

Vereinbarungen zum Schutz von Beschäftigtendaten

Kontrolleinrichtungen, IKT-Systeme, Konzerndatenflüsse

Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen,
Matthias Wilke, Datenschutz- und Technologieberatung (dtb), Kassel

Die Interessenvertretung steht oft vor der Frage, welche Inhalte eine IKT-Vereinbarung zum Arbeitnehmerdatenschutz aufweisen sollte, um die Rechte der Beschäftigten und ihrer Vertretungen zu stärken.¹ Grundsätzlich bedarf das Verwenden von Personendaten im Arbeitsverhältnis der Erlaubnis, entweder durch ein Gesetz, eine (fragwürdige) Einwilligung des Betroffenen oder eine andere Rechtsvorschrift – wie eben eine Betriebs- oder Dienstvereinbarung. Welche Vorgaben dabei zu beachten und welche Klippen zu umschiffen sind, erläutert dieser Beitrag.

Das höchste deutsche Arbeitsgericht hat früh die Betriebsvereinbarung als andere Rechtsvorschrift im Sinne des § 4 Abs. 1 Bundesdatenschutzgesetz (BDSG) anerkannt, die den betrieblichen Umgang mit Beschäftigtendaten erlauben kann.² Seit 1986 wird nunmehr auch darum gestritten, ob Betriebsparteien zu Ungunsten der Beschäftigten von den gesetzlichen Mindeststandards abweichen können.

Vorgegebener Rechtsrahmen

Anlass dafür gab ein Beschluss des Bundesarbeitsgerichts (BAG), der als überholt zu qualifizieren ist.³ Schon dieser Richterspruch zeigte den Betriebsparteien Grenzen hinsichtlich ihrer Befugnisse beim Gestalten von Betriebsvereinbarungen auf. Diese liegen in den Gesetzen, in den Persönlichkeitsrechten der Beschäftigten und im EU-Recht (zurzeit Datenschutzrichtlinie 95/46/EG). Inzwischen ist unbestritten: Die Betriebsparteien haben in derartigen Betriebsvereinbarungen den Persönlichkeitsschutz der im Betrieb beschäftigten Personen gemäß § 75 Abs. 2 BetrVG zu wahren und zu fördern.

Tipp: Grenzen der Regelungsbefugnis beachten

Betriebsvereinbarungen können den Beschäftigtendatenschutz in erster

Linie konkretisieren und auslegen, dürfen aber nicht zu Ungunsten der Beschäftigten von den Vorgaben des BDSG, der Grundrechte, des Unionsrechts zum Datenschutz und sonstiger bereichsspezifischer Datenschutzvorschriften abweichen.⁴

Das Recht auf informationelle Selbstbestimmung der Beschäftigten muss in jeder Betriebsvereinbarung gewahrt bleiben, die die Datenverwendung im Betrieb als vorrangige Rechtsvorschrift legitimieren soll. Auch unwesentliche Unterschreitungen des Datenschutzniveaus sind nicht zulässig.⁵ Ist eine gesetzliche oder tarifliche Regelung abschließend und lässt keine Auswahlmöglichkeit zu, so entfällt das Mitbestimmungsrecht.⁶

Tipp: Günstigere Regelungen für Beschäftigte durchsetzen
Unzweifelhaft können Betriebs- und Dienstvereinbarungen den Beschäftigtendatenschutz zu Gunsten der Beschäftigten verbessern und die gesetzlichen Zulässigkeitsvoraussetzungen für Datenerhebungen auch einschränken.⁷ Betriebsräte sind befugt, den Eingriff in das informationelle Selbstbestimmungsrecht der Beschäftigten mitzubestimmen und zu minimieren. Der Betriebsrat muss keine Kontroll-einrichtung akzeptieren, wenn sie nur dem BDSG-Standard entspricht und

damit datenschutzrechtlich zulässig ist. Hier gibt es keine Grenze der Mitbestimmung.

Zulässige Inhalte

Betriebsräte können den Beschäftigten-datenschutz auch über § 87 Abs.1 Nr. 6 BetrVG mitbestimmen und bei der Einführung und Anwendung technischer Kontrolleinrichtungen Betriebsvereinbarungen erzwingen.⁸ Dieses Mitbestim-

¹ Der Beitrag ist eine Antwort auf Beckschulze/Fackeldey, Systematischer Aufbau von Betriebsvereinbarungen zum Schutz von Beschäftigtendaten, in: RDV 2013, 109 ff.

² Siehe BAG vom 9.7.2013, Az.: 1 ABR 2/13, Rn. 32c, in: ZD 2014, 256 ff. (258)

³ Siehe BAG vom 27.5.1986, Az.: 1 ABR 48/84, in: DB 1986, 1287 ff.; Plocher, Betriebliche Einigung – Update zum Abschluss von Betriebsvereinbarungen, in: DB 2013, 1485 ff.

⁴ Unter vielen Fitting, BetrVG, § 80 Abs. 3, Rn. 30

⁵ Gegen: Freckmann/Störing/Müller, Bisherige und zukünftige Bedeutung der Betriebsvereinbarung im Datenschutz verkannt, in: BB 2011, 2249 ff.; Wolff/Brink/Bäcker, § 4 Rn. 13 ff.

⁶ BAG vom 11.12.2012, Az.: 1 ABR 78/11

⁷ Taeger/Gabel, BDSG, § 4 Rn. 44; Fitting, aaO., § 83 Rn. 30; für die Praxis a.A. Thüsing, Ergonomie und Datenschutz, 41 ff. (45)

⁸ Für Personalräte siehe § 75 Abs. 3 Nr. 17 und § 75 Abs. 3 Nr. 15 BPersVG »Ordnung in der Dienststelle«; Thüsing, aaO., 44, zu Unterschieden bei der Zulässigkeit von Dienstvereinbarungen

mungsrecht soll Eingriffen in das Persönlichkeitsrecht der Beschäftigten durch technische Systeme entgegenwirken und den Grundsatz der freien Entfaltung der Persönlichkeit gemäß § 75 Abs. 2 BetrVG und § 1 Abs. 1 BDSG konkretisieren.

Bei der Regelung von IKT-Systemen, Verfahren und Datenverarbeitungsprozessen und der damit verbundenen Verwendung von Beschäftigtendaten setzen Betriebsräte unterschiedliche Schwerpunkte. Folgende Arten von Betriebsvereinbarungen sind anzutreffen. Sie können als IKT-Rahmenbetriebsvereinbarungen oder als Einzelvereinbarungen zum Beispiel zu biometrischen Systemen, zur digitalen Personalakte oder Videoüberwachung abgeschlossen werden.

Hinzu kommen Betriebsvereinbarungen, die etwa Datenflüsse im Konzern oder Datenübermittlungen in Drittstaaten rechtfertigen. Zudem werden Vereinbarungen abgeschlossen, die den Beschäftigtendatenschutz insgesamt in einem Unternehmen oder in einem Konzern regeln.⁹ Dann werden solche Vereinbarungen getroffen, die nicht-automatisierte Kontrollen wie beispielsweise Torkontrollen¹⁰ und deren Auswirkung auf den Daten- und Persönlichkeitsschutz der Arbeitnehmer betreffen.

Konkrete Bestimmungen

Interessenvertretungen sollten sich vor der Aufnahme von Verhandlungen über notwendige Regelungen in Vereinbarungen verständigen. Die Inhalte von einschlägigen Betriebsvereinbarungen unterscheiden sich oft.

In erster Linie sollten sie das Erheben, Verarbeiten und Nutzen von Beschäftigtendaten regeln, das heißt der konkrete Daten- und Persönlichkeitsschutz im Beschäftigungsverhältnis ist bei technischen Kontrolleinrichtungen und sonstigen Kontrollen normgerecht zu gewährleisten.

Tipps: Datenschutz immer konkret regeln

In Vereinbarungen sollte nicht abstrakt festgestellt werden, dass der Datenschutz beachtet wird oder alle gesetzlichen Vorschriften zum Datenschutz umgesetzt werden. Betriebs-

vereinbarungen zum Beschäftigtendatenschutz müssen konkret regeln, wie das Recht auf informationelle Selbstbestimmung der Beschäftigten gewährleistet werden soll.

So ist der Ist-Zustand bei der Einführung und Anwendung eines IKT-Systems festzuschreiben, vor allem durch Festlegen von Positivlisten und Beschreibungen in Anlagen, die Bestandteil der Vereinbarung werden. Ohne solche Anlagen, die bei jeder Änderung des Systems einver-

betriebsvereinbarung nicht gegen den Willen des Betriebsrats durchsetzen. Betriebsräte sollten die mögliche Rechtsfolge bedenken, dass durch die abgeschlossene IKT-Rahmenbetriebsvereinbarung ihre Mitbestimmung bei einzelnen technischen Kontrolleinrichtungen verbraucht sein kann.¹²

Tipps: Rahmenvereinbarungen müssen Interessenvertretungen nützen
Rahmenbetriebsvereinbarungen sollten eine rechtssichere Öffnungs-



© Denis Junker, Fotolia

Die Betriebsparteien haben den Persönlichkeitsschutz der Mitarbeiter durch entsprechende Vereinbarungen zu wahren und zu fördern.

nemlich fortzuschreiben sind, ist die nachträgliche Kontrolle des Betriebsrats, ob die Bestimmungen der Betriebsvereinbarung eingehalten werden, nicht möglich.

Die betriebliche Vereinbarung als vorrangige Rechtsvorschrift zum Datenschutz muss zudem die personenbezogene Datenverarbeitung und -nutzung ausreichend beschreiben und grundlegende Sachverhalte des Datenschutzes tatsächlich regeln.¹¹

Offene Rahmenvereinbarungen

Rahmenbetriebsvereinbarungen zum Einsatz von IKT-Systemen regeln Grundsätze der Datenverarbeitung, des Beschäftigtendatenschutzes und der Mitwirkung der Interessenvertretung beim Einführen und Anwenden technischer Kontrolleinrichtungen. Diese Vereinbarungen sind unabhängig von einem konkreten System nicht vom Betriebsrat zu erzwingen. Auch der Arbeitgeber kann eine IKT-Rahmen-

klausel für Einzelvereinbarungen enthalten. Diese ist so zu formulieren, dass Arbeitnehmervertreter darüber entscheiden können, ob eine zusätzliche Einzelvereinbarung zu einem besonderen System erforderlich wird. IKT-Rahmenvereinbarungen dürfen zudem gesetzliche Rechte der Interessenvertretungen keinesfalls einschränken und sollten stattdessen die Rechte der Beschäftigten und ihrer Vertretungen deutlich ausweiten, das heißt den Persönlichkeitsschutz nach-

9 Fritz, Beschäftigtendatenschutz im Konzern Deutsche Bahn aus arbeitsrechtlicher Sicht, in: ZfA 2012, 197 ff.
 10 BAG vom 9.7.2013, Az.: 1 ABR 2/13 (a), in: ZD 2014, 256 ff. mit Anm. Wybitul
 11 Hamburgischer Beauftragter für Datenschutz und Informationsfreiheit, 22. Tätigkeitsbericht 2008/2009, 125, www.datenschutz-hamburg.de/
 12 Däubler, Internet und Arbeitsrecht, Rn. 304

Betriebsvereinbarungen zum Beschäftigtendatenschutz

Übersicht zu den wichtigsten Inhalten:

- Zwecke der Kontrolleinrichtung, Zweckbindung
- Geltungsbereich
- Systembeschreibung: Hard- und Software, Daten- und Auswertungskatalog, Schnittstellen, Berechtigungen
- Begriffsbestimmungen
- Art und Umfang der Daten
- Ausschluss von Leistungs- und Verhaltenskontrollen
- Gegebenenfalls Auftragsdatenverarbeitung
- Rechte der betroffenen Beschäftigten, Schutzbestimmungen
- Rechte des Betriebsrats (Informations- und Mitbestimmungsrechte und -verfahren, Überwachungsrechte einschließlich System-Audit mit Sachverständigen)
- Empfänger der Daten
- Technische und organisatorische Maßnahmen, etwa Berechtigungskonzept
- Konkrete Löschrufen
- Verfahren bei Streitigkeiten
- Schlussbestimmungen, Kündigung und Nachwirkung

vollziehbar fördern und die Beteiligung der Betriebsräte im Sinne von freiwilliger Mitbestimmung nach § 88 BetrVG ausbauen und die praktische Arbeit der Arbeitnehmervertreter erleichtern und verbessern.

mäßigkeit bei heimlichen Kontrollen gewahrt bleiben.¹⁴

Entscheidungen von 2013 sollten für alle Betriebsvereinbarungen zum Beschäftigtendatenschutz genutzt werden.

Die Abwägung der Interessen des Arbeitgebers mit den Interessen der Beschäftigten bezieht sich auf alle Details im Umgang mit Beschäftigtendaten, so unter anderem auf die Zweckbestimmung der Daten, den Daten- und Auswertungskatalog, die Vergabe von Zugriffsberechtigungen, die Festlegung von Schnittstellen und die Verwendung von personenbezogenen Daten besonderer Art gemäß § 28 Abs. 6 Nr. 3 BDSG.

Die Verhältnismäßigkeitsprüfung ist zusätzlich auf nicht-automatisierte Kontrollen, Befragungen und sonstige interne betriebliche Ermittlungsverfahren auszuweiten, weil § 32 Abs. 2 BDSG den ersten Absatz der Vorschrift ebenfalls auf nicht-automatisierte Datenerhebung, -verarbeitung und -nutzung ausdehnt.

Gesicherte Informationsrechte

Entwürfe von Arbeitgebern für Vereinbarungen zum Beschäftigtendatenschutz beschränken oft Rechte. So sollen Belegschaftsvertretungen zwar über Änderungen des IKT-Systems informiert werden, ihre Mitbestimmung soll aber künftig nur für wesentliche Änderungen des Systems gelten.

Tipp: Informationsrechte deutlich konkretisieren und ausbauen

Betriebsräte sind über alle Änderungen des IKT-Systems umfassend zu informieren. Nur sie entscheiden, was wesentliche Änderungen sind und ob sie ihre Mitbestimmungsrechte wahrnehmen wollen oder müssen.

Heimliche Kontrollen

Wiederholt regeln Rahmenvereinbarungen, dass bei Verdacht auf Pflichtverletzungen, Ordnungswidrigkeiten und Straftaten Mitarbeiter heimlich kontrolliert werden dürfen und der betriebliche Datenschutzbeauftragte und der Betriebsrat lediglich nach den durchgeführten Kontrollen informiert werden. Damit wird auf § 32 Abs. 1 Satz 2 BDSG reagiert, der die Voraussetzungen für eine Kontrolle von Beschäftigten detailliert regelt, wenn ein zu dokumentierender Anfangsverdacht auf Begehung einer Straftat im Beschäftigungsverhältnis besteht.

Tipp: Regelungen zu heimlichen Kontrollen beachten

Betriebsräte sollten unbedingt bei Entwürfen der Arbeitgeber zu Betriebsvereinbarungen darauf achten, dass die strikten Voraussetzungen¹³ von § 32 Abs. 1 Satz 2 BDSG, bei dem es ausschließlich um den Verdacht auf Begehung einer Straftat im Beschäftigungsverhältnis geht, nicht unterlaufen werden und ihre Mitbestimmung und Mitbeurteilung der Verhältnis-

Verhältnismäßige Nutzung

Interessenvertretungen sollten sich in Vereinbarungen für den Umgang mit Beschäftigtendaten stärker als bisher an § 32 Abs. 1 Satz 1 BDSG orientieren. Danach ist das Verwenden von Beschäftigtendaten nur zulässig, wenn diese für die Begründung, Durchführung und Beendigung des Beschäftigungsverhältnisses erforderlich sind. Betriebsräte haben bei jeder Betriebsvereinbarung zu einer technischen Kontrolleinrichtung oder auch zu Kontrollen ohne Technikeinsatz zu prüfen, ob die gewünschte Datenverwendung verhältnismäßig ist, also ob eine Erlaubnisvorschrift gegeben ist und die vom Arbeitgeber gewünschten Kontrollen des Beschäftigten samt Datenverwendung erforderlich, geeignet und angemessen sind. Aktuell hat das BAG in mehreren Entscheidungen¹⁵ die Schritte der Verhältnismäßigkeitsprüfung im Rahmen des Beschäftigtendatenschutzes dargestellt.¹⁶

Tipp: Verhältnismäßigkeit von Datenschutzregelungen wahren
Die Rechtsprechung des höchsten deutschen Arbeitsgerichts zur Verhältnismäßigkeitsprüfung bei der Videoüberwachung von 2004 und 2008 sowie die aktuellen BAG-

¹³ Däubler/Klebe/Wedde/Weichert, BDSG, § 32 Rn. 125 ff.

¹⁴ Kiesche/Wilke, Anti-Fraud-Management, in: CuA 1/2014, 4 ff.

¹⁵ Siehe unter anderem BAG vom 20.6.2013, Az.: 2 AZR 546/12, in: ZD 2014, 260, Rn. 26 ff.

¹⁶ BAG vom 20.6.2013, Az.: 2 AZR 546/12, in: DB 2014, 246; BAG vom 9.7.2013, Az.: 1 ABR – 2/13 (a); Wybitul/Pötters, BAG definiert Beschäftigtendatenschutz neu, in: BB 2014, 437; Brink/Wybitul, Der »neue Datenschutz« des BAG, in: ZD 2014, 225

In nicht seltenen Fällen sollen sie nur noch über »wesentliche« Änderungen des Systems informiert werden. Das sind unzulässige Einschränkungen der Informationsrechte, denn Betriebsräte sind zur Wahrnehmung ihres Überwachungsrechts und Ausübung ihrer Mitbestimmung nach §§ 87 Abs. 1 Nr. 1 und 6, 94 BetrVG stets umfassend und rechtzeitig zu informieren.

Unabhängige Sachverständige

Betriebsräte sollten sich, so Beckschulze/Fackeldey¹⁷, in einer IKT-Rahmenbetriebsvereinbarung verpflichten, erst einmal alle internen Informationsquellen auszuschöpfen, bevor sie einen Sachverständigen ihres Vertrauens hinzuziehen dürfen. Eine kritikwürdige Entscheidung des BAG¹⁸ sei als generalisierte Verhaltensnorm in die IKT-Rahmenbetriebsvereinbarung aufzunehmen.

Tipp: Externe Sachverständige beauftragen

Betriebsräte sollten sich ihre Rechte gemäß § 80 Abs. 2 und Abs. 3 BetrVG in Betriebsvereinbarungen nicht einschränken lassen. Interne Auskunftspersonen – wie SAP-Projektleiter – sind oft zeitlich nicht in der Lage, dem Gremium die notwendigen Auskünfte zu erteilen. Arbeitnehmervertretungen sollten einen Sachverständigen ihrer Wahl hinzuziehen. Auch Arbeitgeber profitieren von der Expertise dieser Fachleute, etwa beim Überprüfen einer SAP-Betriebsvereinbarung.¹⁹ Betriebsräte sollten die gesetzlichen Regelungen in einer Rahmenbetriebsvereinbarung allenfalls konkretisieren, damit Streitigkeiten vermieden werden. Sie sollten zudem darauf verzichten, den betrieblichen Datenschutzbeauftragten als »geborenen Sachverständigen« in einer Vereinbarung festzuschreiben oder ihm Kontrollrechte über die Datenverarbeitung im Büro der Interessenvertretung einzuräumen.²⁰

Gesichertes Überwachungsrecht

Beckschulze und Fackeldey²¹ vertreten zudem eine Einschränkung des Überwachungsrechts gemäß § 80 Abs. 1 Nr.1

BetrVG. Betriebsräte haben unbestritten das Recht, die Einhaltung des BDSG zu überwachen.

Es ist zwar richtig, dass das BAG²² das Recht auf einen Online-Zugriff des Betriebsrats bei technischen Kontrollsystemen – abgeleitet aus § 80 Abs. 2 BetrVG – ablehnt. Faktisch finden aber Kontrollmaßnahmen durch den Betriebsrat durchaus auf unterschiedliche Art und Weise statt.

Praktiziert werden sowohl Online-Zugriffe als auch Kontrollmaßnahmen zusammen mit dem Arbeitgeber und einem Betriebsrats-Sachverständigen sowie systematische Überprüfungen und Befragungen an Arbeitsplatzrechnern. Beckschulze und Fackeldey bringen einen Fragenkatalog als »freiwillige Leistung« des Arbeitgebers ins Spiel. Mit diesem Fragenkatalog – ausgearbeitet vom Datenschutzbeauftragten – könne der Betriebsrat sein Überwachungsrecht ausüben.

Hiervor ist zu warnen: Ein Beschneiden des Überwachungsrechts der Arbeitnehmervertretung führt dazu, dass die betriebliche Vereinbarung zu dem IKT-System und zum Erheben, Verarbeiten und Nutzen von Beschäftigtendaten nicht mehr als vorrangige Rechtsvorschrift im Sinne des § 4 Abs. 1 BDSG herangezogen werden kann.

Tipp: Überwachungsrecht nicht einschränken

Betriebsräte sollten sich keinesfalls auf einen solchen Fragenkatalog einlassen. Damit könnten sie ihre Rechte nicht mehr ausüben.²³ Eins ist sicher: Die Betriebsräte müssen ihr Überwachungsrecht ungestört wahrnehmen und regelmäßige Kontrollen durchführen können, damit die Betriebsvereinbarung überhaupt als andere Rechtsvorschrift gemäß § 4 Abs. 1 BDSG gelten kann.²⁴

Mutige Mitbestimmung

Betriebsräte sollten sich nicht beirren lassen, wenn sie den Beschäftigtendatenschutz im eigenen Unternehmen voranbringen wollen. Sie sind gefordert, ihre Mitbestimmungsrechte zu nutzen und Leistungs- und Verhaltenskontrollen zu verhindern. Das hat sich in der jeweiligen

Betriebsvereinbarung konkret niederzuschlagen.

Tipp: Worauf Interessenvertretungen zu achten haben

In eine IKT-Rahmenbetriebsvereinbarung gehört ein klares Verbot von Leistungs- und Verhaltenskontrollen. Betriebsräte sollten zudem keinesfalls auf ein eindeutig formuliertes Beweisverwertungsverbot verzichten. Status- oder Stammdaten²⁵ sind nicht von der Mitbestimmung ausgeschlossen. Das vorherige Eingreifen des Betriebsrats bei repressiven Compliance-Maßnahmen wird nicht aufgegeben. Die Belegschaftsvertretung hat einen Anspruch auf namensbezogene Zugriffsberechtigungen. Wenn die Privatnutzung von E-Mail und Internet zulässig ist, muss das Fernmeldegeheimnis nach § 88 des Telekommunikationsgesetzes (TKG) gewahrt bleiben. Für etwaige Kontrollen von E-Mail- und Internet bei privater Nutzung bedarf es einer Betriebsvereinbarung in Verbindung mit einer Einwilligung. Konkrete Löschrufen sind erforderlich. Es ist datenschutzrechtlich unzulässig, Zweckbestimmungen für Datenerhebungen in der Personalabteilung auf Vorrat in einer IKT-Rahmenbetriebsvereinbarung festzuschreiben.

Fazit

Betriebliche Interessenvertretungen sollten sich bei der Durchsetzung von Vereinbarungen zum Beschäftigtendatenschutz vor allem auf konkrete Einzelvereinba-

¹⁷ Siehe Beckschulze/Fackeldey, aaO., 115

¹⁸ BAG vom 4.6.1987, Az: 6 ABR 63/85, in: NZA 1988, 50

¹⁹ Kiesche/Wilke, Eine Lücke im System, in: AiB 3/2014, 23 ff.

²⁰ Anderer Ansicht Beckschulze/Fackeldey, aaO., 115

²¹ Beckschulze/Fackeldey, aaO., 114f.

²² BAG vom 16.8.2011, Az.: 1 ABR 22/10

²³ Wilke (Hrsg.), SAP kompakt für den Betriebsrat

²⁴ Gola/Wronka, Handbuch Arbeitnehmerdatenschutz, Rn. 1689

²⁵ Morgenthaler, Die Einigungsstelle, Rn. 764; Gola/Wronka, aaO., Rn. 1870



IKT-Rechtsprechung

Recht auf Vergessen werden im Internet

Die Suchmaschine Google muss Links auf personenbezogene Daten aus seiner Trefferliste streichen, wenn sie dazu aufgefordert wird. Das hat der Europäische Gerichtshof (EuGH) entschieden. Die Europarichter stärken mit dieser nicht unumstrittenen Entscheidung das Recht auf Vergessen im Internet.

Ein Spanier sah seine Privatsphäre verletzt und hatte sich bei der Datenschutzbehörde seines Landes beschwert. Er gab bei Google seinen Namen ein und fand Hinweise auf der Internetseite



© Google

Die schicke Zentrale von Google Europa mit Sitz im steuerfreundlichen Irland

einer Tageszeitung über eine Zwangsversteigerung seines Grundstücks, die bereits 15 Jahre zurücklag. Er war der Ansicht, dass die Pfändung seit vielen Jahren vollständig erledigt sei und keine Erwähnung mehr verdiene.

Die Beschwerde gegen die Zeitung wurde von der Behörde zurückgewiesen, weil die Informationen rechtmäßig veröffentlicht worden seien. Soweit sie sich gegen die Suchmaschine richtete, wurde ihr hingegen stattgegeben. Die dagegen gerichtete Klage von Google blieb erfolglos.

Der Betreiber einer Internetsuchmaschine sei bei sensiblen Daten, die auf von Dritten veröffentlichten Websites erscheinen, für die von ihm vorgenom-

mene Verarbeitung verantwortlich. Eine Person könne sich daher, wenn bei einer anhand ihres Namens durchgeführten Suche in der Ergebnisliste ein Link zu einer Internetseite mit Informationen über sie angezeigt wird, unmittelbar an den Suchmaschinenbetreiber wenden, um – unter bestimmten Voraussetzungen – das Entfernen des Links aus der Trefferübersicht zu erwirken.

Sollte dieser dem Antrag nicht entsprechen, könne der Betroffene im Anschluss auch an die zuständigen Stellen herantreten.

Das Gericht beruft sich auf die Europäische Datenschutz-Richtlinie 95/46/EG. Es weist in diesem Zusammenhang darauf hin, dass eine Verarbeitung personenbezogener Daten, die von einem solchen Suchmaschinenbetreiber vorgenommen wird, es jedem Internetnutzer ermöglicht, beim Durchführen einer Suche anhand des Namens einer natürlichen Person mit der Ergebnisliste einen strukturierten Überblick über die zu ihr im Internet verfügbaren Informationen zu erhalten. Somit sei es jedem User möglich, ein mehr oder weniger detailliertes Profil der gesuchten Personen zu erstellen. Wegen der potenziellen Schwere dieses Eingriffs sei dieser nicht allein mit dem wirtschaftlichen Interesse von Google zu rechtfertigen.

**Europäischer Gerichtshof
Urteil vom 13.5.2014**

Aktenzeichen: C – 131/12

(Volltext des Urteils unter: <http://curia.europa.eu/juris/documents.jsf?num=C-131/12>)

Google hat mittlerweile ein nicht leicht zu findendes Formular auf seine Website gestellt, mit dem Betroffene Löschanträge einreichen können:

» https://support.google.com/legal/contact/lr_eudpa?product=websearch&hl=de

Zusammenstellung

Olaf J. Lutz, CuA-Redaktion

» redaktion@cua-web.de

nungen zu technischen Kontrolleinrichtungen, IKT-Systemen und –Verfahren, zu nicht-automatisierten Kontrollen oder konzerninternen Datenflüssen mit Beschäftigtendaten konzentrieren.

IKT-Rahmenbetriebsvereinbarungen, die stets einen Kompromiss darstellen, schränken von Zeit zu Zeit gesetzliche Rechte der Betriebsräte ein und führen oftmals nicht zu einer Konkretisierung des betrieblichen Datenschutzes und der Wahrung der entsprechenden Rechte der Interessenvertretung. Zusätzlich verfehlen sie in der Regel den Anspruch, als andere oder vorrangige Rechtsvorschrift zum Datenschutz im Sinne des § 4 Abs. 1 BDSG zu gelten.

Nur eine Rahmenbetriebsvereinbarung zum Beschäftigtendatenschutz, die auch über gesetzliche Mindeststandards hinausgeht, die Beteiligung des Betriebsrats deutlich ausweitet und den Arbeitnehmerdatenschutz nachvollziehbar konkretisiert, ist aus Sicht der Beschäftigten und ihrer Vertretungen lohnenswert.²⁶ Ansonsten sollte der Beschäftigtendatenschutz bei allen Regelungsgegenständen in Einzelvereinbarungen so präzise wie möglich mit den notwendigen Datenschutzregelungen, Geboten, Verboten und Begriffsbestimmungen durch den jeweils zuständigen Betriebsrat²⁷ geregelt werden. Hierfür sind von den Autoren noch zusätzliche Tipps entwickelt worden.

Autor

Dr. Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen

» eberhard.kiesche@t-online.de

» www.aob-bremen.de

Matthias Wilke, Datenschutz- und Technologieberatung (dtb), Kassel

» info@dtb-kassel.de

» www.dtb-kassel.de

cua-web.de

SERVICE

Arbeitshilfen » Tipps aus der Praxis



²⁶ Siehe das Beispiel des DB-Konzerns, www.evg-online.org/Arbeitswelt/Mitbestimmung/Betriebsverfassung/Aktuelles/13_04_10_KBV_BDSG/?-C=&portal_skin=Printable

²⁷ Zur Zuständigkeit des Konzernbetriebsrats bei SAP-Einführung siehe BAG vom 25.9.2012, Az. 1 ABR 45/11