

Überwachung und Datenschutz im Betrieb

Ein ganz normaler Arbeitstag von Gaby B.

Als Gaby B. mit ihrem Pkw auf den unternehmenseigenem Parkplatz fährt, wird sie zum ersten Mal von den betrieblichen IT-Systemen erfasst. Die Videoanlage scannt ihr Nummernschild, und auf dem Weg vom Parkplatz zum Personaleingang stemgelt sie mit ihrer RFID-Chipkarte ihre Kommt-Arbeitszeit. Angeblich aus Sicherheitsgründen sind die Firmenabteilungen in Sicherheitszonen aufgeteilt, und sie muss zweimal das Zugangssystem bedienen. Gaby B. ist Einkaufssachbearbeiterin in einer großen Industrieverwaltung. In ihrem Büro angekommen, fährt sie ihren PC hoch und startet die wichtigsten Programme. Obwohl es noch recht früh ist, liegen bereits drei neue E-Mails von Lieferanten vor. Sie werden automatisch den zugehörigen elektronischen Vorgangsakten zugeordnet und die Arbeitsvorgänge chronologisch mit allen Schreiben, Notizen und E-Mails dokumentiert. In der IT-Abteilung läuft zurzeit ein Projekt, das auch die ein- und abgehenden Telefonate mit Lieferanten den elektronischen Akten zuordnen soll. Jeder Kunden- oder Lieferantkontakt soll dokumentiert werden. Ein Lieferant hat den vorgeschlagenen Gesprächstermin am Nachmittag bestätigt, und Gaby B. trägt ihn in den elektronischen Terminkalender ein.

Gaby B. ist in einem Projekt beteiligt, das die Lieferantenauswahl und -bewertung verbessern soll. Zur Planung und Dokumentation der Aktivitäten ist ein entsprechendes Projektmanagementsystem angelegt worden, in dem ihre Arbeitspakete mit Zeitvorgaben geplant sind und sie ihre *Ist*-Zeiten zurückmelden muss. In einer E-Mail mahnt der Projektleiter einige Arbeitsergebnisse an. Gaby B. ist bereits wieder in Verzug.

Nachdem sie einige dringende Bestellvorgänge am Computer bearbeitet hat, mit internen und externen Telefonaten, muss sie zu einer Dienstbesprechung. Seit einem halben Jahr verfügt sie über ein Notebook, wobei ihr bekannt ist, dass die Position des Notebooks im betrieblichen WLAN permanent geortet werden kann. Beim Weg zum Besprechungsraum muss sie wiederum das Zugangssystem füttern. Zum Glück ist während der Besprechungen die Nutzung von PDAs, oder Blackberry-Geräten verboten. Ihr ist vom Unternehmen auch noch keins zur Verfügung gestellt worden – was sie eher als Vorteil empfindet, da sie nicht permanent, womöglich auch in ihrer privaten Zeit, erreichbar ist. In der kurzen Besprechungspause rufen viele Beschäftigte ihre Handys oder PDAs ab, zum Plausch verbleibt kaum Zeit. Die Raucher müssen das Verwaltungsgebäude verlassen und hierzu ihre Arbeitszeit aus- und einstempeln.

Nach der Mittagspause nimmt Gaby B. sich etwas Zeit, um sich auf das vierteljährliche Zielvereinbarungsgespräch mit ihrem Chef vorzubereiten. Dbei spielen einige Produktivitätskennzahlen eine immer wichtigere Rolle. Sie werden aus den IT-Systemen personen- und abteilungsbezogen erhoben und analysiert.

Nachmittags hat Gaby B. noch einen externen Lieferantentermin, um sich von der Qualität einiger Einkaufsprodukte zu über-

zeugen. Ihren Dienstreiseantrag hat sie bereits am Tag zuvor mit dem Work-Flow-System gestellt, und er ist vom Vorgesetzten genehmigt. Zudem hat sie aus der Unternehmensflotte einen PKW geordert. Die Fahrzeuge sind alle mit einem Navigations- und GPS-System ausgestattet. Das erleichtert zwar die Abrechnung der Reisekosten bei längeren Dienstreisen, dient jedoch zugleich zur Überprüfung der Arbeitszeiten und der gefahrenen Kilometer. Er ist bekannt, dass bei ihrem Unternehmen „nur“ alle 5 Minuten die Position des PKWs dokumentiert wird. Gegen Ende des Termins wird sie von ihrem Vorgesetzten angerufen. Sie sei ja nur wenige Kilometer von einem weiteren Lieferanten entfernt, er fordert sie auf, diesen Lieferanten noch wegen einer Reklamation zu besuchen. Mit einem angemessenen Arbeitsende wird es da wohl nichts.

Gaby B. hat einen guten Bekannten in der IT-Abteilung. Daher weiß sie, dass das Unternehmen ein IT-Projekt realisiert und eine gewaltige zentrale Datenbank als *Data Warehouse* aufgebaut hat. Hier werden nahezu alle Kunden- und Lieferantenvorgänge und somit auch die Beschäftigentransaktionen zentral gespeichert. Wegen der zahlreichen Auswertungs- und Nutzungsmöglichkeiten gibt es wohl noch Ärger mit dem Betriebsrat und dem betrieblichen Datenschutzbeauftragten. Einige Programmierer der IT-Abteilung haben informell ein kleines Auswertungsprogramm erstellt, das für jede Abteilung, aber auch für einzelne Beschäftigte, die Anzahl der IT-Spuren in diesem Data Warehouse pro Tag aufzählt. Bei Gaby B. waren es an diesem Tag 183 Einträge.

Zielsetzungen, betriebliche Regelungen und Mitbestimmungsmöglichkeiten des Betriebsrates bei IT-Überwachung

Die rechtliche Handlungsgrundlage des Betriebsrats ist das Betriebsverfassungsgesetz. Zugespitzt formuliert gewährt es dem Betriebsrat relativ umfassende Informationsansprüche gegenüber dem Arbeitgeber und, z.B. in sozialen Angelegenheiten, eingeschränkte Mitbestimmungsrechte. Im Rahmen dieser Rechte hat der Betriebsrat die allgemeine Aufgabe und das Recht, „darüber zu wachen, dass die zu Gunsten der Arbeitnehmer geltenden Gesetze, Verordnungen, ... Tarifverträge und Betriebsvereinbarungen durchgeführt werden“ (§ 80(1) BetrVG). Hierzu gehören natürlich die Regelungen des Bundesdatenschutzgesetzes BDSG und weiterer Datenschutzgesetze. Der Betriebsrat hat jedoch kein echtes Mitbestimmungsrecht bei der Umsetzung. Er kann sich im Zweifelsfall an die staatlichen Aufsichtsbehörden wenden, z.B. in NRW angesiedelt beim Landesbeauftragten für Datenschutz und Informationsfreiheit (*Idi.nrw.de*).

Ein echtes Mitbestimmungsrecht besteht für den Betriebsrat im Rahmen des § 87(1)6 BetrVG bei der „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen“. Nach der gefestigten, erstmalig im Zusammenhang

mit dem Volkszählungsurteil im Dezember 1983 formulierten Rechtsprechung des Bundesarbeitsgerichts bedeutet das, dass der Betriebsrat bei der Einführung und Nutzung aller IT-Systeme mitzubestimmen hat, mit denen eine Verhaltenskontrolle möglich ist. Das betrifft in der Praxis alle IT-Programme, mit denen personenbezogene Daten von Arbeitnehmern gespeichert werden können, die Aussagen über das Verhalten (Tun oder Unterlassen) ermöglichen. Beispiele sind alle Computeraktivitäten, bei denen das Benutzerkennzeichen und Datum und Uhrzeit gespeichert werden, z.B. das Ein- oder Ausschalten von Hard- oder Software, die protokollierte Änderung von Stamm- oder Bewegungsdaten, das Versenden von E-Mails, Surfen im Internet usw. Da dies praktisch mit jeder Software erfolgt, unterliegt die Einführung jeder Software der Mitbestimmung des Betriebsrats – bezüglich dieses Überwachungsaspekts.

Es soll an dieser Stelle keine umfassende Aufzählung entsprechender Anwendungsprogramme erfolgen. Alle Beschäftigten in Verwaltungen haben Erfahrung mit solcher Software. Heutzutage wird in den Betrieben praktisch jede Aufgabe, jeder Arbeitsablauf mit Hilfe von IT-Systemen unterstützt – und entsprechend viele Datenspuren hinterlassen die Beschäftigten. Einen Eindruck sollte das Beispiel aus dem Arbeitstag von Gaby B. geben. Erschreckend ist dabei nicht nur die detaillierte Dokumentation einzelner Anwendungen, wie E-Mail, Telekommunikationssysteme, Sachbearbeitungssoftware, Projektverwaltung usw. Erschreckend sind vor allem die grundsätzlich bestehenden Verknüpfungsmöglichkeiten, auch wenn sie in der Praxis erst in Anfängen realisiert sind. Die „Vision“ des gläsernen Arbeitnehmers wird Monat für Monat realer. Davon sind vor allem Beschäftigte aus dem Verwaltungs- und Dienstleistungsbereich betroffen.

Für Betriebsräte stellt sich daher nicht die grundsätzliche Frage der Mitbestimmung, sondern die strategische und praktische Frage, wie die Mitbestimmungsrechte ausgestaltet und umgesetzt werden können. Bei der betrieblichen Regelung zu den IT-Überwachungsmöglichkeiten bestehen hierbei drei Hauptziele:

1. Die IT-Überwachung verhindern, begrenzen und mitgestalten,
2. die Beteiligung des Betriebsrates gewährleisten,
3. die Qualitätsstandards aus dem BDSG umsetzen.

Zu 1: Auch wenn die Überwachung der Beschäftigten in aller Regel nicht im Vordergrund des IT-Einsatzes steht, so steigt in den Betrieben der Leistungs- und Arbeitsdruck deutlich an, auch vor dem Hintergrund der wirtschaftlichen Rahmenbedingungen wie der Finanz- und Wirtschaftskrise. Ziel der Betriebsräte ist es, eine Leistungs- und Verhaltenskontrolle mit Hilfe der IT-Daten und -Auswertungen für die Beschäftigten zu verhindern. Häufig wird hierbei noch zu sehr auf einzelne IT-Anwendungen abgestellt, und anwendungssystemübergreifende Verknüpfungen und Auswertungsmöglichkeiten werden zu gering geachtet. Eine Zielformulierung lautet: *Mit Hilfe der IT-Daten und Auswertungen werden keine für die Beschäftigten negativen personellen Maßnahmen wie Abmahnungen, Versetzungen, Abgruppierungen oder Entlassungen begründet.* Diese Formulierung konnte mit Unterstützung der TBS-BeraterInnen in zahlreichen Betriebsvereinbarungen erreicht werden.

Weiterhin ist es wichtig, die einzuführenden IT-Anwendungen nicht als *gegeben* anzusehen. Häufig werden mit den IT-Anwendungen Organisationsvorstellungen und Menschenbilder transportiert, z.B. von eher wenig selbstständigen und streng zu kontrollierenden Beschäftigten. Entsprechend werden mit den Programmen detaillierte Vorgaben und genaue Kontrollen der Arbeitsergebnisse umgesetzt. Hier sind grundsätzliche Diskussionen zu den Einsatzkonzepten und den Gestaltungsoptionen von EDV-Anwendungen zu führen.

Zu 2: Die Mitbestimmung des Betriebsrats gilt nicht nur für die Einführung von Softwaresystemen. Der Betriebsrat muss im gesamten Prozess der Zielsetzung, Planung, Einführung (auch im Sinne von *Customizing*), Anwendung und Veränderung der Softwaresysteme und ihrer Auswirkungen auf die Arbeitsbedingungen der Beschäftigten beteiligt werden. Entsprechend werden unter dieser Zielsetzung vor dem Hintergrund der allgemeinen Regelungen des Betriebsverfassungsgesetz (BetrVG) die Beteiligungsrechte der Betriebsräte konkretisiert. Beispielsweise ist der Betriebsrat im Rahmen des Projektmanagements bei großen IT-Projekten z.B. in der Steuergruppe zu beteiligen. Er hat das Recht, die Einhaltung der Datenschutzgesetze und der betrieblichen Regelungen, z.B. zum Umfang der Datenspeicherung, der Protokollierung oder der Löschrufen zu überwachen. Schließlich werden seine Mitbestimmungsrechte konkretisiert, oder er hat das Recht, zu seiner Unterstützung einen technischen Sachverständigen hinzuzuziehen.

Der Betriebsrat soll den EDV-Einsatz jedoch nicht nur mitgestalten, sondern die Daten der IT-Systeme auch für seine Arbeit nutzen. In den IT-Systemen sind zahlreiche auch für die Betriebsratsarbeit hilfreiche Informationen gespeichert, wie Auftragseingänge, Produktsätze, Fehlzeiten, usw. Mit entsprechenden Leserechten kann der Betriebsrat diese Informationen zeitnah abrufen und strategisch nutzen.

Zu 3: Das Bundesdatenschutzgesetz bietet neben seinen grundlegenden rechtlichen Bestimmungen (z.B. zur Zweckbestimmung und Zweckbindung, Vorabkontrolle oder Verhältnismäßigkeit) eine Reihe praktischer Regelungen, die für die Betriebsratsarbeit und den Abschluss von Betriebsvereinbarungen sehr hilfreich sind. Mit dem Verfahrensverzeichnis ist der Arbeitgeber verpflichtet, eine Art Minimal-Dokumentation zu führen, die die Informationsrechte der Betriebsräte konkretisiert und ihre Umsetzung deutlich vereinfacht. Erfahrungsgemäß wird dieses Verfahrensverzeichnis in vielen Betrieben nicht vollständig oder aktuell gehalten. Löschrufen stehen häufig nur auf dem Papier und werden nicht umgesetzt. Weitere wichtige Regelungen sind natürlich die verpflichtenden technischen und organisatorischen Maßnahmen nach § 9 oder die Anforderungen an die Auftragsdatenverarbeitung nach § 11 BDSG. Die Übermittlung von Daten innerhalb von Unternehmensgruppen oder Konzernen ist für Beschäftigte und Betriebsräte tägliche Praxis und mit besonderen Problemen und Anforderungen verbunden. Wie werden Daten außerhalb der Betriebs- und Unternehmensgrenzen verknüpft und zu welchen Zwecken genutzt? Wer hatte Leserechte oder ist Empfänger? Wer entscheidet über personelle Maßnahmen? Die Probleme werden bei der Datenübermittlung in sogenannte Drittstaaten noch verschärft. Ziel ist es hier, die Standards der Datenschutzgesetze umzusetzen, Kontrollrechte der Betriebsräte

zu gewährleisten und insgesamt einen angemessenen Datenschutzstandard im Unternehmen zu erreichen.

Datenschutz für die Beschäftigten einzuhalten und insbesondere Überwachung zu verhindern, bedeutet in den Betrieben dicke Bretter zu bohren.

Referenz

Klaus Meyer Degenhardt (2009): IT-Beratung für Betriebs- und Personalräte
– notwendiger denn je, Bremen: FIF-Kommunikation 2/2009

Informationen zum Autor finden sich auf Seite 29.

*erschienen in der FIF-Kommunikation,
herausgegeben von FIF e.V. - ISSN 0938-3476
www.fiff.de*