereignisse Gegenstand einer Meldepflicht sind, die Betroffenen informiert werden, sobald die Untersuchung des Vorfalls dadurch nicht mehr gefährdet würde und dass kein Anreiz für die Erstattung anonymer Meldungen gesetzt wird.

V. Ausblick

Es steht gegenwärtig nicht fest, wie ein künftiges Arbeitnehmerdatenschutzgesetz ausgestaltet sein wird. Der Bundesbeauftragte für den Datenschutz beispielsweise fordert für das Arbeitnehmerdatenschutzgesetz die Berücksichtigung der folgenden vier Grundsätze:[86]

(1) Personenbezogene Daten des Arbeitnehmers dürfen nur erhoben, verarbeitet und genutzt werden, wenn dies zur Begründung, Durchführung, Beendigung oder Abwicklung eines Arbeitsverhältnisses erforderlich oder sonst gesetzlich vorgeschrieben ist (nachfolgend vom Verfasser als „Erforderlichkeitsgrundsatz“ bezeichnet).

(2) Die Datenerhebung sollte grundsätzlich beim Arbeitnehmer selbst erfolgen (nachfolgend vom Verfasser als „Grundsatz der Direkterhebung“ bezeichnet).

(3) Personenbezogene Arbeitnehmerdaten dürfen nur für den Zweck, für den sie erhoben worden sind, verwendet werden. Daten, die für diesen Zweck nicht mehr erforderlich sind, sind zu löschen. (nachfolgend vom Verfasser als „Zweckbindungsgrundsatz“ bezeichnet).

(4) Aus Gründen der Transparenz sind Arbeitnehmer umfassend darüber zu informieren, welche Daten zu welcher Zeit, auf welche Weise und zu welchem Zweck über sie erhoben sowie in welcher Art und Weise ausgewertet werden; dies muss umfassende Auskunfts- und Einsichtsrechte des Arbeitnehmers einschließen (nachfolgend vom Verfasser gemeinsam als „Transparenzgrundsatz“ bezeichnet).

Die in den vorgenannten Grundsätzen zum Ausdruck kommenden Schutzziele sind im geltenden Recht aber (zumindest teilweise) bereits verwirklicht:

(1) Nach gegenwärtiger Rechtslage findet der Erforderlichkeitsgrundsatz etwa bereits in § 32 Abs. 1 S. 1 BDSG Niederschlag, wonach personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses nur erhoben, verarbeitet oder genutzt werden dürfen, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Die komplementär anwendbare Regelung in § 28 Abs. 2 Nr. 2 a) BDSG stellt die Zulässigkeit der genannten Maßnahmen ausdrücklich unter den Vorbehalt der Erforderlichkeit und einer Interessenabwägung.

(2) Der Grundsatz der Direkterhebung ist im geltenden Recht bekannt. Gemäß § 4 Abs. 2 S. 1 BDSG gilt, dass personenbezogene Daten beim Betroffenen zu erheben sind. Die in § 4 Abs. 2 S. 2 BDSG enthaltenen Ausnahmen sind nicht weitreichend und setzen zudem die Durchführung einer Interessenabwägung voraus.

(3) Auch der Zweckbindungsgrundsatz ist kein Novum für das deutsche Datenschutzrecht. Gemäß § 28 Abs. 2 Nr. 1 BDSG ist die Verwendung personenbezogener Daten gegenüber der Erstverwendung nicht privilegiert; die Rechtmäßigkeitsvoraussetzungen der Erhebung, Verarbeitung und Nutzung sind in gleicher Weise einzuhalten und § 35 Abs. 2 S. 2 Nr. 3 BDSG fordert die Löschung von Daten, deren fortgesetzte Speicherung für den ursprünglichen Zweck nicht mehr erforderlich ist.

(4) Der Transparenzgrundsatz schließlich findet aktuell in den Vorschriften von §§ 4 Abs. 3 und 33 BDSG Beachtung, wonach sowohl bei der Erhebung - in der Regel wird hier der Arbeitgeber aktiv - als auch bei der erstmaligen Speicherung durch einen Dritten - diese Verpflichtung trifft weitere vom Arbeitgeber eingeschaltete verantwortliche Stellen - eine Unterrichtung der Betroffenen erforderlich ist.

Jedenfalls wird bei der Schaffung des neuen Gesetzes sorgfältig zu prüfen sein, inwieweit tatsächlich spezieller

---

[83] Vgl. dazu auch *Schmidl*, DuD 2007, 756 ff.

[84] Vgl. zu den Einzelheiten und zu dem für Arbeitnehmer resultierenden Schutz am Beispiel der E-Mail-Filterung *Schmidl*, MMR 2005, 343 ff.

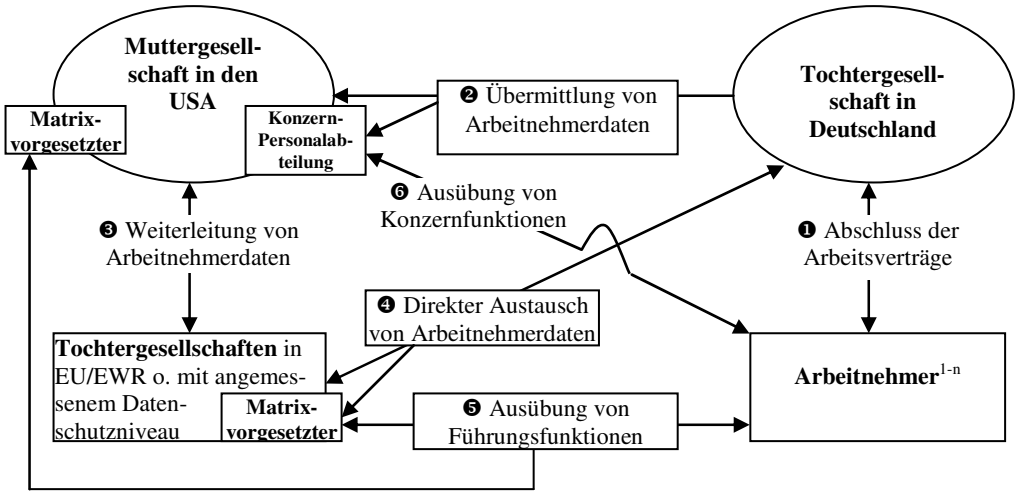
[85] Siehe Whistleblowing – Hotlines: Firmeninterne Warnsysteme und Beschäftigtendatenschutz
Arbeitsbericht der Ad-hoc-Arbeitsgruppe „Beschäftigtendatenschutz“ des Düsseldorfer Kreises unter http://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/Personalwesen/Inhalt/6_Whistleblowing-Hotlines/Whistleblowing-Hotlines.pdf (abgerufen am 23.9.2009).

[86] http://www.bfdi.bund.de/nn_530440/DE/Themen/Arbeit/Arbeitnehmerdatenschutz/Artikel/Arbeitnehmerdatenschutzgesetz.html (abgerufen am 23.9.2009).

Regelungsbedarf besteht, um den Besonderheiten des Arbeitsverhältnisses gerecht zu werden.[87]

[87] Der am 4.9.2009 veröffentlichte Diskussionsentwurf des Bundesarbeitsministeriums verfolgt demgegenüber einen relativ ausführlichen Regelungsansatz. Der Diskussionsentwurf enthält Regelungen zu folgenden Themen: 1. Abschnitt: Allgemeine Bestimmungen – § 1 Zielsetzung, § 2 Anwendungsbereich, § 3 Begriffsbestimmungen, § 4 Zulässigkeit der Datenerhebung und Datenverwendung, § 5 Datengeheimnis, Datensparsamkeit; 2. Abschnitt: Datenerhebung und Datenverwendung vor Begründung des Beschäftigungsverhältnisses – § 6 Datenerhebung im Einstellungsverfahren, § 7 Datenverwendung im Einstellungsverfahren; 3. Abschnitt: Datenerhebung und Datenverwendung nach Begründung des Beschäftigungsverhältnisses – § 8 Datenerhebung, § 9 Datenverwendung, § 10 Besondere Formen der Datenverwendung, § 11 Opto-elektronische Einrichtungen (Videoüberwachung), § 12 Ortungssysteme, § 13 Biometrische Verfahren, § 14 Telekommunikationsdienste, § 15 Telearbeit; 4. Abschnitt: Vertraulichkeit und Sicherheit der Datenverwendung – § 16 Datensicherheit, § 17 Datensicherheit bei besonderen Arten von Beschäftigtendaten; 5. Abschnitt: Rechte und Pflichten – § 18 Benachrichtigung über Erhebung oder Speicherung, § 19 Benachrichtigung über Datenpannen, § 20 Einsichtsrecht, § 21 Auskunftsrecht, § 22 Korrekturen, § 23 Ansprüche, § 24 Maßregelungsverbot; 6. Abschnitt: Sonderbestimmungen – § 25 Datenerhebung oder Datenverwendung im Auftrag des Arbeitgebers, § 26 Datenerhebung oder Datenverwendung innerhalb verbundener Unternehmen, § 27 Grenzüberschreitende Datenerhebung und Datenverwendung; 7. Abschnitt: Organisatorischer Datenschutz – § 28 Bestellung von Beauftragten für den Beschäftigtendatenschutz, § 29 Mitbestimmungsrechte und Kündigungsschutz, § 30 Aufgaben der Beauftragten für den Beschäftigtendatenschutz, § 31 Aufsichtsbehörde; 8. Abschnitt: Besondere Regelungen für Interessenvertretungen – § 32 Rechte der Interessenvertretungen, § 33 Datenerhebung und Datenverwendung; 9. Abschnitt: Schlussvorschriften – § 34 Unabdingbarkeit, Verzicht, Verwirkung, § 35 Bußgeldvorschriften, § 36 Strafvorschriften, § 37 Inkrafttreten.

Graphik 1



Erläuterung zur Graphik 1: Im gewählten Beispielsfall werden die Arbeitnehmerdaten in Schritt 1 erstmalig beim Abschluss des Arbeitsvertrages erhoben. In Schritt ❷ werden Arbeitnehmerdaten übermittelt, soweit dies für die Erreichung der Konzernzwecke (z.B. weltweite Personalverwaltung, Nachfolgeplanung, Erleichterung der weltweiten Zusammenarbeit etc.) notwendig ist. Für die anlässlich von Schritt ❷ erfolgenden Übermittlungen ist die Muttergesellschaft verantwortliche Stelle, gleich ob die Konzernpersonalabteilung oder ein anderer Funktionsträger bei der Muttergesellschaft tatsächlicher Empfänger der Daten ist. Zu den als Schritt ❸ dargestellten Weiterübermittlungen kommt es beispielsweise, wenn Tochtergesellschaften innerhalb des Konzerns für die konzernweite Durchführung bestimmter Aufgaben, z.B. Gehalts- oder Reisekostenabrechnung, zuständig sind. Die als Schritt ❹ dargestellten Direktübermittlungen sind die typische Folge der Tatsache, dass die Matrixvorgesetzten in unterschiedlichen Konzerngesellschaften arbeiten. Für die Mitarbeiterführung und die Ausübung entsprechender Managementfunktionen erhalten diese Daten über „ihre" Berichtspflichtigen auch ohne die Einbindung der Muttergesellschaft. Verantwortliche Stelle ist insoweit die den jeweiligen Matrixvorgesetzten beschäftigende Tochtergesellschaft. Schritt ❺ stellt die möglichen Übermittlungen von Daten im Rahmen der Mitarbeiteranleitung dar, wenn der Matrixvorgesetzte seine Führungsfunktionen wahrnimmt. Schließlich kommen die als Schritt ❻ dargestellten Datenübermittlungen bei der Ausübung von Konzernfunktionen (zum Begriff siehe oben) durch die HR-Abteilung der Muttergesellschaft in Betracht.

Graphik 2