11

Datenschutz und Mitbestimmung

Jens Kränke

Königswinterer Notizen

11

Datenschutz und Mitbestimmung

Jens Kränke

Anhang:
Beschäftigtendatenschutz – Eckpunkte für die geplante Regelung für den Umgang mit Beschäftigtendaten, BMI 31.03.2010

Königswinterer *Notizen*

Impressum

Königswinterer Notizen, Nr. 11, August 2014
Herausgeber: Stiftung Christlich-Soziale Politik e.V., (CSP)
Werner Schreiber, Vorsitzender
Johannes-Albers-Allee 3, 53639 Königswinter
Redaktion: Karsten Matthis und Josef Zolk
Tel. 02223-73119; E-Mail info@azk.de
Internet: www.azk.de
Produktion: TiPP 4, Rheinbach
Die Ausgaben der Königswinterer Notizen erscheinen
in unregelmäßigen Abständen.

Vorwort

Mit der raschen Zunahme an technischen und medialen Innovationen und den zahlreich bekannt gewordenen Fällen von Datenmissbrauch, entsteht bei den Bürgern ein Gefühl des Unbehagens oder Furcht davor, dass Daten über sie erstellt, verarbeitet und weitergeleitet werden, ohne deren Zustimmung oder Wissen.

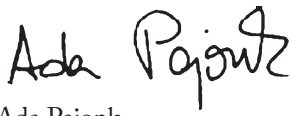
Es stellt sich die Frage, in wie weit die Verbreitung personenbezogener Daten mit Informationstechnik mit den demokratischen Strukturen unserer Verfassung und Gesellschaft vereinbar ist.

Der Bürger hat das Recht auf Selbstbestimmung in Bezug auf seine Daten. Diese Recht umfasst die Befugnis des Einzelnen "grundsätzlich selbst zu entscheiden, wann und innerhalb welcher Grenzen persönliche Sachverhalte offenbart werden." (BVerfGE 65, 1 (42)).

Der Datenschutz stellt in unserer Zeit, in der Daten schnell und mühelos verarbeitet und weitergeleitet werden, ein notwendiges Korrektiv der informationstechnischen Entwicklung dar.

Das Datenschutzgesetz soll den Einzelnen davor schützen, dass er durch den Umgang anderer mit seinen personenbezogenen Daten in seiner Persönlichkeit beeinträchtigt wird.

Denn, wenn wir als Bürger nicht einschätzen können, ob und zu welchen Zweck Daten über uns erhoben, gesammelt und verarbeitet werden, können wir nicht ausschließen, dass das gesammelte Wissen gegen uns eingesetzt wird. Das führt dazu, dass wir beginnen uns so unauffällig wie möglich zu geben und schließlich auf die Ausübung von Grundrechten verzichten. Das Recht, selbst über die Preisgabe seiner Daten zu entscheiden, ist daher auch eine elementare Funktionsbedingung einer demokratischen Gesellschaft, die gerade auf die Handlungs- und Mitwirkungsfähigkeit ihrer Bürger angewiesen ist.



Ada Pajonk
Bildungsreferentin CSP
Fachbereich Betriebs- und Personalräte

Einführung

Der Datenschutz rückt immer mehr in den Fokus des öffentlichen Bewusstseins und nicht erst seit der durch Edward Snowden aufgedeckten NSA-Affäre beschäftigen sich Arbeitnehmervertretungen mit Fragen, des Datenschutzes. Technische Weiterentwicklungen bei der Datenverarbeitung und gesetzliche Verpflichtungen zur Datenerhebung, Speicherung und Nutzung von Arbeitnehmerdaten rufen ganz zwangsläufig Mitbestimmungsakteure auf den Plan.

Datenschutz bedeutet, den Einzelnen davor zu schützen, dass durch den Umgang mit seinen personenbezogenen Daten seine Persönlichkeitsrechte beeinträchtigt werden. Sowohl das Betriebsverfassungsgesetz als auch das Bundespersonalvertretungsgesetz gibt den mitbestimmten Gremien Werkzeuge an die Hand, die Persönlichkeitsrechte der Beschäftigten wirksam zu schützen.

Nach Aufdeckung einiger vermeintlicher und tatsächlicher Datenschutzskandale in den Jahren 2008 und 2009 wurde der Ruf nach einem eigenen Arbeitnehmerdatenschutzgesetz lauter und führte schließlich zu einer Novellierung des bestehenden Bundesdatenschutzgesetzes, welches unter anderem um den § 32 ergänzt wurde. Bei dieser Norm handelt es sich um eine Regelung zur Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses. Sie trat am 1. September 2009 in Kraft. Aber auch diese Norm regelt die Datenverarbeitungen nicht in der wünschenswerten Tiefe, so dass Regelungen über Betriebs- und Dienstvereinbarungen aus Sicht eines wirksamen Datenschutzes zumindest solange notwendig erscheinen, bis der Gesetzgeber wirksame Schutznormen verabschiedet. Anfang 2010 hat das Bundesministerium des Innern den Regelungsbedarf erkannt und ein Eckpunktepapier zum Beschäftigtendatenschutz veröffentlicht. Dieses Papier benennt zwar die Themen Datenerhebung im Einstellungsverfahren, gesundheitliche Untersuchungen, Korruptionsbekämpfung, Videoüberwachung, Ortungssysteme, biometrische Verfahren und die Nutzung von Telefon, E-Mail und Internet am Arbeitsplatz, eine entsprechende gesetzliche Regelung indes ist bis heute ausgeblieben.

Neben dem Arbeitgeber trägt also auch der Betriebs- oder Personalrat die datenschutzrechtliche Verantwortung im Umgang mit den personenbezogenen Daten von Beschäftigten. Dieser Verantwortung ist durch entsprechende Regelungen über Betriebs- und Dienstvereinbarungen nachzukommen.

Datenschutzrechtliche Verantwortung

Diese Verantwortung bringt für den Bereich der Betriebsverfassung § 75 Abs. 2 BetrVG zum Ausdruck, wonach Arbeitgeber und Betriebsrat die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern haben. Für den Bereich der Personalvertretung ist § 68 Abs. 1 Nr. 2 BPersVG einschlägig, danach hat die Personalvertretung darüber zu wachen, dass die zugunsten der Beschäftigten geltenden Gesetze, Verordnungen, Tarifverträge, Dienstvereinbarungen und Verwaltungsanordnungen durchgeführt werden.

Um dieser Verantwortung überhaupt gerecht werden zu können, ist zunächst zu klären, welche Daten zu welchem Zeitpunkt und zu welchem Zweck über einen Beschäftigten wo und wie gespeichert werden.

Das Bundesdatenschutzgesetz verbietet grundsätzlich die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten, erlaubt sie aber unter bestimmten Voraussetzungen. Man spricht in diesem Zusammenhang von Erlaubnistatbeständen. Ein solcher Erlaubnistatbestand bildet bei Beschäftigungsverhältnissen regelmäßig die Bestimmung des § 32 BDSG. Danach dürfen personenbezogene Daten eines Beschäftigten 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. Hierbei ist darauf zu achten, dass die Speicherung von personenbezogenen Daten auf das unbedingt erforderliche Maß zu beschränken ist[1].

Typischerweise beginnt ein Beschäftigungsverhältnis nach Bewerbung mit dem Personalfragebogen, den die Kandidaten auszufüllen haben. Die hierbei anzugebenden Daten des Bewerbers bedürfen nach § 94 BetrVG bereits der Zustimmung des Betriebsrats. Der Gesetzgeber bindet den Betriebsrat also bewusst und zu einem sehr frühen Zeitpunkt in die datenver-

---

1 Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert, vgl. § 3a BDSG.

arbeitenden Prozesse ein. Auch die persönlichen Angaben, die in schriftlichen Arbeitsverträgen zu machen sind erfordern die Zustimmung des Betriebsrats. Der Betriebsrat hat insofern maßgeblichen Einfluss darauf, welche Daten zu welchem Zeitpunkt und zu welchem Zweck über einen Beschäftigten erhoben werden. Im Rahmen seiner Überwachungspflichten hat der Betriebs-, bzw. Personalrat aber weiter auch maßgeblichen Einfluss darauf, wo und wie die Daten gespeichert werden. § 9 BDSG verpflichtet die verantwortliche Stelle, also den Arbeitgeber, zur Schaffung von technischen und organisatorischen Maßnahmen, die den ordnungsgemäßen Ablauf der Datenverarbeitung durch Sicherung von Hard- und Software sowie von Daten vor Verlust, Beschädigung oder Missbrauch schützen sollen.

Die Kontrollmaßnahmen nach § 9 BDSG werden auch die „8 Gebote des Datenschutzes“ genannt und beschreiben so auch sprachlich die Wichtigkeit dieser Maßnahmen. Im Einzelnen versteht man darunter, dass

1. Unbefugten der körperliche Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, verwehrt wird.
2. die unbefugte Nutzung von Datenverarbeitungsanlagen, also dem Eindringen in das EDV-System seitens unbefugter Personen sowie die geregelte Zugriffskontrolle eines grundsätzlich Berechtigten zu verhindern ist.
3. nachträglichen überprüfbar ist, welche personenbezogenen Daten durch wen zu welcher Zeit in Datenvereinbarungssysteme eingegeben bzw. dort verändert oder auch gelöscht und entfernt worden sind.
4. die zur Benutzung Berechtigten nur auf die ihrer jeweiligen Berechtigung unterliegenden Daten zugreifen können.
5. die Daten vor zufälliger Zerstörung, bspw. Wasserschäden, Brand, Blitzschlag, Stromausfall usw. geschützt sind.
6. die zweckbestimmte Verarbeitung gesichert ist.
7. die im Auftrag zu verarbeitenden Daten nur entsprechend den Weisungen des Auftraggebers verarbeitet werden.
8. verhindert wird, dass Datenträger unbefugt gelesen, kopiert, verändert oder gelöscht werden können.

Die Personalakte

Der Arbeitgeber hat das Interesse, aber auch die Pflicht, Informationen über seine Beschäftigten zu speichern. Diese Informationen werden zur Personalakte genommen, wobei zur Personalakte alle Aufzeichnungen, die sich mit der Person des Arbeitnehmers und dem Inhalt und Verlauf seines Beschäftigungsverhältnisses befassen zählen und zwar unabhängig davon, in welcher Form oder unter welcher Bezeichnung die Daten gespeichert sind. Der Arbeitnehmer hat Interesse an der Richtigkeit über die zu seiner Person gespeicherten Daten. Daraus folgt, dass er sowohl einen Auskunftsanspruch über die über ihn gespeicherten Daten, als auch einen Korrekturanspruch gegenüber dem Arbeitgeber hat[2]. Der Betriebs-, bzw. Personalrat fördert dabei die Persönlichkeitsrechte der Beschäftigten durch seine Kontroll- und Einflussmöglichkeiten. Hierbei steht ihm jedoch kein generelles, von konkreten, gesetzlich zugewiesenen Aufgaben losgelöstes Informationsrecht durch Zugriff auf die Personalakten oder ein Personalinformationssystem zu.

Die Führung der Personalakte erfordert Transparenz, Richtigkeit, Zulässigkeit und Vertraulichkeit. Insbesondere bei der Frage nach der Zulässigkeit von Datenerhebungen von Beschäftigten ergeben sich für mitbestimmte Gremien Einflussmöglichkeiten. Prominenteste Norm bildet hierbei wohl § 87 Abs. 1 Nr. 6 BetrVG, wonach der Betriebsrat, soweit eine gesetzliche oder tarifliche Regelung nicht besteht, bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen, mitzubestimmen hat.

Im Zuge des technischen Fortschritts sehen sich Betriebs- und Personalräte mit immer neuen Überwachungsmöglichkeiten konfrontiert. Allein die bloße Nutzung von EDV-Systemen produziert eine Unmenge von Daten in Form von Log-Files, die auch Aufschluss über das Verhalten und die Leistung des jeweiligen Arbeitnehmers geben können. Kommen jetzt noch

---

2 Der Arbeitnehmer hat das Recht, in die über ihn geführten Personalakten Einsicht zu nehmen. Er kann hierzu ein Mitglied des Betriebsrats hinzuziehen. Das Mitglied des Betriebsrats hat über den Inhalt der Personalakte Stillschweigen zu bewahren, soweit es vom Arbeitnehmer im Einzelfall nicht von dieser Verpflichtung entbunden wird. Erklärungen des Arbeitnehmers zum Inhalt der Personalakte sind dieser auf sein Verlangen beizufügen, vgl. § 83 BetrVG.

Daten über die Internet- und E-Mail Nutzung des Betroffenen am multimedialen Arbeitsplatz hinzu, lässt sich ein immer genaueres Bild über den Arbeitnehmer zeichnen und vielleicht noch durch Videoüberwachungen, Ortungssysteme und Telekommunikationsdaten ergänzen. Dabei ist nun zu berücksichtigen, dass dem Arbeitgeber gesetzliche Pflichten auferlegt wurden und nicht grundsätzlich jede Maßnahme dazu dient, den Arbeitnehmer zu überwachen. Schon aus den zu treffenden Maßnahmen zur IT-Sicherheit ergeben sich für den Arbeitgeber Protokollierungspflichten, es sind staatliche Statistiken zu führen, „Anti-Terror"-Richtlinien[3] und Compliance Anforderungen zu beachten.

Die Herausforderung für die Betriebsparteien liegt nun darin, den Spagat zwischen den datenschutzrechtlichen Belangen des Arbeitnehmers einerseits und dem Informationsinteresse des Arbeitgebers andererseits zu schaffen.

Regelungsgegenstände

Das Betriebsverfassungsgesetz verpflichtet beide Betriebsparteien, die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen und zu fördern[4] und scheibt dem Betriebsrat vor, darüber zu wachen, dass die zugunsten der Arbeitnehmer geltenden Gesetze, Verordnungen und Betriebsvereinbarungen durchgeführt werden[5]. Das Bundesministerium des Innern hat bereits in seinem Eckpunktepapier zum Beschäftigtendatenschutz ausgeführt, dass spezialgesetzliche Regelungen zu Datenerhebungen in Beschäftigtenverhältnissen weitestgehend fehlen, soweit Regelungen vorhanden seien, so fänden sich diese verteilt über verschiedene Gesetze. In Ermangelung dieser gesetzlichen Regelungen wird in der betrieblichen Praxis wohl auf die leider nicht immer einheitliche Rechtsprechung der Arbeitsgerichte oder den selteneren obergerichtlichen Urteile abzustellen sein. Neben diesen Fundstellen bieten Betriebs- oder Dienstver-

---

3 Ermittlung von Personen, Gruppen und Organisationen, für die aufgrund einer Sanktion ein umfassendes Verfügungsverbot besteht, vgl. EU-Verordnung 881/2002.

4 Vgl. § 75 Abs. 2 BetrVG

5 Vgl. § 80 Abs. 1 BetrVG

einbarungen betriebsinterne Regelungsmöglichkeiten über den Datenumgang. Dieses Beteiligungsrecht ist zugleich auch Rechtmäßigkeitsvoraussetzung für die Datenerhebung insgesamt. Ein kollektivrechtlicher Rechtsverstoß wirkt als Verarbeitungs- bzw. Erhebungssperre und löst die entsprechenden Korrekturrechte der betroffenen Beschäftigten auf Löschung oder Unterlassung aus. Mit § 87 Abs. 1 Nr. 6 BetrVG gibt der Gesetzgeber dem Betriebsrat das entsprechende Beteiligungsrecht an die Hand. Hiernach hat der Betriebsrat bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen mitzubestimmen.

Die umfangreichen Beteiligungsrechte von Betriebs- und Personalräten im Zusammenhang mit der Erhebung, Verarbeitung und Nutzung von Beschäftigtendaten können hier natürlich nicht abschließend dargelegt werden, so dass nachfolgend exemplarisch auf die immer wiederkehrenden Fragen aus meiner Beratungspraxis eingegangen wird.

Internet und E-Mail

Das Landesarbeitsgericht Niedersachsen hatte sich mit einem Arbeitnehmer zu beschäftigen, der als stellvertretender Leiter eines Bauamts tätig war und seinen Arbeitsplatzrechner ausgiebig für die private E-Mail-Kommunikation nutzte. Mit mindestens zehn verschiedenen Kontaktvermittlern pflegte er Kontakt. Auf seinem Rechner hatte er auch Kontaktbriefe mit erotischem Inhalt und sogar pornografische Fotos abgelegt. Er nutzte so in großem Umfang seine Arbeitszeit zur Pflege seiner umfangreichen private Korrespondenz und seines privaten Fotoarchivs auf dem Dienstrechner[6]. Das Gericht bestätigte schließlich die außerordentliche Kündigung des Arbeitnehmers[7].

---

6 Landesarbeitsgericht Niedersachsen, Urteil vom 31.05.2010 - 12 SA 875/09 -

7 Leitsatz: Die außerordentliche Kündigung eines langjährig beschäftigten Arbeitnehmers kann auch ohne vorangegangene einschlägige Abmahnung gerechtfertigt sein, wenn der Mitarbeiter über einen Zeitraum von mehr als 7 Wochen arbeitstäglich mehrere Stunden mit dem Schreiben und Beantworten privater E-Mails verbringt – an mehreren Tagen sogar in einem zeitlichen Umfang, der gar keinen Raum für die Erledigung von Dienstaufgaben mehr lässt. Es handelt sich in einem solchen Fall um eine „exzessive" Privatnutzung des Dienst-PC.

Unabhängig davon, stellen sich vielfältige Fragen, wie mit privater Nutzung von Internet und E-Mail in Unternehmen umzugehen ist. Grundsätzlich sind dabei zwei Dinge auseinanderzuhalten.

Soweit der Arbeitgeber die private Nutzung des Internets und PC am Arbeitsplatz erlaubt hat, darf er diese nicht mehr überwachen, also zum Beispiel den privaten E-Mail-Verkehr nicht kontrollieren. Sonst würde er die Privatsphäre seiner Mitarbeiter verletzen. Ist die private Internet-Nutzung durch den Arbeitgeber jedoch nicht gestattet, darf er unter bestimmten Voraussetzungen überwachen, was Beschäftigte mit dem Arbeitsplatz-PC oder Firmen-Laptop machen. Dies wird damit begründet, dass eine unerlaubte private Internet-Nutzung letztlich einen Missbrauch der Arbeitszeit darstellt. Um dem zu begegnen, ist eine stichprobenartige Überprüfung durch den Arbeitgeber zulässig. Eine permanente Überwachung als eine Art elektronischer Leistungskontrolle ist aber nicht erlaubt.

In der betrieblichen Praxis empfiehlt sich die Aufstellung einer verbindlichen Richtlinie zur Internet und E-Mail Nutzung am Arbeitsplatz. In dieser Richtlinie sollte die private Nutzung der Internet und E-Mail Dienste ausdrücklich verboten werden, aber dann zulässig sein, wenn zuvor eine Vereinbarung über die genaue Ausgestaltung der Nutzung zwischen Arbeitgeber und Arbeitnehmer abgeschlossen wurde (Verbot mit Erlaubnisvorbehalt). In dieser Vereinbarung sollte dargelegt werden, dass zwischen privater und geschäftlicher Nutzung nicht unterschieden werden kann und der Arbeitnehmer dem Arbeitgeber insoweit ein Kontrollrecht zubilligt

Videoüberwachung

Im März 2008 wurde bekannt, dass über einen Zeitraum von mehr als zwei Jahren Lidl-Vertriebsgesellschaften in rund 80 Fällen die Beschäftigten mit Kameras bespitzelt haben. Die betroffenen Vertriebsgesellschaften mussten wegen erheblicher Datenschutzrechtsverletzungen knapp 1,5 Millionen Euro Bußgeld zahlen.

Nach § 75 Abs. 2 BetrVG hat der Betriebsrat die freie Entfaltung der Persönlichkeit der Arbeitnehmer zu schützen und zu fördern. Diese Vorschrift zielt auf den Schutz der Grundrechte der Arbeitnehmer ab. Der Betriebsrat hat dafür Sorge zu tragen, dass die Videoüberwachung dem Verhältnismäßigkeitsgrundsatz genügt und dass der Arbeitnehmer nicht in der

freien Entfaltung seiner Persönlichkeit gestört wird. So erzeugt schon die Möglichkeit der jederzeitigen Überwachung einen mit dem Anspruch des Arbeitnehmers auf Wahrung seiner Persönlichkeitsrechte regelmäßig nicht zu vereinbarenden Überwachungsdruck, so dass eine Videoüberwachung von Arbeitnehmern grundsätzlich unzulässig ist[8].

Bei der Beantwortung der Frage, ob die Videoüberwachungsanlage dazu bestimmt ist, den Arbeitnehmer zu überwachen[9], kommt es nicht darauf an, dass der Arbeitgeber die Videoüberwachung zur Kontrolle einsetzen will, sondern vielmehr darauf, ob sie dafür „objektiv" geeignet ist. Es reicht damit aus, dass die Mitarbeiterüberwachung nur ein „ungewollter Nebeneffekt" und nicht das eigentliche Beobachtungsobjekt ist[10]. Dies wäre zum Beispiel bei der Überwachung von Bereichen, in denen sich regelmäßig Arbeitnehmer aufhalten, zum Zwecke der Wahrnehmung des Hausrechts der Fall. Die bloße abstrakte Geeignetheit (z.B. die bloße Existenz einer Videokamera, von der Arbeitnehmer jedoch nicht erfasst werden) reicht jedoch für ein Mitbestimmungsrecht des Betriebsrates nicht aus.

Wird das Mitbestimmungsrecht nicht beachtet, ist die Videoüberwachung unzulässig. Manifestiert wird die Mitbestimmung des Betriebsrats durch den Beschluss einer entsprechenden Betriebsvereinbarung. In diesem Sinne hat der Betriebsrat auch ein Mitbestimmungsrecht hinsichtlich der Speicherdauer der Videodaten. Auch diese sollte in einer entsprechenden Betriebsvereinbarung festgehalten werden. Der innere Zusammenhang zwischen § 87 Abs. 1 Nr. 6 und § 75 Abs. 2 BetrVG gebietet es, bei Auslegungszweifeln über Inhalt und Grenzen des Mitbestimmungsrechts nach Nr. 6 derjenigen Auslegung den Vorzug zu geben, die den Persönlichkeitsschutz des einzelnen Arbeitnehmers am besten sichert.

Es bleibt festzuhalten, dass die Videoüberwachung von Arbeitnehmern grundsätzlich unzulässig ist, soweit weder die sich aus dem Betriebsverfassungsgesetz ergebenden Rechte und Pflichten des Betriebsrates beachtet werden noch eine Legitimation nach den Vorschriften des Bundesdatenschutzgesetzes besteht.

Nachfolgender Katalog stellt eine zusammenfassende Übersicht über

---

8 BAG, RDV 1992, 179

9 Vgl. § 87 Abs. 1 Nr. 6 BetrVG

10 Gola/Wronka, Handbuch zum Arbeitnehmerdatenschutz, Frechen 2004, Rz. 1074

die im Zusammenhang mit den Rechten des Betriebsrates zu beachtenden Punkte dar:

- Bezieht sich die Überwachung auf Bereiche, bei denen die Beobachtung von Mitarbeitern im Bereich ihrer Dienstausübung nicht ausgeschlossen werden kann, hat der Betriebsrat ein Mitbestimmungsrecht nach § 87 Abs. 1 Nr. 6 BetrVG.
- Ohne die Zustimmung des Betriebsrates ist die Videoüberwachungsmaßnahme unzulässig.
- Eine Speicherung der Daten darf nur dann stattfinden, wenn der Betriebsrat von seinem Mitbestimmungsrecht Gebrauch gemacht hat.
- Als Rechtsgrundlage bedarf es einer Betriebsvereinbarung, die die Zustimmung des Betriebsrates festhält.
- Aufgrund seiner Kontrollpflicht und dem Anspruch auf Information durch den Arbeitgeber nach § 80 Abs. 2 S. 1, S. 2 BetrVG sind dem Betriebsrat zudem Zugriffsrechte auf gespeicherte Videodaten zu gewähren. Diese sind ebenso wie der Umfang seiner Kontrollrechte in einer entsprechenden Betriebsvereinbarung zu regeln.
- Der Betriebsrat ist davon zu unterrichten, dass Videoüberwachungsmaßnahmen durchgeführt werden sollen und welchem Zweck diese dienen.

Zutrittskontrolle

Datenschutzrechtliches Ziel der Zutrittskontrolle ist es, mit Hilfe geeigneter Maßnahmen das Eindringen Unbefugter in Datenverarbeitungssysteme und deren Nutzung durch Unbefugte zu verhindern[11]. Natürlich gibt es auch für das Unternehmen auf der Hand liegende Gründe, nicht jedem Zutritt auf das Betriebsgelände zu gewähren, so dass der geregelte Zutritt auch durch technische Unterstützung gewährleistet wird. Auf dem Markt findet sich eine Vielzahl von Herstellern, die entsprechende Systeme mit unterschiedlichen Techniken anbieten. Neben Zutrittskarten die zumeist einen

11 Vgl. Anlage zu § 9 BDSG

RFID[12]-Chip beinhalten oder auf dem ein Magnetstreifen aufgeklebt ist, werden auch biometrische Verfahren wie bspw. Fingerabdruck, Iris- oder Netzhautscan, Handflächenabdruck, Handvenen oder Gesichtsmerkmale zur Identifikation eingesetzt. Allen Systemen gemein ist, dass der zum Zutritt Berechtigte zuvor definiert werden muss. Es entstehen also im Nachhinein auswertbare Daten, wer hat wann wo Zutritt erhalten oder wem wurde wann der Zutritt verwehrt. Gerade in größeren Organisationen mit anspruchsvollen Schließkonzepten können mit Hilfe dieser Kontrollmechanismen Bewegungsprofile des Arbeitnehmers im Unternehmen erstellt werden.

Zumindest dann, wenn die Installation eines Zugangssicherungssystems, das bei der Präsentation von codierten Ausweiskarten den Ein- oder Ausgang zu Betriebsräumen freigibt, festhält, wer wann in welcher Richtung den Zugang benutzt, unterliegt das Verfahren der Mitbestimmung des Betriebsrates.

Aus allein datenschutzrechtlicher Sicht, ist eine solche Installation vor dem Hintergrund der Datensicherheit ausdrücklich zu begrüßen. In der betrieblichen Praxis dürfte der Abschluss einer Betriebs-, bzw. Dienstvereinbarung notwendig sein. In einer solchen Vereinbarung wäre mindestens festzulegen, welche Datenkategorien erhoben werden (bspw. Personalnummer, Ausweis-Nummer/PIN-Code, Name und Vorname, Zuordnung der Ausweis-/PIN-Nummer zu einer bestimmten Person, Datum und Uhrzeit des Zutritts, Anzahl der Zutrittsversuche etc.) und an wen diese Daten weitergegeben werden, wer also darauf Zugriff nehmen kann. Daneben wäre zu bestimmen, unter welchen Voraussetzungen die Daten ausgewertet werden dürfen, welche Auswertungen technisch überhaupt möglich sind und wie lange die Daten gespeichert werden.

Der Datenschutzbeauftragte

Die Aufgaben des Datenschutzbeauftragten sind gesetzlich definiert. Nach § 4g BDSG wirkt der Beauftragte für den Datenschutz auf die Einhaltung des Bundesdatenschutzgesetzes und anderer Vorschriften über den Daten-

12 radio-frequency identification (Identifizierung mit Hilfe elektromagnetischer Wellen)

schutz hin. Er hat insbesondere die ordnungsgemäße Anwendung der Datenverarbeitungsprogramme, mit deren Hilfe personenbezogene Daten verarbeitet werden sollen, zu überwachen und hat weiter die bei der Verarbeitung personenbezogener Daten tätigen Personen durch geeignete Maßnahmen mit den Vorschriften des Bundesdatenschutzgesetzes sowie anderen Vorschriften über den Datenschutz und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen.

Der Datenschutzbeauftragte schützt also qua Gesetz, und zwar durch das Hinwirken auf die Einhaltung des Bundesdatenschutzgesetzes, auch die Persönlichkeitsrechte der Beschäftigten. Insoweit sind die Aufgaben von Betriebs-, bzw. Personalrat und dem Beauftragten für den Datenschutz in diesem Teilbereich deckungsgleich, obgleich häufig unterschiedliche Vorgehensweisen zu beobachten sind.

Eine enge Abstimmung für die Verarbeitung von Beschäftigtendaten zwischen Arbeitgeber, Personalvertretung und dem Beauftragen für den Datenschutz ist im Sinne eines wirksamen Schutzes dringend angeraten.

Über den Autor

Jens Kränke wurde 1969 in Hannover geboren, wuchs im Ruhrgebiet auf und machte sein Abitur auf dem Gelsenkirchener Abendgymnasium. Nach Studium der Politik- und Rechtswissenschaften in Münster und Bochum begann er seine berufliche Karriere bei QVC Deutschland. In der Funktion als Datenschutzauditor leistete er im Bereich des Versandhandels Pionierarbeit, als erstes Versandhandelsunternehmen überhaupt erhielt QVC Deutschland das Siegel „Geprüfter Datenschutz" des TÜV Rheinland. Als Konzerndatenschutzbeauftragter der QVC Deutschland Gruppe überwachte er später dort den gesetzeskonformen Umgang mit personenbezogenen Daten innerhalb des Gesamtkonzerns. Danach wechselte er als Senior Consultant Datenschutzmanagement in die Unternehmensberatung und beriet dort namhafte Unternehmen und Sozialversicherungsträger im Bereich des betrieblichen Datenschutzes, bzw. im Bereich des Sozialdatenschutzes. Im Jahre 2011 gründete er die LEXDATA GmbH zum Zwecke der interdisziplinären Unternehmensberatung für die Bereiche des Datenschutzes, der Datensicherheit, des Qualitätsmanagements und der Revision. Als vom Ministerium für Arbeit, Gesundheit und Soziales des Landes NRW sowie vom bayerischen Staatsministerium für Arbeit und Sozialordnung, Familien und Frauen als geeignet anerkannter Bildungsveranstalter ist Jens Kränke für mehrere Institutionen als Dozent für den Datenschutz tätig. Zusatzqualifikationen als Datenschutzauditor (TÜV), Datenschutzbeauftragter nach GDD cert. und Datenschutzbeauftragter nach dem Ulmer Modell (udis) runden sein Bild als fachkundigen Berater ab.

Wir danken dem Autor sehr herzlich für seinen Aufsatz „Datenschutz und Mitbestimmung" aus dem August 2014.

Beschäftigungsdatenschutz –Eckpunkte für die geplante Regelung für den Umgang mit Beschäftigtendaten.

Beschlossen am 31.03.2010 durch das Bundesministerium des Innern.

Ausgangslage und Regelungsbedarf

Seit Jahrzehnten wird über die Notwendigkeit gesetzlicher Regelungen für den Beschäftigtendatenschutz diskutiert. Verschiedene von der Öffentlichkeit stark diskutierte Vorfälle in den vergangenen Jahren – etwa in Unternehmen wie Lidl oder der Deutschen Bahn AG – zeigen, dass eine generelle Regelung des Beschäftigtendatenschutzes notwendig ist.

Es gibt bereits heute zu vielen Fragen des Beschäftigtendatenschutzes eine einzelfallbezogene Rechtsprechung der Arbeitsgerichte. Diese ist allerdings oft uneinheitlich. Obergerichtliche Urteile sind selten. Für zahlreiche in der beruflichen Praxis vorhandene Fragen bestehen derzeit keine speziellen gesetzlichen Regelungen. Soweit Regelungen vorhanden sind, finden sich diese verteilt über verschiedene Gesetze, etwa im Bundesdatenschutzgesetz, Betriebsverfassungsgesetz, Telekommunikationsgesetz oder dem Telemediengesetz.

Die Regierungsparteien haben sich im Koalitionsvertrag darauf verständigt, den Beschäftigtendatenschutz in einem eigenen Kapitel im Bundesdatenschutzgesetz gesetzlich zu regeln.

Auszug aus der Koalitionsvereinbarung vom 26. Oktober 2009 (S. 106):

> „Privatheit ist der Kern persönlicher Freiheit. Wir setzen uns für eine Verbesserung des Arbeitnehmerdatenschutzes ein und wollen Mitarbeiterinnen und Mitarbeiter vor Bespitzelungen an ihrem Arbeitsplatz wirksam schützen. Es dürfen nur solche Daten verarbeitet werden, die für das Arbeitsverhältnis erforderlich sind. Datenverarbeitungen, die sich beispielsweise auf für das Arbeitsverhältnis nicht relevantes außerdienstliches Verhalten oder auf nicht dienstrelevante Gesundheitszustände beziehen, müssen zukünftig ausgeschlossen sein. Es sollen praxisgerechte Regelungen

für Bewerber und Arbeitnehmer geschaffen und gleichzeitig Arbeitgebern eine verlässliche Regelung für den Kampf gegen Korruption an die Hand gegeben werden. Hierzu werden wir den Arbeitnehmerdatenschutz in einem eigenen Kapitel im Bundesdatenschutzgesetz ausgestalten."

Die Federführung hierfür liegt beim Bundesministerium des Innern.

Eckpunkte eines Beschäftigtendatenschutzes

Das Bundesministerium des Innern lässt sich bei der Erstellung eines Gesetzentwurfes zur Regelung des Beschäftigtendatenschutzes von folgenden Grundüberlegungen leiten:

- **Ziel einer gesetzlichen Regelung**
  Durch umfassende, allgemeingültige Regelungen für den Datenschutz am Arbeitsplatz soll die Rechtslage für Arbeitgeber und Beschäftigte gleichermaßen deutlich gemacht und insgesamt mehr Rechtssicherheit erreicht werden. Die Regelungen sollen sich auf die in der betrieblichen Praxis relevanten Datenschutzfragen konzentrieren und sich – soweit vorhanden – weitgehend an der Rechtsprechung der Arbeitsgerichte orientieren. Bestehende Schutzlücken sollen geschlossen werden. Kennzeichnend sollen dabei die Grundprinzipien der Transparenz und Erforderlichkeit sein. Daten, die für den Zweck, für den sie erhoben wurden, nicht mehr erforderlich sind, sollen danach gelöscht werden müssen.

- **Datenerhebung im Einstellungsverfahren**
  Das Fragerecht des Arbeitgebers soll gesetzlich geregelt werden. Der Arbeitgeber soll nur die Beschäftigtendaten erfragen dürfen, die er benötigt, um die Eignung des Bewerbers für eine in Betracht kommende Tätigkeit festzustellen.

  Beispiel:
  Darf der Arbeitgeber z.B. die Bewerberin um eine Anstellung als Buchhalterin fragen, ob sie wegen Unterschlagung vorbestraft ist? Wie ist es mit Vorstrafen wegen Körperver-

letzung? Bei einem Bewerber um eine Anstellung als Möbelpacker ist die Frage nach einer Rückenerkrankung sicher eher zulässig als die Frage, ob er schon einmal in psychologischer Behandlung war.

- **Gesundheitliche Untersuchungen**

Gesundheitliche Untersuchungen oder Prüfungen sollen nur zulässig sein, wenn sie erforderlich sind, um die Eignung für eine konkret vorgesehene Tätigkeit festzustellen. Sie sollen nur mit Einwilligung des Betroffenen und nach den Regeln der Fachkunde durchgeführt werden dürfen. Dem Arbeitgeber soll nur das Ergebnis mitgeteilt werden dürfen, ob der Beschäftigte für die zu besetzende Stelle geeignet ist, nicht jedoch die genaue ärztliche Diagnose im Einzelnen.

Beispiel:
Blutuntersuchungen sollen auf dieser Grundlage nur zulässig sein, soweit sie für die Eignungsfeststellung des Beschäftigten erforderlich sind. Dies kann der Fall sein zum Schutz des Beschäftigten vor gesundheitlichen Gefahren am Arbeitsplatz, z.B. wenn er bei seiner (vorgesehenen) Tätigkeit in Kontakt mit allergenen Stoffen kommt. Auch der Schutz Dritter kann eine Blutuntersuchung erfordern, z.B. bei einem Piloten, von dessen allgemeinem Gesundheitszustand die Sicherheit der Passagiere abhängt oder bei einem Chirurgen zur Feststellung, ob eine HIV-Infizierung vorliegt.

Eine Sekretärin müsste sich dagegen diesen Untersuchungen nicht unterziehen. Blutuntersuchungen zur Klärung, ob der Beschäftigte alkohol- oder drogenabhängig ist, sollen nicht routinemäßig zulässig sein.

- **Korruptionsbekämpfung/Durchsetzung von Compliance-Anforderungen**

Gesundheitliche Untersuchungen oder Prüfungen sollen nur zulässig sein, wenn sie erforderlich sind, um die Eignung für eine konkret vorgesehene Tätigkeit festzustellen. Sie sollen nur mit Einwilligung des

Betroffenen und nach den Regeln der Fachkunde durchgeführt werden dürfen. Dem Arbeitgeber soll nur das Ergebnis mitgeteilt werden dürfen, ob der Beschäftigte für die zu besetzende Stelle geeignet ist, nicht jedoch die genaue ärztliche Diagnose im Einzelnen.

- **Videoüberwachung**

Ganz allgemein soll die Videoüberwachung von nicht öffentlich zugänglichen Betriebsstätten nur zulässig sein, soweit sie zur Wahrung wichtiger betrieblicher Interessen erforderlich und verhältnismäßig ist. Eine heimliche Videoüberwachung eines Beschäftigten soll nur unter erschwerten Voraussetzungen (bei konkreten Verdachtsfällen) zugelassen werden. Die Videoüberwachung von Betriebsräumen, die überwiegend zur privaten Lebensgestaltung des Beschäftigten dienen, soll untersagt werden.

Beispiel:
Die offene Videoüberwachung der Eingänge eines Betriebsgeländes (Zutrittskontrolle) oder eines Verteilzentrums für Wertbriefe (Schutz des Eigentums) sollen zulässig sein. Heimlich soll ein Beschäftigter mit einer Videokamera demgegenüber nur überwacht werden dürfen, wenn ein konkret belegter Verdacht besteht, dass er z.B. im Betrieb Geld gestohlen hat und die Videoüberwachung erforderlich und verhältnismäßig ist, um die Tat aufzudecken. Sofern ein Betriebsrat existiert, hat dieser ein Mitbestimmungsrecht.

Eine vorbeugende heimliche Videoüberwachung soll nicht zulässig sein. Unzulässig soll auch z.B. die Überwachung des Bereitschaftsdienstzimmers eines Arztes oder einer Krankenschwester im Krankenhaus sein, da dieses überwiegend der privaten Lebensgestaltung dient (Ausruhen, Schlafen).

- **Ortungssysteme**

Die Erhebung von Beschäftigtendaten durch Ortungssysteme (z.B. GPS) soll nur während der Arbeits- und Bereitschaftszeiten zur Sicherheit des Beschäftigten oder zur Koordinierung des Einsatzes des Be-

schäftigten zugelassen werden. Die Ortung soll zudem nur zulässig sein, wenn schutzwürdige Interessen des Beschäftigten am Ausschluss der Datenerhebung nicht überwiegen. Wird ein Ortungssystem zur Diebstahlsicherung von Sachen (z.B. Kfz) eingesetzt, soll eine personenbezogene Ortung verhindert werden.

Beispiel:
Eine in der Betriebspraxis wichtige Frage ist, wie sich Ortungssysteme, mit denen der genaue Aufenthaltsort der Mitarbeiter ermittelt werden kann, datenschutzrechtlich bewerten lassen. Hier soll ein interessengerechter Ausgleich gefunden werden. So sollen etwa Speditionen den Einsatz ihres Fuhrparks mithilfe von Ortungssystemen koordinieren dürfen. Auch im Überlebensanzug des Mitarbeiters einer Bohrinsel soll ein Ortungssystem installiert werden dürfen, um ihn im Falle des Über-Bord-Gehens schnell finden und retten zu können. Die Ortung dient in einem solchen Fall der Sicherheit des Beschäftigten. Die Ortung eines Außendienstmitarbeiters (z.B. über das Handy), der seine Arbeit selbst organisiert und koordiniert, sollte hingegen unzulässig sein, da in diesem Fall der Arbeitgeber für das Funktionieren seines Betriebes nicht jederzeit den Aufenthaltsort seines Mitarbeiters zu kennen braucht

- **Biometrische Verfahren**

Biometrische Merkmale eines Beschäftigten soll der Arbeitgeber elektronisch nur erheben und verwenden dürfen, soweit dies aus betrieblichen Gründen zu Autorisierungs- und Authentifikationszwecken erforderlich ist und keine schutzwürdigen Belange des Beschäftigten entgegenstehen. Eine Verwendung zu anderen Zwecken soll ausgeschlossen werden.

Beispiel:
Biometrische Merkmale, wie der Fingerabdruck oder die Iris, sollen z.B. in Zugangskontrollsystemen genutzt werden dürfen, um nur berechtigten Beschäftigten Einlass zu gewähren.

- **Nutzung von Telefon, E-Mail und Internet**
  Der Arbeitgeber soll – insbesondere zur Gewährleistung des ordnungsgemäßen technischen Betriebs, zu Abrechnungszwecken sowie zu Zwecken der Korruptionsbekämpfung/Compliance – die Nutzung von Telekommunikationsdiensten und Telemedien am Arbeitsplatz im erforderlichen Maß kontrollieren dürfen. Dabei sind die berechtigten schutzwürdigen Interessen des Beschäftigten zu beachten. Die Inhalte von Telefonaten sollen einem besonderen Schutz unterliegen.

  Beispiel:
  Ist die Nutzung des Internets nur zu beruflichen Zwecken erlaubt, soll der Arbeitgeber das Nutzungsverhalten des Beschäftigten ohne Anlass nur stichprobenhaft kontrollieren dürfen, um etwa festzustellen, ob verbotene Inhalte aufgerufen werden.

  Ist die Nutzung des Internets demgegenüber auch für private Zwecke erlaubt, sollen wie bisher die Vorschriften des Telemediengesetzes gelten.

- **Kollektivrechtliche Vereinbarungen**
  In Betriebs-/Dienstvereinbarungen oder Tarifverträgen sollen wie bisher eigenständige Grundlagen und Einschränkungen für eine zulässige Datenerhebung und -verwendung im Beschäftigungsverhältnis vorgesehen werden können. Die vorgesehenen Regelungen sind daher im Rahmen der grundgesetzlichen Wertungen, zwingenden Gesetzesrechts und den sich aus allgemeinen Grundsätzen des Arbeitsrechts ergebenden Beschränkungen dispositiv.

- **Beteiligungsrechte, insbesondere Mitbestimmungsrechte der Interessenvertretungen**
  Die Beteiligungsrechte der Interessenvertretungen der Beschäftigten sollen durch die Neuregelungen nicht beeinträchtigt werden. Das bedeutet, dass das bestehende Mitbestimmungsrecht des Betriebsrates bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten und die Leistung eines Beschäftigten

zu überwachen (§ 87 Absatz 1 Nr. 6 Betriebsverfassungsgesetz), unangetastet bleiben soll.

- **Einwilligung**
  Die Zulässigkeit der individuellen Einwilligung des Beschäftigten in die Erhebung, Verarbeitung oder Nutzung seiner personenbezogenen Daten soll auf ausdrücklich geregelte Fälle beschränkt werden, um der besonderen Situation des Beschäftigten im Arbeitsverhältnis Rechnung zu tragen.

- **Ausscheiden aus dem Beschäftigungsverhältnis**
  Der Arbeitgeber darf Beschäftigtendaten auch erheben, verarbeiten und nutzen soweit deren Kenntnis erforderlich ist, um nach der Beendigung des Beschäftigungsverhältnisses bestehende Pflichten – etwa buchhalterische oder steuerliche Nachweiszwecke – zu erfüllen. Werden die Daten nicht mehr für den Zweck benötigt, für den sie gespeichert wurden, sind sie zu löschen.

Weiteres Verfahren

Das Bundesministerium des Innern befindet sich in der Endphase der Erstellung eines Gesetzentwurfes zur Regelung des Beschäftigtendatenschutzes. Ein Gesetzentwurf soll nach Abstimmung mit den Bundesministerien bis zur Sommerpause dem Kabinett zur Beschlussfassung vorgelegt werden.

(Stand 2010)

Notizen

Notizen

Stiftung Christlich-Soziale Politik e. V.
Arbeitnehmer-Zentrum Königswinter (AZK)
Johannes-Albers-Allee 3
53639 Königswinter
Tel.: 02223 / 73 119
www.azk.de