Reinhard Linz

Datenschutz im Konzern – Eine Lagebeschreibung aus Betriebsratssicht

„Datenschutz durch Mitbestimmung" ist eine gängige und durchaus treffende Floskel, wenn Autoren über den Datenschutz im Arbeitsverhältnis schreiben. Natürlich gibt es Datenschutz im Betrieb auch ohne Mitbestimmung. Das Bundesdatenschutzgesetz (BDSG) und die aus dem Grundgesetz abzuleitenden Datenschutzrechte gelten schließlich auch im Arbeitsverhältnis und auch dann, wenn gar kein Betriebsrat gebildet wurde. Aber der Einfluss des Betriebsrats auf den Arbeitnehmerdatenschutz kann sehr groß und sehr nützlich sein. Wir werfen einen Blick darauf, in welcher Weise die besonderen Rahmenbedingungen in einem Konzern die Einflussmöglichkeiten des Betriebsrats prägen.

Starke Rechte für den Betriebsrat

Praktisch die gesamte Verarbeitung von Arbeitnehmerdaten im Betrieb unterliegt nach dem Betriebsverfassungsgesetz (BetrVG) den Beteiligungsrechten der Betriebsräte, in weiten Bereichen sogar harten Mitbestimmungsrechten. Dreh- und Angelpunkt ist das Mitbestimmungsrecht aus § 87 Abs. 1 Nr. 6 über technische Einrichtungen, die zur Leistungs- oder Verhaltenskontrolle geeignet sind. Damit sind so gut wie alle computergestützten Systeme erfasst. Hinzu kommen das Informations- und Beratungsrecht über die Planung von technischen Anlagen (§ 90), die Mitbestimmung über Personalfragebögen (§ 94) und über die Ordnung und das Verhalten der Arbeitnehmer im Betrieb (§ 87 Abs. 1 Nr. 1), der Auftrag nach § 75 Abs. 2, die freie Entfaltung der Persönlichkeit der Arbeitnehmer zu schützen und zu fördern, sowie der Auftrag nach § 80 Abs. 1 Nr. 1 über die Einhaltung zugunsten der Arbeitnehmer geltender Rechtsvorschriften zu wachen. Ob Arbeitszeiterfassung, Produktionsplanung, Mitarbeiterbefragungen, Personalinformationssysteme oder Social Media im Unternehmen, der Betriebsrat ist zu beteiligen.

Natürlich ist in allen genannten Beispielen auch der betriebliche Datenschutzbeauftragte im Spiel. Aber der Betriebsrat ist mächtiger. Er ist bei der Gestaltung der betrieblichen Datenverarbeitungsprozesse nicht nur Beratungspartner des Managements. In den meisten Fällen ist seine explizite Zustimmung erforderlich, bevor ein System in Betrieb gehen darf. Und während Betriebsräte bei Verletzung dieses Rechts immer wieder die Arbeitsgerichte anrufen, hört man nur selten, dass ein Datenschutzbeauftragter die Aufsichtsbehörde zu Hilfe ruft, wenn sein Rat zur DV-Gestaltung unbeachtet bleibt.

Verstärkung für den Datenschutz

Nützlich ist der Einfluss der Betriebsräte, weil sie Regelungen für die Datenverarbeitung herbeiführen, die die spezifischen Gegebenheiten eines bestimmten Geschäftsprozesses in ihrem individuellen Unternehmen berücksichtigen und daher praxisnäher und viel konkreter sein können, als die stets generell-abstrakten Gesetzesvorschriften. Während das Gesetz recht allgemein verlangt, dass nur die personenbezogenen Daten gespeichert werden dürfen, die für einen legitimen Zweck erforderlich sind, kann eine Betriebsvereinbarung (BV) eine genaue Auflistung der Datenarten enthalten, die z.B. in einer Rückmeldung aus der Auftragsfertigung von Motoren am Unternehmensstandort Köln erfasst werden sollen.

Betriebsräte können auch System-Revisionen durchführen und gegen Verletzungen von IT-Betriebsvereinbarungen notfalls gerichtlich vorgehen. Die politischen Handlungsoptionen kommen noch dazu. Wenn ein Betriebsrat den Arbeitnehmerdatenschutz konsequent verfolgt, in Betriebsversammlungen und Publikationen immer wieder thematisiert, für Schulung und Aufklärung sorgt, dann hat das erheblichen Einfluss darauf, welchen Stellenwert dem Datenschutz in der gesamten Betriebskultur zugemessen wird.

So bietet sich für Betriebsräte ein weites Feld, um sozusagen als Lobbyisten für die Betroffenen, hier die Arbeitnehmer, tätig zu werden. Die Möglichkeiten zu nutzen und den eigenen Zielen gerecht zu werden, ist allerdings schon in einem einzelnen Betrieb nicht leicht. In einem Konzern wird es noch ein Stück schwieriger.

Große Konzerne – Große Systeme – Große Aufgaben für kleine Gremien

Wenn Konzernunternehmen ihre Geschäftsprozesse standardisieren und miteinander verzahnen, verzahnen sie selbstverständlich auch ihre Datenverarbeitung in gemeinsam genutzten IT-Systemen. Und die sind typischerweise groß. Hierbei geht es nicht um Kantinenabrechnung oder Parkplatzverwaltung, wobei Daten von Beschäftigten eines einzelnen Standorts verarbeitet werden. Vielmehr geht es um Systeme von Anbietern wie SAP, SuccessFactors oder Taleo, die das zentrale Personalmanagement unterstützen sollen und für den ganzen Konzern sämtliche Stellenausschreibungen, die Bewerberauswahl, die Dokumentation von Zielvereinbarungen, die Beurteilung von Beschäftigten, die Verteilung von Gehältern und Prämien, die Suche nach passenden Mitarbeitern für freie Stellen, die Karriere- und Nachfolgeplanung und die Personalentwicklungspläne und -maßnahmen abbilden. Ähnliche Großsysteme gibt es

für das zentrale Controlling, die Produktionsplanung, die Lagerverwaltung, die Kundenbetreuung und vieles mehr.

Um allein die technischen Funktionen solcher Systeme zu verstehen, Risiken zu identifizieren und Gestaltungsoptionen zu erkennen, brauchen selbst „technik-affine" Menschen sehr viel Zeit und Bereitschaft, sich in die Besonderheiten eines Systems einzuarbeiten. Die arbeitsorganisatorische Seite kommt noch dazu. Es gilt, die von der Integration betroffenen Geschäftsprozesse an den einzelnen Standorten zu betrachten, da sie einerseits ein wichtiges Maß für die Erforderlichkeit der personenbezogenen Datenverarbeitung darstellen, andererseits aber auch selbst nach Datenschutzkriterien (um-)gestaltet werden müssen. Dabei werden Betriebsräte ein besonderes Augenmerk auf die Bedürfnisse der Arbeitnehmer nach Erhalt und Qualität der Arbeit sowie auf deren Gewohnheiten und Präferenzen haben, auf Aspekte also, die zusätzlich zu den klassischen Arbeitgeberzielen Effektivität und Effizienz mit dem Datenschutz in Einklang gebracht werden sollen. Hier entsteht für die Betriebsräte ein Kapazitätsproblem. Für Konzernbetriebsräte (KBR) kann das in besonderem Maße zutreffen; denn anders als bei den örtlichen Betriebsräten wächst die Zahl ihrer Mitglieder im Allgemeinen nicht parallel zur Zahl der vertretenen Beschäftigten.

So fällt die Aufgabe, für eine sehr große Zahl von Beschäftigten an verschiedenen Standorten den Arbeitnehmerdatenschutz in vielfach verästelten Geschäftsprozessen zu gestalten, oftmals einer sehr kleinen Zahl von Konzernbetriebsratsmitgliedern zu, für die der Arbeitnehmerdatenschutz obendrein nur eine von vielen Aufgaben darstellt.

Datenschutz-Controlling

Mehr Arbeitskraft und mehr Kompetenz sind die naheliegenden Forderungen angesichts dieser Schwierigkeiten. Tatsächlich konnten manche Betriebsräte durch Vereinbarungen über die Größe der Gremien oder die Zahl der Freistellungen eine gewisse Entlastung schaffen.

Unabhängig davon können Betriebsräte nach § 80 Abs. 2 BetrVG die Unterstützung „sachkundiger Arbeitnehmer" in Anspruch nehmen, die sich bei den Arbeitsabläufen oder in der Technik auskennen und nicht selbst Mitglied des Gremiums zu sein brauchen. Selbstverständlich kann auch der betriebliche Datenschutzbeauftragte mit seiner Sachkunde helfen. Wenn geeignete interne Experten fehlen oder der Betriebsrat an deren Unbefangenheit zweifelt, kann er nach § 80 Abs. 3 BetrVG auch externe Sachverständige seines Vertrauens zu Rate ziehen.

Leider zeigt die Erfahrung, dass all dies das Kapazitäts- und Kompetenzproblem lindert, aber nicht strukturell löst. Einem erweiterten Projektteam auf der Betriebsratsseite gelingt dann vielleicht nach monatelanger Arbeit eine ordentliche Regelung zum Datenschutz in *einem* System. Währenddessen aber werden durch die Einführung oder Änderung anderer Systeme Fakten geschaffen, die der Betriebsrat – und oft auch der nicht minder überlastete Datenschutzbeauftragte – erschöpft hinnehmen, ohne sie wesentlich beeinflusst oder auch nur gründlich geprüft zu haben.

Aussichtsreicher wäre es, dem strukturellen Mangel strukturell zu begegnen, indem man verbindliche Standards für DV-Projekte schafft. So wie ein Kostencontrolling heute selbstverständlich zur Projektarbeit gehört, sollte auch eine Art Datenschutz-Controlling eine Standard-Aufgabe jedes DV-Projekts sein. Konformität mit geltenden Datenschutzvorschriften, besser noch Datenschutz-Exzellenz sollte zum unverzichtbaren Qualitätsmerkmal jedes DV-Prozesses erklärt werden, und die dafür notwendigen Arbeiten sollten *in* den Projekten geleistet werden. Die Projektleitung ist dann nicht nur dafür verantwortlich, dass nach dem Projekt ein neues DV-Verfahren funktioniert, sondern auch dafür, dass alle Datenschutzanforderungen erfüllt sind.

Die Datenschutzaufgaben gehören selbstverständlich in den Projektplan. Wie bei jeder anderen Projektaufgabe sind die erwarteten Ergebnisse zu definieren, die ausführenden Personen sind zu benennen, der erwartete Zeitbedarf und die Kosten sind zu planen, und – sehr wichtig – die Meilensteine sind so zu fixieren, dass auch Datenschutzergebnisse geprüft und freigegeben werden. Betriebsrat und Datenschutzbeauftragter gehören dann zu den Freigabe-Instanzen sowohl für den Projektplan als auch für das Passieren der Meilensteine. Die Erarbeitung der notwendigen Datenschutzergebnisse kann man ihnen jedoch nicht, jedenfalls nicht vollständig aufbürden. Das wird bei der Kapazitätsplanung des Projektes schnell deutlich werden.

Zu den Pflichtaufgaben jedes DV-Projektes muss es gehören, mindestens die folgenden, für den Datenschutz wichtigen Konzepte zu erarbeiten und zu dokumentieren:

- Datenmodell: Welche personenbezogenen Daten werden zu welchem Zweck verarbeitet, und worin begründet sich die Erforderlichkeit?
- Löschkonzept: Welche Daten müssen wann gelöscht werden, und mit welchen organisatorischen und technischen Verfahren geschieht das?
- Auswertungskonzept: Wie und zu welchem Zweck werden personenbezogene Daten ausgewertet und wodurch ist die Erforderlichkeit begründet?
- Betriebliches Berechtigungskonzept: Welche Stellen müssen welche Informationen bekommen?
- Technisches Berechtigungskonzept: Wie werden Zugriffsbeschränkungen technisch realisiert?
- Konzept für die Datenweitergabe: Wer ist Empfänger der personenbezogenen Daten, welche Rechtsgrundlage erlaubt die Datenweitergabe und welche Verträge werden mit den Datenempfängern als Dritte im Sinne des BDSG oder als Auftragsdatenverarbeiter abgeschlossen?
- Revisionskonzept: Welche technischen und organisatorischen Hilfsmittel stehen für die Datenschutz-Revision zur Verfügung?
- Sicherheitskonzept: Mit welchen Maßnahmen wird den im vorliegenden Fall zu beachtenden Sicherheitsanforderungen Rechnung getragen?

Diese Themen überschneiden sich mit den Themen des Verfahrensverzeichnisses nach §§ 4e und 4g BDSG. Die Angaben sollten aber detaillierter ausfallen, als es in den Verfahrensverzeichnissen üblich ist. Für viele der notwendigen Datenschutz-Dokumente kann man Fragenraster, Checklisten oder gar Formulare vorbereiten, was den gewünschten

Detaillierungsgrad festlegt, eine gewisse Mindestqualität sichert und insgesamt die Arbeit erleichtert.

Der Konzernbetriebsrat könnte sich bemühen, ein solches Datenschutz-Pflichtprogramm für jedes DV-Projekt in eine IT-Rahmenbetriebsvereinbarung aufzunehmen. Das wäre zwar eine freiwillige, nicht per Einigungsstelle erzwingbare Vereinbarung, würde also die grundsätzliche Bereitschaft des Managements voraussetzen, sich auf derartige Standards einzulassen. Man würde damit aber jenseits schöner Worte in Broschüren und auf Homepages den Datenschutz wirklich zum festen Bestandteil der Geschäftsprozesse machen. Betriebsräte und Datenschutzbeauftragte würden entlastet, weil sie Datenschutzkonzepte mehr beurteilen als entwickeln müssten, und praxisnahe Datenschutz-Vorkehrungen würden in jeden Verarbeitungsprozess sozusagen von vornherein eingebaut. Und – was im Zeitalter der Kennzahlen-Fixierung nicht zu unterschätzen ist – ein erheblicher Teil der Kosten für die Datenschutzarbeiten würde verursachungsgerecht den DV-Projekten zugeordnet und nicht, wie es sonst oft geschieht, dem Betriebsrat oder dem Datenschutzbeauftragten.

Diffuser Informationsbedarf in der Matrixorganisation

Modern und typisch für große Unternehmen und Konzerne ist die sogenannte Matrix-Organisation: Beschäftigte werden nach verschiedenen Ordnungskriterien in mehrere Hierarchien eingebunden und haben in der Folge nicht mehr nur einen Chef, sondern gleich mehrere direkte Vorgesetzte. Der herkömmliche Chef wird zum sogenannten „disziplinarischen Vorgesetzten". Daneben gibt es aber „funktionale Vorgesetzte", z.B. einen in der Spartenhierarchie Nutzfahrzeuge, einen in der Funktionshierarchie Konstruktion und schließlich noch den Leiter eines einzelnen Projektes Elektrocaddy Zürich. Eine solche Struktur lässt sich gar nicht mehr in den zwei Dimensionen einer Matrix darstellen. Daher trägt man in das klassische Organigramm neben der Baum-Hierarchie, die die disziplinarische Ordnung repräsentiert, noch gestrichelte Linien („Dotted Lines") ein, die die anderen Hierarchien darstellen sollen. Es entsteht ein Bild, das eher einem Gestrüpp als einer Ordnung gleicht. Wenn zusätzlich – und das ist in Konzernen durchaus normal – abgesehen von der disziplinarischen alle Vorgesetztenhierarchien kreuz und quer durch die Konzernunternehmen verlaufen, ist das Organigramm endgültig nicht mehr grafisch darstellbar.

Klar ist, dass jeder der verschiedenen Vorgesetzten irgendwelche Informationen über die ihm zugeordneten Beschäftigten braucht, seien es Urlaubszeiten, Qualifikationen, Bezüge, Interessen, vereinbarte Ziele oder Beurteilungen. Was genau welcher Vorgesetzte wissen muss, ist aber kaum zu ermitteln; denn die Aufgaben und Kompetenzen in der komplizierten Struktur sind oftmals gar nicht oder nur sehr vage definiert. Obendrein ändert sich diese Struktur in großen Unternehmen tatsächlich jeden zweiten Tag, und es gibt keine Stelle und keine Dokumentation, die über den aktuellen Stand verlässlich Auskunft geben könnten.

Auf der Grundlage solcher Strukturen, die erforderlichen und damit legitimierbaren Datentransfers bzw. Zugriffsberechtigungen in IT-Systemen zu ermitteln, ist – gelinde gesagt – eine Herausforderung für die Datenschützer. Der Sog zu einer Totalfreigabe aller Mitarbeiterdaten für alle Vorgesetzten („damit nur alle ihren Job erledigen können") ist enorm, aber sicher nicht angemessen.

Worauf der Betriebsrat und ebenso der Datenschutzbeauftragte hier drängen sollten, ist

- klare Aufgabendefinition und Aufgabentrennung in der multidimensionalen Hierarchie,
- Beweislast für die Erforderlichkeit eines Datenzugriffs bei den Antragstellern und
- notfalls auch eine durch den Datenschutz begründete Änderung der Organisationsstruktur hin zu klar abgegrenzten, reduzierten Zuständigkeiten.

Insofern kann die Mitbestimmung des Betriebsrats über den Arbeitnehmerdatenschutz indirekt zu einer – begrenzten – Mitbestimmung über die Arbeitsorganisation werden, obwohl die an sich nicht der Mitbestimmung unterliegt. Solches durchzusetzen, ist zwar bestimmt nicht einfach, ist aber begründet durch die Notwendigkeit, die Anwendung technischer Überwachungseinrichtungen auch organisatorisch zu gestalten.

Datenaustausch über Unternehmensgrenzen hinweg – Betriebsvereinbarungen als Rechtsgrundlage

Konzerne organisieren ihre Arbeit über Unternehmensgrenzen hinweg. Produktionssegmente und auch Managementfunktionen werden auf wenige Standorte konzentriert. Konzerninterne Fertigungsketten, die sich über verschiedene Standorte erstrecken, werden eng aufeinander abgestimmt. Für manche Verwaltungsfunktionen werden sogar neue Konzernunternehmen gegründet, sogenannte Shared-Service-Organisationen, die dann sozusagen als gemeinsame Fachabteilungen für mehrere Konzernunternehmen Standard-Dienste wie zum Beispiel den Einkauf, das Finanz-Controlling oder die Personalverwaltung übernehmen. Aber auch strategische Management-Funktionen werden in sog. Centers of Expertise gebündelt und einem einzigen federführenden Unternehmen für eine ganze Region wie etwa Europa, den mittleren Osten und Asien („EMEA") zugeordnet. Im Personalbereich werden dann z.B. die Konzeption und die Umsetzung einheitlicher Entlohnungssysteme, Personalbeurteilungsverfahren, Karrierewege und Stellenbesetzungsverfahren von einem CoE HR zentral beobachtet und gesteuert.

Diese Organisationsformen – meist gekoppelt mit multidimensionalen Matrix-Strukturen – verursachen Datenströme zwischen Unternehmen, die einer besonderen Rechtsgrundlage bedürfen und, weil gesetzliche oder tarifvertragliche Regelungen hierzu höchstens ausgestaltungsbedürftige Rahmenregeln vorgeben, zugleich Gegenstand der Mitbestimmung sind.

Sofern die Datenübertragung im Rahmen einer Auftragsdatenverarbeitung innerhalb Europas erfolgt, bildet § 11 BDSG die Erlaubnisnorm. Allerdings dürfte die Arbeitsverteilung im Konzern die Merkmale einer Auftragsdatenverarbeitung nur in Ausnahmefällen erfüllen, etwa beim reinen Rechenzentrumsbetrieb durch eine Konzerntochter. Selbst Shared-Service-Organisationen,

die überwiegend Standard-Dienstleistungen erbringen, haben oft so große Freiräume bei der Erledigung ihrer Aufgaben, dass man von einer Funktionsübertragung ausgehen muss. Wenn eine Shared-Service-Organisation für das Beschäftigungsverhältnis erforderliche Dienstleitungen erbringt, z.B. das Reisemanagement oder die Entwicklung individueller Schulungspläne für Konzernmitarbeiter, kann damit auch eine im Sinne von § 32 BDSG erforderliche Datenübermittlung für Zwecke des Beschäftigungsverhältnisses verbunden sein. Soweit jedoch Daten für das strategische Management, für die Koordination verteilter Produktionsprozesse oder eine konzernweite Personalvermittlung übertragen werden, kommt eine Auftragsdatenverarbeitung nicht in Betracht, weil die Daten von den Empfängern auch für eigene Zwecke genutzt werden, und § 32 greift nicht, weil dies Zwecke sind, die außerhalb des individuellen Beschäftigungsverhältnisses liegen.

Dann kann es mit der datenschutzrechtlichen Erlaubnisnorm schwierig werden, erst recht natürlich, wenn sensible Arbeitnehmerdaten wie zum Beispiel Qualifikationen und Beurteilungen oder krankheitsbedingte Fehlzeiten kommuniziert werden sollen. Meistens läuft es auf die Frage hinaus, ob die Abwägung der Interessen der verantwortlichen Stelle mit denen der Betroffenen gemäß § 28 Abs. 1 Ziff. 2 BDSG zu Gunsten des Unternehmens ausfällt, das die Daten an seine Konzernschwestern weitergeben will. Bei dieser Abwägung ist die Gesamtsituation zu würdigen, in der der Datentransfer stattfinden soll, und die wird auch von geltenden Betriebsvereinbarungen geprägt. Je besser die betroffenen Arbeitnehmer trotz Übermittlung ihrer Daten im Konzern vor Verletzungen ihres Persönlichkeitsrechts geschützt werden, desto geringer ist in diesem Abwägungsprozess ihr Interesse am Ausschluss der Übermittlung zu werten. Sollte also eine Konzernbetriebsvereinbarung insgesamt enge Grenzen für die Verarbeitung und Nutzung der im Konzern kommunizierten Arbeitnehmerdaten ziehen, indem sie z.B. Verwendungszwecke, Zugriffsberechtigungen, Löschfristen und Revisionsverfahren für alle beteiligten Konzernunternehmen festlegt, könnte dies den Ausschlag dafür geben, dass die Datenübermittlung zulässig ist. Wenn die Konzernunternehmen nicht durch andere Verträge vergleichbare Verpflichtungen eingegangen wären, hätten KBR und Konzernleitung damit als Ergebnis der Mitbestimmung überhaupt erst eine datenschutzrechtliche Zulässigkeitsvoraussetzung geschaffen, die sonst gefehlt hätte.

Wenn die Datenübermittlung nicht nur Unternehmens-, sondern auch Ländergrenzen überschreitet, sind die Empfänger nicht dem BetrVG unterworfen. Dann kann eine Betriebsvereinbarung ihre legitimierende Wirkung nur in Kombination mit einem Vertrag zwischen den Konzernunternehmen entfalten, der die ausländischen Töchter zur Einhaltung der dort festgelegten Regeln verpflichtet. Die besonderen Voraussetzungen nach den §§ 4b und 4c BDSG für eine Datenübermittlung ins Ausland, namentlich in Länder außerhalb von EU und EWR müssen natürlich zusätzlich erfüllt sein.

Eine Betriebsvereinbarung kommt allerdings auch als eigenständige Rechtsgrundlage in Betracht, wenn sie die Datenübermittlung als „andere Rechtsvorschrift“ im Sinne von § 4 Abs. 1 BDSG erlaubt. Eine knappe Betriebsvereinbarung, in der ein großzügiger Betriebsrat der Übermittlung von Arbeitnehmerdaten vorbehaltlos zustimmt, würde allerdings noch nicht ausreichen, weil die aus den Grundrechten ableitbaren Mindeststandards des Persönlichkeitsschutzes sichergestellt sein müssen. Es ist jedoch keineswegs geklärt, in welche ergänzenden Vorschriften die Übermittlungserlaubnis einer BV eingebettet sein muss, um die Standards der Verfassung zu erfüllen. Sie dürften den bei der Interessenabwägung abzulegenden Maßstäben ähnlich sein.

Ob als Faktor bei der Interessenabwägung oder als „andere Rechtsvorschrift“ – klar ist, dass eine Betriebsvereinbarung eine datenschutzrechtliche Grundlage schaffen kann, die die Datenübermittlung im Konzern erst zulässig macht. Entsprechend sorgsam sollten die Betriebsparteien vorgehen, damit der durch das BDSG gewährte Schutz der Daten nicht aufgeweicht, sondern möglichst gestärkt wird.

Falsche Verhandlungspartner

In ausländisch geführten Konzernen ergeben sich für den Betriebsrat bei seinen Bemühungen um den Datenschutz oft besondere Schwierigkeiten.

Ein verbreitetes Problem besteht darin, dass dem Betriebsrat ein kompetenter Verhandlungspartner fehlt. Häufig sitzt er Managern einer deutschen Konzerntochter gegenüber, die wichtige Entscheidungen gar nicht selbst treffen dürfen, sondern sich erst bei „höheren“ Stellen im Ausland rückversichern müssen. Wenn auch noch das für die IT federführende Unternehmen seinen Sitz im Ausland hat, sind manche deutsche Geschäftsführer nicht einmal imstande, über die Datenverarbeitungsprozesse und die Einrichtung der beteiligten IT-Systeme fundiert Auskunft zu erteilen.

Diese Situation macht die Beratungen außerordentlich zäh und mühsam. Die Kommunikation mit den Fachleuten im Hintergrund verläuft schleppend und mit vielen Missverständnissen. Denn in Paris, San Diego und Bangalore hat man nur vage Vorstellungen davon, was ein Betriebsrat ist, warum er so viele Fragen zu Sonderaspekten der Datenverarbeitung stellt und was das mit den Interessen von Beschäftigten zu tun hat. Auch die grundlegenden Vorstellungen von Datenschutz und seiner Bedeutung erweisen sich als unterschiedlich. So erhält man Auskünfte, die formal korrekt sein mögen, aber die falschen Schwerpunkte setzen und nicht wirklich weiterhelfen. Zusagen, bestimmte Daten nicht zu speichern, auf manche Auswertungen zu verzichten oder Berechtigungen einzuschränken, sind noch schwerer zu bekommen. Warum sollte man sich hier festlegen? Bloß weil ein Betriebsrat in Deutschland das will?

Um voranzukommen und am Ende ein gutes Ergebnis zu erzielen, müssen Fachleute und Entscheider an den Verhandlungstisch. Sind die in Deutschland nicht anzutreffen, sollten auch Auslandsreisen kein Hindernis sein. Wenn der europäische IT-Chef gemeinsam mit seinem SAP-Berechtigungsexperten aus Helsinki nach Köln fliegt, um mit dem Gesamtbetriebsrat zu verhandeln, sind beide formal nicht die Repräsentanten des der Mitbestimmung unterliegenden Unternehmens. Trotzdem führen derarti-

ge Gespräche erfahrungsgemäß schneller zum Ziel: Neben dem Austausch über Interessen und Absichten kann man zügig zu den Kernfragen kommen und die Gestaltungsoptionen klären. Nur wenn sich verhandlungsfähige Personen gegenübersitzen, kommt Bewegung in die Sache: Positionen können überdacht und Kompromisslinien ausgelotet werden. So wird mancher Knoten durchschlagen, der im schriftlichen „Antragsverfahren" nur immer dicker geworden wäre. Nach dem zweiten Treffen können dann auch Videokonferenzen fruchtbar verlaufen. Damit Datenschutz gelingt, müssen die richtigen Leute einander kennenlernen. In internationalen Konzernen kann das internationale Verhandlungskommissionen erforderlich machen.

Internationale Umzingelung

Ein weiteres Problem ist spiegelbildlich zum ersten: Auch der ausländischen Konzernmutter fehlt ein Gegenpart, mit dem sie über den Arbeitnehmerdatenschutz im Konzern verhandeln könnte oder müsste. Es gibt keinen „globalen" Betriebsrat, der alle Arbeitnehmer eines Konzerns vertritt. Die gemeinsame Vertretung der in der EU beschäftigten Arbeitnehmer eines Konzerns ist der Europäische Betriebsrat; er hat jedoch nur Informations- und Beratungsrechte. Innerhalb und erst recht außerhalb der EU gibt es kaum ein Land, in dem die Arbeitnehmervertretung in Sachen Datenverarbeitung ähnlich harte Mitbestimmungsrechte hat wie in Deutschland.

So können amerikanische und asiatische Konzerne internationale Informationssysteme weitgehend ohne Mitbestimmung durch Arbeitnehmervertretungen aufbauen. Und das ist der bevorzugte Weg: Das Kernsystem wird in Japan eingerichtet und in Betrieb genommen und dann nach und nach in den Tochtergesellschaften in anderen Ländern „ausgerollt" z.B. in der Reihenfolge Korea, Kanada, Südafrika, England, Frankreich, Skandinavien, Benelux und Polen bis am Ende Deutschland und vielleicht Österreich regelrecht umzingelt sind von den Ausläufern des großen, vernetzten Informationssystems.

Nachdem das System seit mehreren Jahren in allen anderen Ländern produktiv eingesetzt wird, tritt der deutsche Betriebsrat in die Verhandlungen über Datenkataloge, Schnittstellen, Leistungskennzahlen und Zugriffsberechtigungen ein, weil das System nun auch in Deutschland eingeführt werden soll. Die verbleibenden Optionen zu seiner Ausgestaltung und Einsatzweise sind jetzt nur noch marginal, die Verhandlungsspielräume der deutschen Manager auch. Ihre persönliche Leistungsbeurteilung und der Jahresbonus hängen davon ab, ob der Anschluss der deutschen Niederlassung bis zum nächsten Jahreswechsel vollzogen ist. Wo kann das hinführen?

Wenn der Betriebsrat auf seinen Gestaltungsanspruch pocht und Forderungen zur Verbesserung des Arbeitnehmerdatenschutzes stellt, werden die Verhandlungen bald scheitern, und die Arbeitgeberseite wird angesichts ihres Termindrucks in die Einigungsstelle streben.

Nun kommt es auf den Vorsitzenden an. Das wird höchstwahrscheinlich ein Arbeitsrichter sein, und er wird zu Beginn der Verhandlungen betonen, dass auch internationale Konzerne in Deutschland deutsches Arbeitsrecht beachten müssen. Aber nach welchen Kriterien wird er die Forderungen des Betriebsrats nach einer (Um-)Gestaltung der vom neuen System geprägten DV-Prozesse bewerten? Wie stark wird er sich von den „immensen Kosten" beeindrucken lassen, die die Arbeitgeberseite für die verlangten Anpassungen vorhersagt? Wird er eine auf konkrete Zahlen gestützte Kostenprognose verlangen? Und welches Gewicht wird er dem Gebot des § 90 BetrVG beimessen, über die Planung technischer Anlagen so rechtzeitig mit dem Betriebsrat zu beraten, dass die „Vorschläge und Bedenken des Betriebsrats bei der Planung berücksichtigt werden können"? Gerade auch um die Einflussmöglichkeiten zu sichern, hat der Betriebsrat außerdem nach § 87 Abs. 1 Nr. 6 BetrVG nicht nur bei der Anwendung, sondern schon bei der Einführung technischer Einrichtungen mit Überwachungspotential ein Mitbestimmungsrecht. Sieht der Vorsitzende das Informations-, Beratungs- und Mitbestimmungsrecht also schon verletzt, und ist das Kostenargument wegen der bisher vorenthaltenen Einflussmöglichkeiten nur noch von geringem Gewicht?

Es bedarf schon eines soliden Selbstbewusstseins des Vorsitzenden, um trotz des massiven Drängens eines Weltkonzerns im Verfahren genügend Zeit für eine verständliche Darstellung der geplanten DV-Verfahren, für eine ernsthafte Erwägung aller Datenschutzaspekte und eine gründliche Analyse der objektiven Gestaltungsoptionen zu reservieren. Denn schon dies kann etliche Sitzungstage in Anspruch nehmen. Dem Unternehmen in einem Spruch dann auch noch kostspielige und erneut zeitraubende Umbauten am System zuzumuten, kommt schon einer Mutprobe gleich, der die meisten Vorsitzenden lieber ausweichen werden.

Es kommt aber auch auf die Entschlossenheit des Betriebsrats an, und die bestimmt sich nicht allein nach der Güte der verhandelten Datenschutzregelungen. Vielmehr spielen noch ganz andere Faktoren eine Rolle, die für die Beschäftigten unter Umständen eine viel handfestere Bedeutung haben. Da geht es zum Beispiel um Arbeitsplätze. Wenn die Geschäftsprozesse nicht rationalisiert und global integriert werden, leidet die Konkurrenzfähigkeit des gesamten Unternehmens. Sogar die konzern-interne Konkurrenz entfaltet ihre Wirkung. Wenn die Datenschutzanforderungen in Köln so kompliziert werden und letztlich die Geschäftsprozesse behindern, dann erhält vielleicht das Werk in Prag den Zuschlag für die neue Produktlinie. Auch wenn nie ganz sicher ist, ob solche Befürchtungen sich bewahrheiten, machen sie es dem Betriebsrat schwer, für die deutschen Standorte als den einzigen im ganzen Konzern eine strikte Haltung beim Arbeitnehmerdatenschutz aufrechtzuerhalten und gegenüber seinen Wählern zu begründen.

Das pragmatische Ergebnis besteht dann oft darin, dass im Wesentlichen der in den Nachbarländern etablierte Ist-Stand als Soll für die deutsche Konzerntochter festgeschrieben wird. Der Betriebsrat kann dann bei künftigen Änderungen erneut mitbestimmen. Das Feld echter Gestaltung aber schrumpft auf das Schulungskonzept für die neuen Benutzer in Deutschland (mit verpflichtender Sensibilisierung für die neuen Datenschutz-Risiken) und auf die Zusicherung eines jederzeitigen Revisionsrechts auch beim ausländischen System-

betreiber und dies vielleicht sogar mit einem dafür einzurichtenden eigenen Systemzugang.

Es zeigt sich deutlich, dass die Gestaltung des Arbeitnehmerdatenschutzes keineswegs nur eine Frage des Rechts ist, sondern in hohem Maße von den Überzeugungen, dem Willen und der Kompetenz der Akteure, letztlich also von Macht und Politik bestimmt wird. Das mag vielleicht erschrecken, ist aber in der betrieblichen Demokratie ganz normal und kann bei Wahrung fairer Umgangsformen auch durchaus gute Früchte tragen. So ist es eben beim „Datenschutz durch Mitbestimmung".