Stellungnahme

zum Entwurf Rahmen-KBV
„Beschäftigtendatenschutz bei Einsatz von IT-Systemen“

von

Prof. Dr. Wolfgang Däubler, Universität Bremen

I. Einleitung

Der vorliegende Entwurf enthält einen auf hohem Niveau angesiedelten Beschäftigtendatenschutz. Er behandelt praktisch alle Fragen, die in diesem Zusammenhang zu stellen sind. Außerdem ist er in gut lesbarem Stil geschrieben, was ihm allein schon eine gewisse Ausnahmestellung sichert.

Bei einzelnen Fragen tauchen noch Probleme auf, die im Folgenden unter II abgehandelt sind. Außerdem werden unter III noch einige Vorschläge zur Verbesserung der Kontrollrechte des Betriebsrats angefügt, die ggf. bei § 23 des Entwurfs einzufügen wären.

II. Einzelregelungen

1. Rubrum

Als Partner der KBV wird auf Arbeitgeberseite ausschließlich die „Vattenfall Europe AG“ genannt. Dies genügt nach der Rechtsprechung, um zugleich alle von dieser Konzernspitze abhängigen Gesellschaften in den Geltungsbereich einzubeziehen.

> BAG Urt. v. 22. 1. 2002 – 3 AZR 554/00 – NZA 2002, 1224, 1226; ebenso in der Literatur Trittin, in: Däubler/Kittner/Klebe/Wedde (Hrsg.), BetrVG, 12. Aufl., Frankfurt/Main 2010, § 58 Rn 107 m. w. N.

In § 15 Abs. 4 ist jedoch von der „Vattenfall Group“ die Rede, in Bezug auf die auch inhaltliche Regelungen getroffen werden. Sollte es sich dabei nicht nur um eine „Teilmenge“ der zur Vattenfall Europe AG gehörenden Unternehmen handeln, müsste sie im Rubrum als vertragsschließende Partei gleichfalls genannt werden.

2. Personeller Geltungsbereich – Arbeitnehmer oder „Beschäftigte“?

In § 1 Abs. 1 ist wie auch anderen Stellen des Entwurfs von „Beschäftigtendatenschutz“ die Rede. Dies entspricht der Terminologie des BDSG, das in seinem § 3 Nr. 11 diesen

Begriff zugleich definiert. Danach ist er sehr viel weiter als der Arbeitnehmerbegriff und umfasst beispielsweise auch freie Mitarbeiter und andere arbeitnehmerähnliche Personen.

Die Organe der Betriebsverfassung können nur für Arbeitnehmer und Auszubildende sprechen und grundsätzlich auch nur für sie Betriebsvereinbarungen schließen. Nach § 5 Abs.1 Satz 2 BetrVG sind die in Heimarbeit Beschäftigten einbezogen, die „in der Hauptsache“ für den Betrieb arbeiten. Alle anderen arbeitnehmerähnlichen Personen sind nach herrschender Ansicht ausgeklammert.

> S. statt aller Fitting, BetrVG, Handkommentar, 25. Aufl. München 2010, § 5 Rn 92; Rost NZA 1999, 113 ff.; Koch, in: Erfurter Kommentar zum Arbeitsrecht, 11. Aufl., München 2011, § 5 Rn 2

Für sie kann also jedenfalls keine normativ wirkende (Konzern-)Betriebsvereinbarung geschlossen werden. Möglich ist allerdings, den Arbeitgeber zu verpflichten, diese Gruppe von Beschäftigten wie Arbeitnehmer zu behandeln und sie so mittelbar in den Geltungsbereich einzubeziehen. Entsprechendes hat das BAG in Bezug auf leitende Angestellte angenommen, für die der Betriebsrat gleichfalls nicht sprechen kann, die aber auf diesem Wege in den Genuss von Sozialplanleistungen kommen können.

> BAG 31. 1. 1979, AP Nr. 8 zu § 112 BetrVG 1972: ebenso Hess, in: Hess/Schlochauer/Worzalla/Glock/Nicolai, BetrVG, 7. Aufl. Köln 2008, §§ 112, 112a Rn 80; Gamillscheg, Kollektives Arbeitsrecht, Band II, München 2008, S. 1137.

Diesen Grundsatz wird man auch hier anwenden und so alle „Beschäftigten“ im Sinne des § 3 Abs.11 BDSG in den Schutzbereich der Konzernbetriebsvereinbarung einbeziehen können.

Damit die Konzernbetriebsvereinbarung effektiv in diesem Sinne gehandhabt wird, sollte man zwei redaktionelle Veränderungen vornehmen:

Zum einen sollte man durchgehend von „Beschäftigungsverhältnis“ sprechen und den Ausdruck „Arbeitsverhältnis“ vermeiden. Andernfalls könnte der Eindruck entstehen, dass im einen Fall alle „Beschäftigten“, im anderen nur die Arbeitnehmer erfasst sein sollen.

Zum zweiten sollte man beim persönlichen Geltungsbereich in § 2 Abs.2 den Begriff des Beschäftigten in der Weise definieren, dass man auf den Personenkreis des § 5 Abs.1 BetrVG verweist und ausdrücklich betont, der Arbeitgeber sei verpflichtet, andere Beschäftigte im Sinne des § 3 Abs.11 BDSG wie Arbeitnehmer im Sinne des § 5 Abs.1 BetrVG zu behandeln. Man könnte beispielsweise formulieren:

„(2) Persönlicher Geltungsbereich
Die vorliegende Konzernbetriebsvereinbarung gilt für alle Beschäftigten im Sinne des § 5 Abs.1 BetrVG. Dazu zählen insbesondere

- Arbeitnehmerinnen und Arbeitnehmer (auch wenn sie sich in einem ruhenden Arbeitsverhältnis befinden)
- Praktikantinnen und Praktikanten
- Auszubildende und andere zu ihrer Berufsbildung Beschäftigte
- Bewerberinnen und Bewerber
- Personen, deren aktives Beschäftigungsverhältnis im Vattenfall Konzern beendet ist.

Darüber hinaus verpflichtet sich die Arbeitgeberseite, alle Beschäftigten im Sinne des § 3 Abs.11 BDSG nach den hier niedergelegten Grundsätzen zu behandeln.“

3. Beschäftigtendaten bei Zugriffssicherung

Im zweiten Teil von § 2 Abs. 3 sind Beschäftigtendaten behandelt, die im Rahmen der Zugriffssicherung erhoben werden. Im zweiten Satz heißt es, sie dürften nicht „zur Auswertung von Verhaltens- und/oder Leistungskontrollen herangezogen werden.“ Damit ist der wichtigste Fall einer Zweckänderung erwähnt, doch sind auch andere denkbar. Ich würde deshalb einen Wortlaut vorziehen, der jeden anderen Verwendungszweck als die Zugriffssicherung ausschließt und deshalb formulieren:

„Im Rahmen der Zugriffssicherung erhobene Beschäftigtendaten dürfen für keinerlei andere Zwecke, insbesondere nicht zu Verhaltens- und Leistungskontrollen herangezogen werden."

4. Übermittlung ins Ausland

§ 2 Abs. 4 behandelt die „Auslandsdatenverarbeitung im internationalen Bereich" und bekennt sich zu dem Grundsatz, dass Beschäftigtendaten, die in das Ausland exportiert werden, den deutschen Schutzstandard mitnehmen. Dabei bleibt letztlich offen, wie dies praktisch umgesetzt werden soll. Wie würden beispielsweise die „geeigneten Maßnahmen" aussehen, die Vattenfall nach dieser Vorschrift ergreifen müsste, um eine Beeinträchtigung oder Umgehung des datenschutzrechtlichen Standards zu vermeiden, wenn die Lohnabrechnung in Indien erfolgen würde? Läge „Auslandsdatenverarbeitung im internationalen Bereich" vor, wenn lediglich der Server in einem Drittstaat stehen würde, alle Befehle aber hier eingegeben würden? Um Unsicherheiten und Meinungsverschiedenheiten zu vermeiden, sollte man eine klare Regelung treffen, die die in § 2 Abs.4 enthaltene Grundsatzentscheidung konsequent umsetzt. Man könnte etwas formulieren:

„Findet die Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten ganz oder teilweise im Ausland statt, so wird Vattenfall durch vertragliche Abmachung mit dem ausländischen Partner dafür sorgen, dass kein geringeres Maß an Datenschutz als nach deutschem Recht und nach dieser Vereinbarung praktiziert wird. Insbesondere müssen die Rechte des Betroffenen nach § 21 und die des Betriebsrats nach § 23 auch in diesem Fall gewahrt bleiben. Bei Verstößen gilt § 24."

Durch diese Formulierung wird sichergestellt, dass je nach den konkreten Verhältnissen unterschiedliche Maßnahmen getroffen werden, um ein Absinken des Schutzniveaus zu vermeiden. Findet ein Teil der Datenverarbeitung beispielsweise in einem anderen EU-Mitgliedstaat statt, so sind angesichts des prinzipiell gleichwertigen Schutzniveaus sehr viel weniger weitgehende Regelungen zu treffen als wenn es um Drittstaaten wie Indien oder die USA geht. Die Sicherung der Informations- und Kontrollrechte des Einzelnen dürfte keine Probleme machen, da sie beispielsweise auch in den sog. Safe-Harbor-

Grundsätzen in den USA niedergelegt sind. Der betrieblichen Interessenvertretung vergleichbare Befugnisse einzuräumen, kann schwerlich für den ausländischen Partner unzumutbar sein.

5. Zweckbestimmung und Zweckänderung

Bei § 4 Abs.4 liegt wohl ein redaktionelles Versehen vor, da ein Unterschied zwischen der „Durchführung konkreter Arbeitsaufgaben“ und der „Erledigung von konkreten Arbeitsaufträgen“ zu erkennen ist. Auch ist nicht einsehbar, weshalb die Festlegung eines konkreten Zwecks im Sinne des § 28 Abs.1 Satz 2 BDSG nur in diesen Fällen Platz greifen soll: Wird beispielsweise ein Zugangskontrollsystem als solches eingerichtet, dürfen die dabei anfallenden Daten nicht zur Pünktlichkeitskontrolle benutzt werden. Ich würde deshalb formulieren:

„Beschäftigtendaten dürfen nur insoweit verarbeitet oder genutzt werden, als dies durch den vor oder bei der Erhebung festgelegten Zweck im Sinne des § 28 Abs.1 Satz 2 BDSG eindeutig legitimiert ist.“

Die (zu begrüßende) enge Festlegung des Zwecks ist dann ohne größeres Interesse, wenn eine nachträgliche Zweckänderung unter leicht zu erfüllenden Voraussetzungen möglich ist. § 28 Abs.2 BDSG lässt die Zweckänderung u. a. auch dann zu, „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.“ (so § 28 Abs.2 Nr. 1 unter Verweisung auf § 28 Abs.1 Satz 1 Nr. 2). Dies ist eine sehr offene Formulierung, deren praktische Anwendung viele Zweifelsfragen mit sich bringt. Unterstellt, das Betreten und Verlassen des Betriebsgeländes wird um Wege der Zugangskontrolle erfasst – hat dann der einzelne Arbeitnehmer ein schutzwürdiges Interesse daran, dass seine Unpünktlichkeit nicht ans Tageslicht kommt und besteht Grund zu der Annahme, dass dieses Interesse des Beschäftigten „überwiegt“? Ich würde empfehlen, insoweit nicht auf das BDSG zu verweisen, sondern eine eigenständige Regelung zu treffen. Man könnte daran denken, eine Zweckänderung nur dann zuzulassen, wenn hinter ihr ein „deutlich überwiegendes

Interesse des Arbeitgebers“ steht, dem auf andere Weise nicht Rechnung getragen werden kann. Damit wären sehr viel präzisere Konturen erreicht. Vorschlag für § 6:

„Die Zweckbestimmung, die einer Erhebung, Verarbeitung oder Nutzung von Beschäftigtendaten zunächst nach § 4 zugrunde gelegt wird, kann nachträglich nur dann erweitert oder geändert werden, wenn dies durch ein deutlich überwiegendes Interesse des Arbeitgebers gerechtfertigt ist, dem auf anderem Wege nicht Rechnung getragen werden kann. Die Beteiligungs- und Mitbestimmungsrechte der zuständigen Betriebsräte bleiben unberührt.“

6. Nebendatenverarbeitung

Die Vorschrift des § 7 ist in ihrer Tragweite nicht recht überschaubar. Die Ermächtigung, auch außerhalb „kollektivrechtlich geregelter Systeme und Verfahren“ Beschäftigtendaten zu verarbeiten, läuft insoweit auf einen Verzicht auf das Mitbestimmungsrecht nach § 87 Abs.1 Nr. 6 hinaus. Weshalb diese Regelung? An welche konkreten Fälle ist dabei gedacht? Warum soll eine Verarbeitung in oder aus Excel-Tabellen „außerhalb“ kollektivrechtlich geregelter Systeme und Verfahren liegen?

7. Begriff Beschäftigtendaten

§ 8 sieht eine weite Auslegung des Begriffs „Beschäftigtendaten“ vor. Dies ist dann sinnvoll, wenn der Beschäftigtendatenschutz den Betroffenen besser schützt als das allgemeine Datenschutzrecht – was vertretbar ist, aber im Hinblick auf die zu erwartende Neuregelung keineswegs ausgemacht erscheint. Wenn man eine weite Auslegung bevorzugt, so muss man sich auch zu den Daten irgendwie verhalten, die im Zusammenhang mit der Rolle des Beschäftigten als Konsumenten entstehen. Soll es wirklich die Möglichkeit geben, über die Abrechnungssysteme die Essgewohnheiten zu erfassen? Dies könnte die Entscheidung über einen Auslandseinsatz erheblich beeinflussen; wer immer das „Diätessen“ bevorzugt, ist für einen Einsatz in Russland nicht besonders gut geeignet. Eine solche Auswertung wäre zwar eine Zweckeentfremdung, aber diese ist ja nicht unter allen denkbaren Umständen ausgeschlossen. Deshalb wäre ich für eine strikte Trennung. Man könnte etwa als Abs. 2 formulieren:

„Beschäftigtendaten über die Inanspruchnahme von betrieblichen Leistungen wie Kantinenessen und den Bezug von Waren und Energie dürfen unter keinen Umständen mit den übrigen Beschäftigtendaten verknüpft werden."

8. Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten ohne Erlaubnistatbestand

§ 9 Abs. 1 verlangt einen „klaren Erlaubnistatbestand" für die Datenerhebung usw. durch den Arbeitgeber. Dies ist zu begrüßen, weil es zusammen mit der engen Zweckbestimmung einer Pauschalerlaubnis entgegenwirkt. Nach Abs.2 ist es Sache des Arbeitgebers, die Notwendigkeit seines Vorgehens und das Vorliegen eines Erlaubnistatbestands zu beweisen. Redaktionell könnte man Abs. 2 etwas umformulieren und wie folgt fassen:

„Im Zweifelsfall muss der Arbeitgeber nachweisen, weshalb die Erhebung, Verarbeitung und Nutzung der Beschäftigtendaten notwendig war und auf welche Umstände sich der von ihm geltend gemachte Erlaubnistatbestand stützte."

Aus der betrieblichen Realität ist auch der Fall bekannt, dass ein Vorgesetzter auf eigene Faust Dateien anlegt, um besser z. B. über die Mitglieder seiner Gruppe Bescheid zu wissen. Hierfür gibt es keinerlei Rechtsgrundlage. Dies sollte man ausdrücklich in der KBV festhalten und als § 9 Abs. 3 formulieren:

„Unzulässig sind insbesondere das Erheben, Verarbeiten und Nutzen von Beschäftigtendaten, soweit Vorgesetzte ohne Ermächtigung des Arbeitgebers handeln."

9. Direkterhebung und soziale Netze

§ 12 sichert den Grundsatz der Direkterhebung dadurch ab, dass der Arbeitgeber nicht auf Informationen aus dem Internet zugreifen darf. Sie ist sehr zu begrüßen, wenngleich die „Dunkelziffer" in diesem Bereich sehr hoch sein wird und ohne polizeistaatliche Mittel

keine wirkliche Kontrolle möglich ist. Wichtig ist eine solche Vorschrift auch deshalb, weil § 28 Abs.1 Satz 1 Nr. 3 BDSG den Zugriff auf allgemein zugängliche Daten schon dann erlaubt, wenn das Interesse des Betroffenen am Ausschluss der Datenverarbeitung nicht „offensichtlich“ überwiegt.

In redaktioneller Hinsicht sollte man die sozialen Netzwerke ausdrücklich erwähnen. § 12 wäre daher wie folgt zu fassen:

„Beschäftigtendaten müssen direkt beim Betroffenen erhoben werden. Eine Erhebung von Beschäftigtendaten aus anderen Quellen (z. B. aus dem Internet, insbesondere aus sozialen Netzwerken oder von Auskunfteien) ist ohne ausdrücklichen Erlaubnistatbestand ebenso verboten wie die anschließende Verarbeitung und Nutzung. § 28 Abs.1 Satz 1 Nr. 3 BDSG findet keine Anwendung. Dies gilt auch dann, wenn der Betroffene die Daten freiwillig ins Internet gestellt und so öffentlich zugänglich gemacht hat.“

In § 13 Abs. 2 sollen die Daten, die ein Bewerber in eine Jobbörse eingestellt hat, verwertbar sein, in § 12 steht das Gegenteil. Was soll gelten? Ich wäre dafür, dass die in die Jobbörse eingestellten Informationen durchaus verwertet werden dürfen. Insoweit würde § 13 Abs.2 einen „ausdrücklichen Erlaubnistatbestand“ im Sinne von § 12 darstellen.

10. Screening im Betrieb

Der Arbeitgeber ist an sich keine Instanz der Strafverfolgung; das sollte man grundsätzlich der Polizei, der Staatsanwaltschaft und den Gerichten überlassen. Dennoch kann es Fälle geben, in denen der Arbeitgeber ein berechtigtes Interesse an einer Aufklärung hat. Dem trägt der aktuell geltende § 32 Abs.1 Satz 2 BDSG Rechnung , der „zu dokumentierende tatsächliche Anhaltspunkte“ verlangt, die den Verdacht einer Straftat begründen. Die geplante Neuregelung will dies verschlechtern und eine anonymisierte oder pseudonymisierte „Rasterfahndung“ im Betrieb zulassen. Ergibt sich ein Verdacht, soll eine Re-Personalisierung möglich sein, was zugleich die geringe Schutzintensität der „Flucht in die Anonymität“ deutlich macht.

Abs. 1 spricht nur von „Sachverhaltsaufklärung“, nennt in Klammern „Ermittlungen“ und fügt dann nicht näher bestimmte „interne Maßnahmen“ hinzu. Im Datenschutzrecht geht es um die Erhebung personenbezogener Daten und um die Auswertung vorhandener Dateien oder anderer Unterlagen. Dies sollte man auch bei der Formulierung deutlich machen. Ich würde vorschlagen, in Abs. 1 die heutige Regelung des § 32 Abs. 1 Satz 2 festzuschreiben und zu formulieren:

„Zur Verhinderung oder Aufdeckung von Straftaten dürfen Beschäftigtendaten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begehen wird oder begangen hat, und wenn Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.“

Dies geht sogar zugunsten der Arbeitgeberseite noch über § 32 Abs. 1 Satz 2 insofern hinaus, als auch drohende Straftaten einbezogen sind.

Abs. 2 lässt unter bestimmen Voraussetzungen eine „Beweissicherung“ auch ohne Einschaltung des Betriebsrats zu, der erst nachher informiert werden muss. Welche Fälle damit gemeint sind, ist unklar. Im Einzelhandel, wo dies praktisch die größte Rolle spielt, wird normalerweise der Betriebsrat eingeschaltet, wenn es z. B. um die Auswertung von Videoaufzeichnungen geht; Unzuträglichkeiten haben sich dabei nicht ergeben. Zu denken ist an den aus einer Spielbank bekannten Fall, dass ein Betriebsratsmitglied in den Verdacht einer betrügerischen Manipulation geriet und der Betriebsrat nicht eingeschaltet wurde, um eine „Vorwarnung“ zu vermeiden. Eine solche faktische Preisgabe des Mitbestimmungsrechts ist nicht akzeptabel. Wenn der Arbeitgeber hier Bedenken hat, soll er sich eben an die Staatsanwaltschaft wenden.

In Abs. 2 würde ich daher Satz 1 beibehalten, die „Ausnahmefälle“ in Satz 2 dagegen streichen.

11. Die Sonderregelung des § 15

Eine definitive Beurteilung dieser sehr eingehenden Bestimmung ist nicht möglich, da mir die Anlagen nicht vorliegen. Bei Abs. 6 würde ich die „freiwillige“ Zustimmung des

Mitarbeiters durch ein Zustimmungsrecht des Betriebsrats ergänzen, da er über die nötige Unabhängigkeit verfügt, um etwaige Zumutungen zurückzuweisen. Bei Abs. 7 habe ich mich gefragt, warum auch die Personalnummer in die „konzerninterne“ Öffentlichkeit aufgenommen werde soll; sie taucht in vielen Zusammenhängen wieder auf, so dass mit ihr versehene Informationen ihre innerbetriebliche „Abschirmung“ verlieren.

In Abs. 10 wird nicht klar, wer die jeweiligen „Dateneigner“ sind. Geht es um den Betroffenen oder seinen Arbeitgeber? Vermutlich das letztere. Dann ist es aber nicht genügend, die Befugnis zur Datenverarbeitung allein an eine Vollmacht zu binden. Vielmehr müsste auch hier der Grundsatz der Zweckbindung konsequent eingehalten werden.

12. Übermittlung an Dritte und Auftragsdatenverarbeitung

Die Bestimmung des § 16 ist gut formuliert und bietet wenig Angriffsflächen. Im ersten Absatz sollte man statt „Arbeitsverhältnisses“ „Beschäftigungsverhältnisses“ sagen, weil sonst Missverständnisse aufkommen könnten. In Abs. 2 würde ich das Informationsrecht des Betriebsrats auf den ganzen Vertrag mit dem Auftragnehmer erstrecken, nicht nur auf die „Vertragspassagen, welche die Einhaltung der Regelungen dieser Vereinbarung sicherstellen.“ M. E. erstreckt sich auch der gesetzliche Informationsanspruch auf den ganzen Vertrag – nicht anders als im Personalbereich, wo der Betriebsrat z. B. den gesamten Vertrag über die Arbeitnehmerüberlassung oder den gesamten Werkvertrag zur Kenntnis bekommt, um prüfen zu können, ob er ggf. Mitbestimmungsrechte hat.

> s. BAG 31. 1. 1989, AP Nr. 33 zu § 80 BetrVG 1972; BAG 9. 7. 1991, AP Nr. 94 zu § 99 BetrVG 1972; ebenso Fitting § 80 Rn 63; weitere Nachweise bei Buschmann, in: Däubler/Kittner/Klebe/Wedde, a. a. O., § 80 Rn 75

Grundgedanke ist, dass man erst bei Kenntnis des ganzen Vertrags wirklich beurteilen kann, ob die Rechte des Betriebsrats in vollem Umfang aufrechterhalten sind.

Ob man diesen Informationsanspruch überhaupt durch Betriebsvereinbarung beschränken könnte, erscheint höchst zweifelhaft, weil dies einem Verzicht auf Betriebsratsbefugnisse gleichkommt.

Zum Verbot des Verzichts auf Betriebsratsbefugnisse s. grundlegend Joussen RdA 2005, 31 ff. m. w. N.

Jedenfalls ist hier kein besonderer Anlass für einen solchen Verzicht ersichtlich.

13. Grundsätze des Systemeinsatzes

Bei § 17 sind nur redaktionelle Anmerkungen zu machen. In Abs. 2 sollte man hervorheben, dass Leistungs- und Verhaltenskontrollen „zwischen den Betriebsparteien" vereinbart sein müssen; andernfalls könnte jemand auf die Idee komme, dass auch die Einwilligung des Einzelnen genügt. Auch muss hervorgehoben werden, dass die ausnahmsweise vorgenommene Zulassung nicht für Daten nach § 31 BDSG gilt. Ich würde deshalb Abs. 2 ein wenig ergänzen und formulieren:

„Die Systeme werden nicht zum Zwecke einer Leistungs- und Verhaltenskontrolle verwendet, es sei denn, dies werde ausdrücklich zwischen den Betriebsparteien vereinbart. Beschäftigtendaten, die ausschließlich zu Zwecken der Datenschutzkontrolle, der Datensicherung oder zur Sicherstellung eines ordnungsgemäßen Betriebs einer Datenverarbeitungsanlage gespeichert werden (§ 31 BDSG), dürfen nur für diese Zwecke verarbeitet oder genutzt werden, ohne dass eine abweichende Vereinbarung zulässig wäre."

Gut finde ich die Bestimmung des Abs. 4.

14. Infrastruktur- und Betriebssysteme

Bei § 18 könnte nur insoweit ein Bedenken bestehen, als relativ pauschal auf die „Aufklärung eines strafrechtlich relevanten Sachverhalts unter zwingender Einbeziehung des zuständigen Betriebsrats" verwiesen wird, was als Ermächtigung zu einem solchen Vorgehen gedeutet werden könnte. M. E. müsste auf § 14 in der oben unter 10. vorgeschlagenen Fassung Bezug genommen werden. Im vierten Bullet-Point von § 18 müsste es also heißen:

„zur Aufklärung eines strafrechtlich relevanten Sachverhalts unter zwingender Einbeziehung des zuständigen Betriebsrats, sofern die Voraussetzungen des § 14 Abs.1 gegeben sind."

15. Rollen und Berechtigungskonzepte

Die Bestimmung des § 19 ist inhaltlich zu begrüßen, weil sie den Gedanken der Datensparsamkeit auf den Umfang von Zugriffsberechtigungen erstreckt. Die Überprüfung durch die interne Revision ist ebenfalls in Ordnung, doch könnte man sich eine entsprechende Vorschrift zugunsten des zuständigen Betriebsrats durchaus vorstellen. Darauf wird unter III noch zurückzukommen sein.

16. Information der Beschäftigten

Nur wenige Veränderungen kommen bei § 21 in Frage.

In Abs. 1 müsste von „Beschäftigtendatenschutz" statt von „Arbeitnehmerdatenschutz" die Rede sein; zur Begründung kann auf das unter 2. Gesagte verwiesen werden.

Der Auskunftsanspruch nach Abs.2 ergibt sich an sich schon aus § 34 BDSG. Ihn zeitlich zu strecken (und damit – bösartige Menschen unterstellt – viel Raum für Manipulationen zu lassen) besteht kein Anlass. Auch ist es wegen § 6 Abs. 1 BDSG unzulässig, den Informationsanspruch nach § 34 zu verkürzen.

Dazu Dix, in: Simitis (Hrsg.), Bundesdatenschutzgesetz. Kommentar, 7. Aufl., Baden-Baden 2011, § 6 Rn 3 ff.

Ich würde deshalb folgende Formulierung vorschlagen:

„(2) Auf Antrag/Anfrage des Beschäftigten auf detaillierte Datenauskunft nach § 34 BDSG hat die verantwortliche Stelle diese unverzüglich, spätestens innerhalb eines Zeitraums von maximal vier Wochen ab Eingang des Ersuchens zu erteilen."

Man könnte auch einfacher formulieren:

„(2) Der Beschäftigte hat nach § 34 BDSG ein Auskunftsrecht in Bezug auf alle zu seiner Person gespeicherten Daten. Macht er davon in Bezug auf einen bestimmten Bereich oder generell Gebrauch, so ist ihm die Auskunft unverzüglich, spätestens innerhalb von vier Wochen nach Eingang seines Ersuchens zu gewähren."

Die Einschaltung des betrieblichen Datenschutzbeauftragten bringt inhaltlich nicht viel, verzögert aber das Verfahren. Je länger man warten muss, bevor man eine Auskunft in Händen hält, umso weniger wird man von diesem Recht Gebrauch machen.

Abs. 3 betrifft die sog. Datenpannen, die seit 2009 in § 42a BDSG geregelt sind. Die Regelung ist inhaltlich in Ordnung, doch sollte die verantwortliche Stelle nicht nur den betrieblichen Datenschutzbeauftragten und den betroffenen Beschäftigten, sondern auch den Betriebsrat in Kenntnis setzen. Dies rechtfertigt sich schon dadurch, dass häufig auch seine Mitbestimmungsrechte nach § 87 Abs.1 Nr. 6 BetrVG betroffen sind. Werden beispielsweise Beschäftigtendaten unbefugterweise an Dritte wie z. B. eine Detektei weitergegeben, so kann dies geeignet sein, Verhalten und Leistung der Arbeitnehmer wirksamer zu überwachen.

17. Einführung oder Änderung von IT-Systemen

Sehr zu begrüßen ist die Regelung des Abs.1, wonach der zuständige Betriebsrat so rechtzeitig informiert werden muss, dass er noch Gestaltungsalternativen einbringen kann. Geschieht dies nicht (eine Frage, die nicht angesprochen ist), kann die Fortführung des Projekts wohl durch einstweilige Verfügung untersagt werden, bis die Beteiligung des Betriebsrats nachgeholt ist. Dies dürfte aber schwerlich im Text der Betriebsvereinbarung unterzubringen sein.

Was den ebenfalls in Abs.1 angesprochenen Informationsanspruch des Betriebsrats angeht, so ist die Liste mit den einzelnen Punkten durchaus beeindruckend. Dennoch würde ich ein „insbesondere" vor „folgende Informationen" einfügen, da man nicht

wissen kann, ob bei einem neuen System Dinge eine Rolle spielen, die nicht in der Liste enthalten sind.

Abs. 3 betrifft den Probebetrieb. Die Rolle des Betriebsrats ist dabei recht unbestimmt umschrieben. Der Funktionsumfang soll vorab mit ihm „abgestimmt“ sein, er ist an der Überprüfung der Systemfunktionen „beteiligt“. Was heißt das konkret? Beide Begriffe finden sich nicht im Gesetz. Warum soll man kein Zustimmungsrecht des Betriebsrats vorsehen?

Erfreulich ist die Bestimmung des Abs. 5, die eine Freischaltung grundsätzlich erst nach beendeter Qualifizierung vorsieht.

18. Umgang mit Verstößen

Die Vorschrift ist wie viele andere grundsätzlich zu begrüßen.

Das in Abs.1 enthaltene Verwertungsverbot ist wichtig, weil die Rechtsprechung etwa beim Verstoß gegen Mitbestimmungsrechte nicht immer konsequent ist und zum Teil eine Verwertung zulässt. Gerade deshalb sollte Abs. 1 noch kategorischer gefasst werden. Eine Verwertung rechtswidrig erlangter Informationen sollte generell und nicht nur gegenüber dem Betroffenen ausgeschlossen werden. Außerdem sollte man klarstellen, dass „rechtswidrig erlangt“ auch solche Beschäftigtendaten sind, bei deren Gewinnung die Rechte des Betriebsrats übergangen wurden. Ich würde deshalb formulieren:

„(1) Beschäftigtendaten, die rechtswidrig erlangt wurden, dürfen nicht verwendet werden. Rechtswidrig erlangt sind auch solche Daten, bei deren Gewinnung Rechte des Betriebsrats nicht beachtet wurden.“

Was die weiteren Sanktionen angeht, so könnte man noch hinzufügen, dass Schadensersatzansprüche unberührt bleiben. Formulierungsvorschlag:

„(4) Schadensersatzansprüche des Betroffenen, auch solche aus § 7 BDSG, bleiben unberührt.“

III. Kontrollrechte des Betriebsrats

Gute datenschutzrechtliche Regelungen erfüllen nur dann ihre Funktion, wenn ihre Einhaltung kontrolliert werden kann. Insoweit könnte man den § 23 des Entwurfs erweitern und eine effektive Kontrollkompetenz etablieren. Zu denken wäre etwa an folgende Regelungen:

1. Online-Zugriff

Für den Betriebsrat kann es wichtig sein, auf bestimmte Dateien selbst zugreifen zu können, ohne erst den Umweg über die Personalabteilung gehen zu müssen. Dies erleichtert nicht nur die Gewinnung von Informationen, sondern versetzt den Betriebsrat auch in die Rolle, ohne jede „Zwischenschaltung" anderer Instanzen die Einhaltung des Datenschutzrechts und der vorliegenden Betriebsvereinbarung überprüfen zu können. Dabei wäre er selbstredend auf ein Leserecht beschränkt, das ja in § 15 Abs. 9 durchaus vorkommt – allerdings zugunsten eines Teils des Managements. Welche Dateien man dabei aussucht, ist eine Frage der betrieblichen Verhältnisse und des Verhandlungsprozesses. In einem Bremer Beispiel waren dies insbesondere Dateien zum Arbeitsschutz und zu den Kommens- und Gehenszeiten, weil diese erkennen lassen, ob Überstunden abgeleistet wurden, die der Zustimmung des Betriebsrats bedurft hätten. Eine Musterbetriebsvereinbarung sieht deshalb vor:

„Dem Betriebsrat wird ein direkter Zugriff auf folgende Datenarten eingeräumt:

- Anwesenheitszeiten der Arbeitnehmer,
- Gefährdungsanalysen
- ….."

2. Kontrolle der Zugriffsberechtigungen

Einen besonders sensiblen Bereich stellen die Zugriffsberechtigungen von einzelnen Beschäftigten (einschließlich des Vorstands) auf bestimmte Datenbestände dar. Sind insoweit die gesetzlichen und die durch die KBV vorgeschriebenen Grenzen eingehalten? Oder kommen bestimmte Personen auch an solche Dateien ran, mit denen sie eigentlich

gar nichts zu tun haben? Die erwähnte Musterbetriebsvereinbarung (die mit diesem Inhalt einvernehmlich in einer Einigungsstelle beschlossen wurde) sieht folgende Regelung vor:

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

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

Der direkte Zugang zu den mit EDV befassten Mitarbeitern ist aus dem Gesetz nicht herleitbar, da Adressat für das Auskunftsrecht nach § 80 Abs.2 BetrVG der Arbeitgeber als solcher ist, der bestimmt, welche konkrete Person die Information erteilt. Durch Betriebsvereinbarung lässt sich jedoch auch eine andere Handhabung vorsehen. Dass man dabei den Betriebsrat ermächtigen kann, in eigener Verantwortung Weisungen zu erteilen, wird u. a. an der Rechtsprechung des BAG deutlich, wonach dem Betriebsrat die Alleinverwaltung von betrieblichen Sozialeinrichtungen übertragen werden darf.

BAG 24. 4. 1986, AP Nr. 7 zu § 87 BetrVG 1972 Sozialeinrichtung

Ob eine entsprechende Regelung durchsetzbar ist, ob man insbesondere auch die Arbeitsplätze leitender Angestellter und der Geschäftsführung einbeziehen kann, steht auf einem anderen Blatt. Im konkreten Fall vertrat die Geschäftsführung den Standpunkt, sie habe nichts zu verbergen und könne durch eine solche Regelung mehr Vertrauen schaffen. Für den Betriebsrat war auch die Überlegung maßgebend, in einem – wenn auch sehr kleinen – Bereich die betriebliche Hierarchie zu durchbrechen.

3.Eigenqualifizierung von Betriebsratsmitgliedern

Kontrollrechte sind für den Betriebsrat nur dann von Nutzen, wenn er selbst über die nötige Sachkunde verfügt, um Risiken und technische Umgehungsmöglichkeiten einschätzen zu können. Deshalb sieht die Betriebsvereinbarung vor, dass bei der Einführung neuer Systeme zwei seiner Mitglieder in gleicher Weise informiert und geschult werden müssen wie diejenigen, die unmittelbar mit dem System zu arbeiten haben. Dies ist im Zusammenhang mit den Informationsrechten des Betriebsrats im Allgemeinen festgelegt, wo es heißt:

„(1) Die Benutzer von neuen oder geänderten IuK-Systemen werden rechtzeitig vor ihrem Einsatz im Rahmen des Erforderlichen für ihre Aufgabe geschult; dabei sind die §§ 96 bis 98 BetrVG zu beachten. Die Benutzer sind berechtigt, Vorschläge für die Gestaltung der Arbeitsplätze und der Arbeitsabläufe zu machen.

(2)Die Qualifizierungsmaßnahmen nach Abs. 1 müssen über die für die Bedienung erforderlichen Kenntnisse hinaus einen Einblick in die Funktionsweise des Systems geben und seine Bedeutung innerhalb der betrieblichen Arbeitsabläufe deutlich machen. Auch ist auf die Erkenntnisse ergonomischer Arbeitsgestaltung hinzuweisen.

(3)Die Qualifizierungsmaßnahmen sind in engem zeitlichem Zusammenhang mit der geplanten Einführung bzw. der Änderung durchzuführen. Im Rahmen des Erforderlichen sind sie zu wiederholen. Sie finden grundsätzlich während der Arbeitszeit statt. Die Kosten trägt der Arbeitgeber.

(4)Bis zu zwei Mitglieder des Betriebsrats, die an einer betrieblichen Arbeitsgruppe zur Vorbereitung der Einführung oder Änderung eines Systems beteiligt sind, können an den erforderlichen Qualifizierungs- und Schulungsmaßnahmen teilnehmen. § 37 Abs.6 und 7 BetrVG bleibt unberührt.

(5)Jedem Benutzer von IuK-Systemen sind die notwendigen Trainingsunterlagen in deutscher Sprache zur Verfügung zu stellen. Außerdem ist jederzeit eine qualifizierte

Betreuung bei der Anwendung des Systems zu gewährleisten. Das Beschwerderecht nach den §§ 84, 85 BetrVG bleibt unberührt.
(6)Mit dem Abschluss dieser Vereinbarung sind alle Anwender und ihre Vorgesetzten verpflichtet, regelmäßig an Seminaren teilzunehmen, die der betriebliche Datenschutzbeauftragte nach § 4g Abs.1 Satz 4 Nr. 2 BDSG anbietet. In einem Zyklus von etwa zwei Jahren findet eine Auffrischung des Wissens über den betrieblichen Datenschutz sowie eine Information über neue gesetzliche oder interne Regelungen statt. Die Teilnahme an den Veranstaltungen nach Satz 1 und 2 wird durch schriftliche Bestätigung dokumentiert."

Entscheidend kommt es im vorliegenden Zusammenhang auf Abs. 4 an. Die anderen Bestimmungen könnten ggf. in die Regelungen des § 22 integriert werden.

4. Unterstützung durch Experten

Denkbar ist, dass der Betriebsrat trotz seiner Auskunftsrechte noch ein Informationsdefizit besitzt. Für solche Fälle muss ihm der Rückgriff auf einen Experten möglich sein. Das gesetzliche Verfahren nach § 80 Abs.3 BetrVG ist schwerfällig, wenn der Arbeitgeber sein Einverständnis verweigert: In einem solchen Fall muss dann erst ein arbeitsgerichtliches Beschlussverfahren durchgeführt werden, das häufig erst zu einem Abschluss kommt, wenn längst vollendete Tatsachen geschaffen sind. Deshalb sollte ein einfacherer Weg beschritten werden. Man könnte etwa formulieren:

„Fehlt dem Betriebsrat nach seiner Einschätzung die nötige Sachkunde, um ein Projekt oder ein auftauchendes Problem beurteilen zu können, so muss er sich an die zuständigen innerbetrieblichen Stellen wenden. Hält er deren Auskunft für nicht ausreichend, kann er sich der Hilfe eines externen Sachverständigen bedienen. Die Kosten hierfür trägt der Arbeitsgeber."

5. Vorschlag

§ 23 könnte wie folgt ergänzt werden:

„(1) Der zuständige Betriebsrat kann nach § 80 Abs.2 BetrVG alle Informationen verlangen, die er für die Ausübung seiner Befugnisse und zur Durchführung dieser Betriebsvereinbarung benötigt. Er hat außerdem das Recht, die mit Datenverarbeitung befassten Arbeitnehmer über die Einhaltung der bestehenden datenschutzrechtlichen Regeln zu befragen. Diese müssen ggf. bestimmte Anwendungen zu Prüfzwecken durchführen, soweit dies der Betriebsrat verlangt. Der Vorgesetzte ist vorher zu informieren.

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

(3) Dem Betriebsrat wird ein direkter Zugriff auf folgende Datenarten eingeräumt:

- Anwesenheitszeiten der Arbeitnehmer,
- Gefährdungsanalysen

  …..

(4) Wie bisher Abs. 3

(5) Der Betriebsrat kann jederzeit Einblick in das vom betrieblichen Datenschutzbeauftragten nach § 4g Abs.2 BDSG geführte Verfahrensverzeichnis nehmen. Der Arbeitgeber sorgt dafür, dass dieses vollständig ist und sich auf dem neuesten Stand befindet.

(6) Wie bisher Abs. 5

(7) Wird ein neues IT-System eingeführt oder ein bestehendes geändert, so können bis zu zwei Mitglieder des zuständigen Betriebsrats an den aus diesem Anlass stattfindenden Informations- und Schulungsveranstaltungen teilnehmen.

(8) Fehlt dem Betriebsrat nach seiner Einschätzung die nötige Sachkunde, um ein Projekt oder ein auftauchendes Problem beurteilen zu können, so muss er sich an die zuständigen innerbetrieblichen Stellen wenden. Hält er deren Auskunft für nicht ausreichend, kann er sich der Hilfe eines externen Sachverständigen bedienen. Die Kosten hierfür trägt der Arbeitsgeber."

Der neue Abs. 5 trägt der Tatsache Rechnung, dass der Datenschutzbeauftragte ein Verfahrensverzeichnis führen muss, das in wesentlichen Punkten nach § 4g Abs.2 Satz 2 BDSG öffentlich zugänglich ist. Es fällt daher nicht aus dem Rahmen, wenn der Betriebsrat jederzeit Einsicht nehmen kann und dabei als innerbetriebliche Instanz auch diejenigen Teile wie Zugriffsberechtigungen und Datensicherungsmaßnahmen zu Gesicht bekommt, die nicht zur Veröffentlichung bestimmt sind.

Abs. 2 ist nicht aufgegriffen worden, da das Informationsrecht des Betriebsrats nicht davon abhängt, ob der Verdacht eines Verstoßes gegen datenschutzrechtliche Normen besteht. Erforderlich ist lediglich ein Aufgabenbezug.

Fitting, a. a. O., § 80 Rn. 51 ff., m. w. N.

Inwieweit es möglich ist, den § 23 in der hier vorgeschlagenen Weise umzugestalten, kann aus Sicht des Verfassers nicht beurteilt werden.