Der gläserne Beschäftigte?

Rechtliche Hürden und Anforderungen an Kontrolle von Zeit und Zutritt

Kontrollmöglichkeiten der Mitarbeiter, etwa über Zeiterfassungssysteme oder Zutrittsbeschränkungen für Räume oder Schränke, stellen Arbeitgeber im ständigen Digitalisierungsprozess und mit zunehmender Fortentwicklung der zur Verfügung stehenden technischen Systeme vor rechtliche Herausforderungen. Denn die Systeme müssen gleichzeitig ihren Zweck erfüllen, aber auch das Recht der Beschäftigten zum Schutz vor Dauerüberwachung und -kontrolle gewährleisten.

Überwachung von Beschäftigten

Die Digitalisierung des Arbeitsalltags birgt die Gefahr totaler Kontrolle über den Beschäftigten durch (vielleicht auch nur als solche empfundene) Dauerüberwachung. Eine solche Überwachung beginnt bereits mit dem Durchlaufen bestimmter Kontrollmechanismen durch den Beschäftigten hinsichtlich seiner Arbeitszeit. Derartige Mechanismen gibt es viele, etwa als Stempeluhren oder Chipkarten. Der Arbeitgeber kann seinen Beschäftigten aber auch „heimlich" kontrollieren, indem er Systeme zur Leistungsabfrage am Arbeitsplatz einführt. Ein solches System stellen z.B. Keylogger dar, welche die Anzahl oder Inhalte der Tastaturanschläge des Arbeitnehmers erfassen und damit zu einer Verhaltens- und Leistungskontrolle beitragen können. Mittels Keyloggern kann der Arbeitgeber die Zeit kontrollieren, in der sich der Beschäftigte an seinem Arbeitsplatz befunden und dabei gearbeitet hat – oder nicht.

Rechtliche Grenzen der Überwachung

Ist das Unternehmen mitbestimmt, zwingt das Mitbestimmungsrecht (z.B. § 87 Abs. 1 BetrVG) den Arbeitgeber, vor Einführung von zur Leistungs- oder Verhaltenskontrolle geeigneten Maßnahmen die Zustimmung des Betriebsrats, Personalrats oder der Mitarbeitervertretung einzuholen. Sollte eine Maßnahme ohne diese Zustimmung eingeführt werden, führt dies zu ihrer Unwirksamkeit und kann arbeitsgerichtlich untersagt werden, selbst wenn die Maßnahme rechtlich zulässig sein sollte.

Rechtliche Grenzen werden aber nicht nur durch das Arbeitsrecht gesetzt. Auch die Regelungen im Datenschutzrecht sind zwingend zu beachten. Bereits der bisherige § 32 BDSG, der durch § 26 BDSG-neu ab dem 25. Mai 2018 abgelöst wird, regelte schon, dass Beschäftigtendaten nur dann erhoben werden dürfen, wenn dies dem Vollzug des Beschäftigungsverhältnisses dient. Das ist nur der Fall, wenn die Daten für dessen Begründung, Durchführung oder Beendigung Relevanz haben. Liegt diese Voraussetzungen nicht vor, ist die Verarbeitung der Beschäftigtendaten dennoch nicht per se unzulässig. Der Beschäftigte kann in jede Verarbeitung seiner personenbezogenen Daten auch einwilligen (§ 4a Abs. 1 BDSG/Art. 7 DS-GVO).

Neu ist in § 26 Abs. 2 BDSG-neu, dass eine freiwillige Einwilligung auch dann vorliegt, wenn durch die Datenverarbeitung ein rechtlicher oder wirtschaftlicher Vorteil für den Arbeitnehmer erreicht wird oder der Arbeitgeber und sein Beschäftigter gleichgelagerte Interessen verfolgen. Während durch die Kontrolle der tatsächlichen Arbeitszeit beim Beschäftigten noch ein Vorteil dahingehend erreicht werden kann, dass etwaige Überstunden sekunden- oder minutengenau erfasst werden und ein konkreter Ausgleich dadurch ermöglicht wird, kann bei einer verdeckten Leistungskontrolle des Beschäftigten, z.B. mittels Keylogger, nicht von einem gleichgelagerten Interesse des Beschäftigten ausgegangen werden. Keylogger kommen damit nur in wenigen Ausnahmefällen zur Aufklärung von Straftaten nach § 26 Abs. 1 S. 2 BDSG-neu in Betracht.

Rechte der Beschäftigten

Während schon heute das Auskunftsrecht, Berichtigungs- und Löschpflichten in Bezug auf Datenverarbeitungen bekannt sind, steht der Arbeitgeber unter den ab dem 25. Mai 2018 geltenden neuen Regelungen der Datenschutz-Grundverordnung (Art. 12-23 DS-GVO) vor weiteren Herausforderungen in Bezug auf die Rechte der Beschäftigten bei der Verarbeitung von deren Daten.

Unter der DS-GVO und dem BDSG-neu wird die transparente und umfassende Informationspflicht der betroffenen Person großgeschrieben. Der Arbeitgeber ist dann angehalten, den Beschäftigten „fair und transparent" z.B. über die Zwecke der Verarbeitung und die Rechtsgrundlage der Verarbeitung, über die Dauer der Speicherung und über das Bestehen eines Auskunftsrechts zu informieren. Das kann durch Mit-

teilungen im Intranet oder in Anlagen zu Betriebs- oder Dienstvereinbarungen erfolgen, die die vom Gesetz verlangten Mindestinhalte aus Art. 13, Art. 14 DS-GVO umfassen.

Zutrittskontrollsysteme

Zutritte zu Gebäuden, Räumen oder einzelnen Systemen können mittels Raumabsicherung (z.B. Scan von Fingerabdruck, Scan von Gesicht) oder auch durch Schließmechanismen, die nur mit bestimmten Schlüsseln entsperrt werden können, verhindert werden. Auch hierbei kommt es heute regelmäßig zur Erfassung personenbezogener Daten, z.B. wenn die Kennziffer eines Zugangsmittels wie einer Chipkarte beim Versuch zum Betreten eines Raums vom System mit Datum und Uhrzeit protokolliert wird oder der Zutrittsversuch eine Videoüberwachung auslöst.

Verarbeitung biometrischer Daten

Problematisch stellt sich die Verwendung von Systemen dar, die biometrische Daten erheben. Ausgestaltet als Fingerabdruckscan oder Gesichtsscan kann eine Zutrittskontrolle zugeschnitten auf den einzelnen Beschäftigten erfolgen. Bislang nicht als besondere personenbezogene Daten angeführt, sind nach Art. 9 Abs. 1 DS-GVO auch für biometrische Daten nun eigene Erlaubnistatbestände erforderlich. Einzig unter den Voraussetzungen des § 26 BDSG-neu, also zur Durchführung des Beschäftigungsverhältnisses, als auch bei Vorliegen einer Einwilligung des Beschäftigten ist die Erhebung der biometrischen Daten möglich. Es kommt bei jedem Scan jedoch darauf an, dass der Betroffene wissentlich und auch willentlich gescannt wird.

Darüber hinaus ist in die Beurteilung mit einzubeziehen, ob die Kenntnis der biometrischen Daten des Beschäftigten für den Zweck, den der Arbeitgeber verfolgt, tatsächlich notwendig ist oder sich die Zutrittsverhinderung auch mithilfe von datenschutzrechtlich weniger einschneidenden Maßnahmen erreichen lässt. Abgewogen werden muss dabei, ob tatsächlich erst die Kenntnis der biometrischen Daten die Zutrittsverhinderung umfassend gewährleisten kann oder ob die Zutrittsverhinderung durch mildere Maßnahmen (z.B. Schlüsselkarten) genauso effektiv erreicht werden kann.

Verschwiegenheitspflicht der Beschäftigten

Zum umfassenden Schutz der Daten innerhalb des Unternehmens ist Arbeitgebern zu empfehlen, die Preisgabe der Daten nach außen durch die Verpflichtung der Mitarbeiter zur Verschwiegenheit zu verhindern. In solchen Verschwiegenheitserklärungen verpflichten sich die Beschäftigten, Stillschweigen über die ihnen bekanntwerdenden Daten zu bewahren. Sollte der Beschäftigte gegen eine solche Erklärung verstoßen und Daten entgegen seiner Verschwiegenheitspflicht preisgeben, ist der Arbeitgeber zur Abmahnung oder sogar zur Kündigung berechtigt. Für den Beschäftigten kann die Preisgabe der Informationen darüber hinaus auch strafrechtliche Relevanz erlangen (§ 17 Abs. 1 UWG).

Fazit

Zeiten- und Zutrittskontrollen sind sowohl arbeitsrechtlich als auch datenschutzrechtlich konform ausführbar. In mitbestimmten Betrieben sind insbesondere die Beteiligungsrechte von Betriebsrat und Personalvertretern zu berücksichtigen. Das Datenschutzrecht zieht die Grenzen für Zeiten- und Zutrittskontrollen in der Notwendigkeit der Kenntnis der personenbezogenen Daten für das Beschäftigungsverhältnis oder der Einwilligung des Beschäftigten.

SASCHA KREMER,
Fachanwalt für IT-Recht, Datenschutzbeauftragter und -auditor, LOGIN Partners Rechtsanwälte, Pulheim

JANA SCHMINDER,
Support Lawyer, LOGIN Partners Rechtsanwälte, Pulheim