Datenschutz

Mitarbeiterkontrollen – Rechte und rechtliche Grenzen

Es gehört zum beruflichen Alltag, dass Kontrollhandlungen des Arbeitgebers und (datenschutz)rechtliche Interessen des Arbeitnehmers kollidieren. Wo die praxisrelevanten Problemfelder genau liegen, welche gesetzlichen Grundlagen und ungeschriebenen Grundsätze greifen, soll im Folgenden beschrieben werden.

Arbeitnehmerdatenschutz in der Praxis

Arbeitnehmer- und Arbeitgeberinteressen korrelieren häufig negativ miteinander – insbesondere dann, wenn eine „Überwachung" am Arbeitsplatz befürchtet wird.

Aus datenschutzrechtlicher Sicht wird mit dem Begriff „Überwachung" die zielgerichtete Beobachtung und Informationserhebung von Personen, Objekten oder Gegenständen in Verbindung gebracht. Die Möglichkeit der Überwachung durch den Arbeitgeber kann sich dabei von der Telefon-, E-Mail- und Internetnutzung oder dem Einsatz von GPS-Systemen bis hin zu Videoüberwachungsanlagen erstrecken. Probleme ergeben sich des Weiteren in alltäglichen Situationen wie etwa der Arbeitszeiterfassung, der Veröffentlichung von Mitarbeiterfotos (u. a. auf Betriebsversammlungen, Webseiten etc.) oder auch bei gezieltem Monitoring von Social Networks, um ein Bild von dem privaten Leben des (potenziellen) Mitarbeiters zu gewinnen.

Telefonnutzung

Das Telefonieren am Arbeitsplatz zu dienstlichen Zwecken gehört in der Regel zum Alltag eines jeden Arbeitnehmers. Telefoniert der Arbeitnehmer privat, so stellt sich die Frage, unter welchen rechtlichen Voraussetzungen dies erlaubt ist und ob der Arbeitgeber überprüfen darf, mit wem der Arbeitnehmer zu welchem Zeitpunkt Gespräche führt. Ab wann handelt es sich um eine unzulässige Verhaltens- und Leistungskontrolle des Arbeitgebers?

Der Grundsatz lautet: Der Arbeitnehmer darf am Arbeitsplatz nicht privat telefonieren, es sei denn, der Arbeitgeber erlaubt private Gespräche in einem gewissen Umfang. Die arbeitgeberseitige Speicherung und Überwachung dieser Gespräche ist dann jedoch verboten.

Derartige Fragestellungen werden in der Regel im Arbeitsvertrag oder in Betriebsvereinbarungen geregelt.

Oftmals wird die unvermeidliche private Nutzung konkludent, also stillschweigend, über einen längeren Zeitraum geduldet, sofern die Gespräche sich in einem zumutbaren Rahmen bewegen und der Arbeitnehmer die arbeitsvertraglich geschuldete Leistung erbringt. Diese Fallkonstellation fällt unter das „Fernmeldegeheimnis", das in Art. 10 Abs. 1 Grundgesetz (GG) verankert ist. Danach ist es dem Arbeitgeber gemäß § 88 Abs. 1 Telekommunikationsgesetz (TKG) nicht gestattet, die näheren Umstände, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war, sowie die Inhalte des Telefonates zu kontrollieren.

Im Gegensatz dazu sind dienstliche Gespräche nicht vom Fernmeldegeheimnis erfasst. Diese dürfen laut Rechtsprechung stichprobenartig kontrolliert werden. Voraussetzung hierfür ist, dass die Privatsphäre des Gesprächspartners nicht verletzt wird, z. B. durch die Erfassung der vollständigen Telefonnummer.

Verbietet der Arbeitgeber die Privatnutzung explizit, z. B. in einer Betriebsvereinbarung, die nur dienstliche Gespräche erlaubt, dürfen die Telefonnummern von externen Gesprächspartnern (Vorwahl und ein Teil der Rufnummer) gespeichert und – nach Auffassung staatlicher Datenschutzaufsichtsinstanzen und höchstrichterlichen Entscheidungen – die von einem Arbeitnehmer verursachten Kosten, aufgeschlüsselt nach Zeitpunkt und Dauer, festgehalten werden. Die Daten dürfen zum Zwecke der Missbrauchs- und Ko-

stenkontrolle (z. B. unerlaubte private Nutzung auf Kosten des Arbeitgebers bei einem Privatnutzungsverbot) verwendet und über eine Dauer von ca. drei Monaten gespeichert werden.

Die Nutzung der Telefondaten zu anderen Zwecken wie etwa Verhaltens- und Leistungskontrollen ist lediglich unter besonderen Voraussetzungen erlaubt, die im Folgenden erläutert werden.

Abhören bzw. Aufzeichnung von Telefonaten zur Qualitätskontrolle

Zahlreiche Branchen, die Dienstleistungen über das Telefon erbringen, haben ein erhebliches Interesse daran, die eigene Servicequalität über ein kontinuierliches Qualitätsmanagement zu verbessern. Eine Auswertung zum Zwecke der Qualitätskontrolle, der Kontrolle der Arbeitnehmer und auch im Kontext der Schulung von Neuzugängen erfolgt über das Abhören und Aufzeichnen bzw. Speichern der Gesprächsinhalte.

Derartige Maßnahmen stellen jedoch einen erheblichen Eingriff in das Grundrecht auf informationelle Selbstbestimmung dar. Grundsätzlich soll jede Person selbst darüber frei entscheiden können, ob und welche ihrer Daten erhoben und verarbeitet werden.

Wegen der unterschiedlichen Eingriffsintensität in das Selbstbestimmungsrecht erfolgt eine Unterscheidung zwischen Abhören und Aufzeichnen von Telefongesprächen. Ferner ergibt sich die Frage, ob es sich um ein heimliches oder offenes Abhören bzw. Aufzeichnen handelt. Der Grundsatz lautet: Die unbefugte Aufzeichnung bzw. das Abhören ist verboten und wird gemäß § 201 Strafgesetzbuch (StGB) sogar mit einer Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bewehrt.

Im Umkehrschluss bedeutet dies, dass eine ausdrückliche schriftliche und freiwillige Einverständniserklärung

- des Kunden (bereits vor Gesprächsaufzeichnung) und
- des Arbeitnehmers (nicht Bestandteil der arbeitsvertraglichen Regelungen und daher gesondert einzuholen)

im Sinne des § 4a Abs. 1 Satz 3 Bundesdatenschutzgesetz (BDSG) vorliegen muss. Sie allein rechtfertigt die Aufzeichnung bzw. das Abhören. Des Weiteren ist eine Aufklärung über die Identität der verantwortlichen Stelle zu veranlassen und der Zweck der Erhebung und Verarbeitung gemäß § 4 Abs. 3 Satz 1 BDSG darzulegen. Auf die Schriftform kann im Sinne dieses Gesetzes verzichtet werden, soweit wegen besonderer Umstände eine andere Form angemessen ist (z. B. bei einem einmaligen telefonischen Kontakt).

Eine Einwilligung ist zwar stets Voraussetzung für die Zulässigkeit der Maßnahme, zunächst sollten jedoch weitere bestehende Möglichkeiten ausgeschöpft werden (z. B. Testanrufe). Damit kann ein möglicher Verstoß gegen den Grundsatz der Datenvermeidung und Datensparsamkeit nach § 3a BDSG vermieden werden. Im Rahmen der Einarbeitungsphase von neuen Beschäftigten ist das Mithören von Telefongesprächen zum Zwecke der Einarbeitung und Schulung gestattet.

Werden Telefonate mittels technischer Einrichtungen aufgezeichnet bzw. abgehört, so unterliegt dies der Mitbestimmungspflicht des Betriebsrates (§ 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz (BetrVG)), da das Verhalten oder die Leistung des Arbeitnehmers überwacht wird. Erforderlich ist in diesem Fall der Abschluss einer Betriebsvereinbarung, in der das konkrete Verfahren seine Regelung findet.

E-Mail

Die private Nutzung dienstlicher E-Mail-Accounts durch den Arbeitnehmer am Arbeitsplatz stellt einen ähnlich gelagerten Sachverhalt dar. Erlaubt oder duldet der Arbeitgeber die Nutzung der in der Regel für dienstliche und dienstlich veranlasste E-Mails vergebenen Adresse auch zu privaten Zwecken, so führt dies zu (datenschutz)rechtlichen Implikationen. Beispielsweise muss er sich fragen, ob er ohne Weiteres auf das E-Mail-Postfach eines ehemaligen Arbeitnehmers zugreifen und Nachrichten archivieren darf.

Diverse Gerichte, so auch das Landesarbeitsgericht (LAG) Berlin-Brandenburg (Urteil vom 16.02.2011 – AZ 4 Sa 2132/10), vertreten die Auffassung, dass ein Arbeitgeber nicht allein dadurch zum Dienstanbieter im Sinne des TKG wird, dass er seinen Beschäftigten gestattet, einen dienstlichen E-Mail-Account auch privat zu nutzen. Da eine Verletzung des TKG maßgebliche Konsequenzen nach sich ziehen kann, geht der überwiegende Teil der Rechtswissenschaftler gerade aus diesem Grunde davon aus, dass der Arbeitgeber zum Anbieter von TK-Diensten wird, wenn er seinen Beschäftigten die Möglichkeit der privaten E-Mail-Nutzung eröffnet.

Sodann ist eine Beachtung des Fernmeldegeheimnisses notwendig, da sich zwischen Arbeitgeber und Arbeitnehmer ein Anbieter-Nutzer-Verhältnis im Sinne des TKG ent- >

wickelt. Eine unbefugte Archivierung bzw. Überprüfung des E-Mail-Verkehrs stellt eine strafbare Verletzung des Fernmeldegeheimnisses nach § 206 StGB dar. Aus diesem Grunde wird regelmäßig zunächst ein generelles Verbot ausgesprochen und die private Nutzung nur unter der Voraussetzung, dass der Arbeitnehmer bestimmten Einschränkungen (z. B. Archivierung von E-Mails) schriftlich zustimmt, gestattet.

Sofern ein Betriebsrat besteht, sollte die Regelung zur Nutzung des E-Mail-Kontos durch eine Betriebsvereinbarung ergänzt werden, die regelmäßige Kontrollen und arbeitsrechtliche Konsequenzen bei Verstößen beinhaltet, vgl. auch Landesarbeitsgericht (LAG) Niedersachsen (Urteil vom 31.05.2010 – 12 Sa 875/09, § 206 StGB).

Internetnutzung/Social Network

Liegen der Privatnutzung des Internets innerhalb der Arbeitszeit keine konkreten Regelungen zugrunde, so können sich mangels Transparenz weitreichende Konsequenzen für Arbeitgeber und Arbeitnehmer ergeben. Wird eine private Nutzung geduldet, ist fraglich, wo die zulässigen Grenzen liegen und welche Risiken arbeitgeberseitige Überwachungsmöglichkeiten bergen.

Das Bundesarbeitsgericht (BAG) vertritt die Auffassung, dass die private Nutzung des Internets grundsätzlich verboten ist, sofern diese nicht ausdrücklich erlaubt oder in einem gewissen Rahmen stillschweigend geduldet wurde („betriebliche Übung"). Eine ausdrückliche Erlaubnis kann beispielsweise, unter Beachtung technischer und rechtlicher Gegebenheiten, in individualvertraglichen Abreden oder Betriebsvereinbarungen geregelt werden.

Wird die private Internetnutzung ohne gezielte Regelungen durch den Arbeitgeber geduldet, so gelten für den Arbeitnehmer dennoch Einschränkungen, wie z. B. dass

- die Privatnutzung des Internets grundsätzlich auf arbeitsfreie Zeiten zu reduzieren ist, so dass die vertraglich geschuldete Arbeitsleistung nicht darunter leidet,
- das Betriebssystem vor Störungen zu schützen ist,
- Rufschädigungen des Arbeitgebers und
- zusätzliche oder unzumutbare Kosten zu vermeiden sind,
- die Installation von Fremdsoftware verboten ist etc.

Die stillschweigende Duldung führt in der Praxis sehr oft zu Komplikationen. Verstößt der Arbeitnehmer gegen vorliegende Einschränkungen, so kann dies ggf. zu einer fristlosen Kündigung führen. Beruft sich der Arbeitnehmer hingegen auf den sogenannten „Grundsatz der betrieblichen Übung", so kann die Wirkung einer betrieblichen Übung vom Arbeitgeber nur in Ausnahmefällen beseitigt werden.

Eröffnet der Arbeitgeber seinen Beschäftigten die Möglichkeit der privaten Internetnutzung, so wird er zum Anbieter von TK-Diensten. Damit muss das Fernmeldegeheimnis zwingend beachtet werden, da sich zwischen Arbeitgeber und Arbeitnehmer ein Anbieter-Nutzer-Verhältnis im Sinne des TKG (gemäß §§ 3 Nr. 6, 10, 88) entwickelt. Die Strafbarkeit bemisst sich nach § 206 StGB. Folglich darf der Arbeitgeber in seiner Eigenschaft als Diensteanbieter die näheren Umstände von Seitenaufrufen gemäß § 100 Abs. 1 TKG lediglich zum Erkennen, Eingrenzen oder Beseitigen von Störungen an Telekommunikationsanlagen protokollieren. Andernfalls drohen Bußgelder, vgl. auch Landesarbeitsgericht (LAG) Hamm (Urteil vom 18.01.2007 – AZ 15 Sa 558/06, § 206 StGB).

Wie sieht es mit der Frage aus, ob sich der Arbeitgeber Informationen über den Arbeitnehmer aus Social Networks verschaffen und verwerten darf? Gemäß § 4 Abs. 2 BDSG sind personenbezogene Daten grundsätzlich beim Betroffenen zu erheben (Direkterhebungsgebot), es sei denn, eine Rechtsvorschrift sieht dies anders vor (weitere Ausnahmen in § 4 Abs. 2 Nr. 1 und Nr. 2 BDSG). Derzeit liegen die Voraussetzungen für eine vom Direkterhebungsgebot abweichende Ausnahmeregelung bei Datenerhebung des Arbeitgebers in Social Networks nicht vor, so dass der Arbeitgeber nach Auffassung des Bundesarbeitsgerichts (BAG) sowie des Landesarbeitsgerichts (LAG) Hamm (Urteil vom 18.01.2007 – AZ 15 Sa 558/06) auf diesen Plattformen keine Daten erheben oder dort erhobene Daten verwenden darf.

Veröffentlichung von Arbeitnehmerdaten im Internet

Die Außendarstellung von Unternehmen über den Webauftritt ist heutzutage kaum mehr wegzudenken. Hier werden häufig auch Fotos von Arbeitnehmern sowie deren Kontaktdaten veröffentlicht. Diese unterliegen datenschutz-, per-

AUTORIN UND ANSPRECHPARTNERIN

Aysegül Kalkan
IT-Sicherheit & Datenschutz,
E-Mail: ayseguel.kalkan@geno-tec.de

sönlichkeits- und arbeitsrechtlichen Zulässigkeitsvoraussetzungen. Für Privatunternehmen richtet sich die Zulässigkeit der Nutzung personenbezogener Daten von Arbeitnehmern nach den Bestimmungen des Bundesdatenschutzgesetzes (§ 3 Abs. 1 BDSG). Die zu klärende Frage lautet: Welche Arbeitnehmerdaten dürfen unter welchen rechtlichen Voraussetzungen im Internet veröffentlicht werden und wo liegen die Grenzen?

Der Umgang mit Arbeitnehmerdaten richtet sich nach dem Erforderlichkeitsprinzip und danach, ob die konkrete Verwendung der Daten – unter Berücksichtigung der Interessenlage beider Parteien – notwendig ist. Dies gilt insbesondere für das Internet, weil die veröffentlichten Daten weltweit abrufbar sind und somit jedermann zur Verfügung stehen. Folgende rechtliche Rahmenbedingungen sollten bei der Veröffentlichung beachtet werden: Der Veröffentlichung steht gemäß § 4 Abs. 1 BDSG nichts entgegen, wenn es ein Gesetz erlaubt oder der Betroffene vorher schriftlich eingewilligt hat. Nach § 32 Abs. 1 Satz 1 BDSG dürfen Arbeitnehmerdaten zum Zwecke des Beschäftigungsverhältnisses veröffentlicht werden, wenn dies für die Durchführung des Beschäftigungsverhältnisses erforderlich ist, soweit einer Veröffentlichung gemäß § 32 Abs. 1 Satz 2 BDSG keine berechtigten Interessen des Arbeitnehmers entgegenstehen. Es erfolgt eine Unterscheidung in „Funktionsträger“ mit übergeordnetem Verantwortungsbereich und Personen, die als offizielle Ansprechpartner fungieren und das Unternehmen in Führungspositionen nach außen repräsentieren. Letztere müssen eine Veröffentlichung ihrer „Basiskommunikationsdaten“ (z. B. Vorname und Familienname, Titel und akademischer Grad, postalische Dienstanschrift, dienstliche Telefon- und Telefaxnummer ohne direkte Durchwahlnummer, dienstliche E-Mail-Adresse, Funktion) ohne ausdrückliche Einwilligung hinnehmen, sofern die Veröffentlichung in Zusammenhang mit der ausgeübten Tätigkeit steht und in Erfüllung der Arbeitspflicht erfolgt (Grundsatz der Datensparsamkeit und Zweckbindung). „Personenzusatzdaten“ von Funktionsträgern hingegen (z. B. private Erreichbarkeitsdaten, Geburtsdatum, Lebenslauf, Fotos, Staatsangehörigkeit, Angaben zur Konfession, Angaben zur Mitgliedschaft in einer Gewerkschaft, sonstige Angaben zu persönlichen Eigenschaften oder Vorlieben wie Hobbys) dürfen grundsätzlich nur mit vorheriger Einwilligung des Betroffenen veröffentlicht werden. Die Veröffentlichung der Daten von „Nichtfunktionsträgern“ (z. B. sonstige Angestellte ohne Kontakt zu externen Dritten, Boten, Pförtner) bedarf stets der schriftlichen Zustimmung des einzelnen Mitarbeiters. Gemäß §§ 22, 23, 33 Kunsturhebergesetz (KunstUrhG) dürfen Fotos, bis auf einige Ausnahmen, ohne das Vorliegen einer entsprechenden Einverständniserklärung nicht an die Öffentlichkeit gelangen.

Fazit

Der Kontrollbefugnis des Arbeitgebers sind vom Gesetzgeber und von der Rechtsprechung Grenzen gesetzt. Einen einheitlichen Gesetzesrahmen über die Zulässigkeit und Reichweite von Mitarbeiterkontrollen gibt es nach derzeitiger Rechtslage nicht. Die Kontrollmechanismen und Kontrollrechte des Arbeitgebers sind nach geltendem Recht in dreifacher Hinsicht eingeschränkt: Die Kontrollmaßnahmen dürfen nur unter Beachtung des allgemeinen Persönlichkeitsrechts des Arbeitnehmers erfolgen. Umfassende Vorschriften zum Arbeitnehmerdatenschutz, zur Behandlung personenbezogener Daten von Arbeitnehmern, sind nicht existent und lediglich in § 32 BDSG verankert. Zuletzt unterliegen die Kontrollmechanismen dem Mitbestimmungsrecht des Betriebsrats und können aus diesem Grunde nicht einseitig durch den Arbeitgeber eingeführt werden. ▬