



## Kontrolle und Überwachung von Mitarbeitern

*Stephanie Reese, Rechtsanwältin in Hannover*

*Mai 2022*

Die rechtmäßige Handhabung von Kontrolle und Überwachung von Mitarbeitern wird unter der voranschreitenden Digitalisierung immer bedeutender. Umso wichtiger ist es für Unternehmen und Mitarbeiter zu wissen, in welchem Rahmen solche Kontrollen und Überwachungen zulässig sind und ob der Mitarbeiter oder der Betriebsrat zustimmen muss.

Die Gründe für die zunehmende Veranlassung von Kontrollen oder Überwachungen aus Sicht der Unternehmen sind vielfältig. Vor allem die fortschreitende Mobilität in der Arbeitswelt, nicht zuletzt gefördert durch die pandemiebedingten Umstände, haben zum vermehrten Einsatz von Kontrollen und Überwachungen geführt und tun dies auch weiterhin.

Auch ist mit der modernen Technik die Möglichkeit „mal eben zu schauen, was der Mitarbeiter so macht“ bei einer installierten Überwachungssoftware nur einen Klick entfernt.

Insbesondere die durch das Infektionsschutzgesetz (IfSG) vorgegebene temporäre Homeoffice-Pflicht, stellte die Unternehmen so auch vor die Herausforderung und Frage, wie sie die Einhaltung der Arbeitszeit durch die Mitarbeiter überprüfen bzw. nachvollziehen können.

### Allgemeines

Mitarbeiterkontrollen können sowohl als reine Vorkehrungsmaßnahme präventiv stattfinden als auch bei

konkretem Verdacht anlassbezogen durchgeführt werden.

Überwachungen finden je nach Art der gewählten Überwachung offen oder verdeckt statt. Typische offene Überwachungsmaßnahmen sind der Einsatz von Videokameras auf dem Betriebsgelände oder von Magnetkarten zur Arbeitszeiterfassung. Demgegenüber stellt beispielsweise Spionagesoftware auf dem Computer zur Dokumentation der Nutzung des Mitarbeiters eine verdeckte Überwachungsmaßnahme dar.

### Gesetzliche Grundlagen

Das Gesetz setzt allen Überwachungsmaßnahmen Grenzen. Bereits das Grundgesetz verlangt, dass Maßnahmen der Mitarbeiterüberwachung grundsätzlich nicht gegen das Persönlichkeitsrecht, das Selbstbestimmungsrecht und das Recht am eigenen Bild der Mitarbeiter verstoßen dürfen.

Darüber hinaus gibt Art. 88 des Datenschutzgrundverordnung (DSGVO) den EU-Mitgliedstaaten das Recht, eigene Vorschriften im Umgang mit Mitarbeiterdaten zu erlassen. Von dieser Möglichkeit hat die Bundesrepublik Deutschland Gebrauch gemacht und in § 26 Bundesdatenschutzgesetz (BDSG) die „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses“ geregelt. Für ein bestehendes Arbeitsverhältnisses bestimmt § 26 Abs. 1 Satz 1 BDSG:



*(1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies (...) nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist.*

### **Offene und verdeckte Mitarbeiterüberwachung**

Bei der Kontrolle und Überwachung von Mitarbeitern können also offene Verfahren oder aber verdeckte Maßnahmen zum Einsatz kommen. Dazu muss der Unternehmer aber die jeweiligen konkreten Voraussetzungen kennen, um sich nicht rechtswidrig zu verhalten.

#### *Offene Mitarbeiterüberwachung*

Eine offene, dem Mitarbeiter bekannte, Überwachung ist zulässig, wenn das Unternehmen berechtigte Interessen hierfür hat und diese auch nachweisen kann. Plant das Unternehmen, seine Mitarbeiter offen zu überwachen, hat es bei allen Überwachungsmaßnahmen und der Datenspeicherung die Einwilligung der betroffenen Mitarbeiter einzuholen.

Eine offene Mitarbeiterüberwachung kommt in Betracht, wenn ein im Logistikbereich tätiges Unternehmen GPS-Tracking benutzt und dieses für einen reibungslosen Arbeitsprozess den Standort bestimmen muss. Ebenso besteht ein berechtigtes Interesse des Arbeitgebers, wenn er die Arbeitszeit durch Stundenzettel kontrolliert. Schließlich hat jeder Arbeitgeber eine Dokumentationspflicht. Hierbei muss das Unternehmen über jede einzelne Maßnahme aufklären, die von beiden Seiten unterschriebene Einwilligung dafür einholen und die Mitarbeiter über ihr Widerrufsrecht informieren.

Das Unternehmen hat die Einwilligung dahingehend zu dokumentieren, welche Daten zu welchem Zweck

verarbeitet werden. Ebenso ist zu dokumentieren, wie lange die Daten gespeichert werden.

Nicht zweckmäßig ist demgegenüber die Einholung einer grundsätzlichen Einwilligung über eine Regelung im Arbeitsvertrag. Grund hierfür ist das dem Datenschutz immanente Prinzip der „Datensparsamkeit und der zweckgebundenen Verarbeitung“.

Sollen personenbezogene Daten erhoben werden, die für die Durchführung, Beendigung oder Aufnahme des Arbeitsverhältnisses erforderlich sind, bedarf es keiner Einwilligung des Mitarbeiters. Zu solchen Daten gehören z.B. allgemeine Personen- und Kontaktdaten oder auch die Steuer-ID.

#### *Verdeckte Mitarbeiterüberwachung*

Überwachungsmaßnahmen, die gegenüber dem Mitarbeiter verdeckt erfolgen, sind nur in Ausnahmefällen zulässig. Dies ist z.B. der Fall, wenn der Verdacht einer schwerwiegenden Verletzung gegen eine Pflicht aus dem Arbeitsvertrag oder auch einer Straftat besteht. Beim Verdacht einer Straftat muss der Arbeitgeber die Grenzen des § 26 Abs. 1 Satz 2 BDSG im Blick behalten:

*Zur Aufdeckung von Straftaten dürfen personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse der oder des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmaß im Hinblick auf den Anlass nicht unverhältnismäßig sind.*

Damit eine solche Überwachung zulässig ist, muss das Unternehmen also den Verdacht einer Straftat oder einer groben Pflichtverletzung des Arbeitsvertrages durch den Mitarbeiter gut begründen können und alle mildereren Mittel als die einer verdeckten Überwachung ausgeschöpft haben.



Hat ein Unternehmen beispielsweise den Verdacht, dass ein Mitarbeiter Ausstattungen oder Waren des Unternehmens stiehlt oder Adressaufkleber umlabelt und das Paket dadurch vom vorgesehenen Versandzweig abgeleitet wird, und möchte daraufhin eine Videokamera installieren, muss es zuerst prüfen, ob es nicht mit einem milderem Mittel den Fall aufklären oder einen solchen Diebstahl verhindern kann.

Bevor der Arbeitgeber also Überwachungsmaßnahmen trifft, muss er zuvor Dokumentationsmaßnahmen vorausgehen lassen. So könnte das Unternehmen bei der Übergabe der Schicht prüfen, ob die Ausstattung noch vollständig ist.

Auch an eine Taschenkontrolle der Mitarbeiter bei Verlassen des Betriebsgeländes ist zu denken; diese müsste das Unternehmens ebenfalls sehr gut begründen können. Neutralere sind Portalsysteme am Ausgang, die getaggte Gegenstände und Waren digital dektieren.

Wird beispielsweise ein Mitarbeiter beobachtet, wie er früher geht als er in seinem Arbeitszeitkonto dokumentiert, darf das Unternehmen diesem Verdacht nachgehen. Es muss aber dem Mitarbeiter zuerst eine Führungskraft oder einen vertrauensvollen Kollegen an die Seite stellen, bevor es eine Überwachungssoftware nutzen darf.

Dies gilt auch im Falle des Arbeitens aus dem Homeoffice. Damit das Unternehmen die Arbeitszeit des im Homeoffice arbeitenden Mitarbeiters erfassen kann, darf das Unternehmen allerdings die Login-Daten auswerten.

Auch in zeitlicher Hinsicht unterliegen die Überwachungen Beschränkungen. So darf der Arbeitgeber Überwachungssoftware nur punktuell, nicht aber über mehrere Tage hinweg ohne besonderen Grund einsetzen.

### *Strafen bei unrechtmäßiger verdeckter Mitarbeiterüberwachung*

Im Falle rechtmäßiger verdeckter Mitarbeiterüberwachung und Bestätigung des im Raum stehenden

Verdachts, dürfen Unternehmen in arbeitsrechtlicher Hinsicht den Mitarbeiter abmahnen oder im Falle einer schwerwiegenden arbeitsvertraglichen Pflichtverletzung kündigen.

Bei einer unrechtmäßigen verdeckten Mitarbeiterüberwachung drohen dem Unternehmen im schlimmsten Fall Bußgelder von bis zu 20 Millionen Euro oder in Höhe von 4 Prozent des weltweiten Jahresumsatzes.

Unter Umständen kann eine unrechtmäßige verdeckte Mitarbeiterüberwachung auch eine Straftat darstellen und betroffene Mitarbeiter können Schmerzensgeld gegen das Unternehmen geltend machen. Daher sollten Unternehmen obige Grundsätze unbedingt einhalten.

### **Mitwirkung des Betriebsrats**

Im Einzelnen wäre von Seiten des Unternehmens noch ein etwaiges Mitbestimmungsrecht des Betriebsrats zu beachten.

Entscheidet sich das Unternehmen zum Beispiel für die Durchführung einer Taschen- und Torkontrolle oder für den Einsatz von Ortungsgeräten und existiert ein Betriebsrat, so hat dieser mitzubestimmen.

Auch die Einführung einer elektronischen Arbeitszeiterfassung kann der Mitbestimmung des Betriebsrats unterliegen. So legen Teile der Rechtsprechung die in § 87 Abs. 1 Nr. 6 BetrVG geregelte Mitbestimmungspflicht weit aus. Hiernach hat der Betriebsrat mitzubestimmen bei der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen. Die Arbeitsgerichte beziehen hier zum Teil die elektronische Zeiterfassung mit ein.

Die Einsichtnahme in die Arbeitszeit sollte auf das erforderliche Maß beschränkt sein für die zur Einsichtnahme berechtigten Personen. Ebenso muss die Einsichtnahme gemäß § 26 Abs. 1 BDSG für die Durchführung des Beschäftigungsverhältnisses gerechtfertigt sein. So ist der Betriebsrat zwar gemäß § 80 Abs. 1 Nr. 1 BetrVG zur Überwachung dahingehend verpflichtet,



dass die für die Beschäftigten geltenden Gesetz und sonstige Regelungen eingehalten werden und damit auch das ArbZG.

Der Betriebsrat darf dieser Pflicht allerdings vorerst nur dadurch nachkommen, dass anonymisierte Daten zur Verfügung gestellt und ihm gerade nicht umfassende Leserechte eingeräumt werden. Kommt es hierbei zu Abweichungen oder Unstimmigkeit bei der Arbeitszeit, könnte sich in einem folgenden Schritt immer noch eine Identifizierung des einzelnen Mitarbeiters zur Klärung der Unstimmigkeit anschließen.

## Schutz von Geschäftsgeheimnissen

Einer besonderen Herausforderung hat sich das Unternehmen zu stellen, wenn es einerseits bedacht ist, Geschäftsgeheimnisse zu schützen, andererseits aber den Arbeitnehmerdatenschutz beachten muss.

Das Geschäftsgeheimnisgesetz (GeschGehG) verpflichtet die Unternehmen, Konzepte zu entwickeln und einzusetzen, um für das Unternehmen wertvolles Wissen zu schützen und unternehmensintern zu halten. Um zu überprüfen, ob die Geschäftsgeheimnisse auch weiterhin geheim bleiben, ist das Unternehmen zu angekündigten und anlassbezogenen Stichprobenkontrollen berechtigt.

## Fazit

Unternehmen sehen sich zunehmend der Herausforderung gegenüber, den Spagat zwischen Arbeitnehmerschutzrechten und der Wahrung und Sicherung eigener Interessen und Daten zu meistern. Halten sich Unternehmen aber an die oben ausgeführten Grundsätze, gelingt ihnen auch vor dem Hintergrund einer zunehmend digitalisierten und mobilen Arbeitswelt eine Wahrung und Sicherung ihrer Interessen und Daten.

+++

## IMPRESSUM

### HERAUSGEBER

HERFURTH & PARTNER Rechtsanwaltsgesellschaft mbH  
Luisenstr. 5, D-30159 Hannover  
Fon 0511-30756-0 Fax 0511-30756-10  
Mail [info@herfurth.de](mailto:info@herfurth.de), Web [www.herfurth.de](http://www.herfurth.de)  
Hannover · Göttingen · Brüssel  
Member of the ALLIURIS GROUP, Brussels

### REDAKTION

Leitung: Ulrich Herfurth, Rechtsanwalt, zugelassen in Hannover und Brüssel (verantw.)

Mitarbeit: Angelika Herfurth, Rechtsanwältin, FA Familienrecht; Sibyll Hollunder-Reese, M.B.L. (HSG), Rechtsanwältin; Günter Stuff, Steuerberater; Xiaomei Zhang, Juristin (China), Mag. iur. (D); Thomas Gabriel, Rechtsanwalt; JUDr. Yvona Rampáková, Juristin (CR); Dr. Jona Aravind Dohrmann, Rechtsanwalt; Prof. Dr. jur. Christiane Trüe LL.M. (East Anglia); Dr. jur. Reinhard Pohl, Rechtsanwalt; Konstantin Kuhle, Rechtsanwalt; Antonia Herfurth, Rechtsanwältin; Tobias Wundram, Rechtsanwalt; Stephanie Reese, Rechtsanwältin; Sara Nesler, Mag. iur. (Torino), LL.M. (Münster).

### KORRESPONDENTEN

u.a. Amsterdam, Athen, Brüssel, Budapest, Helsinki, Istanbul, Kopenhagen, Lissabon, London, Luxemburg, Mailand, Madrid, Moskau, Oslo, Paris, Stockholm, Warschau, Wien, Zug, New York, Toronto, Mexico City, Sao Paulo, Buenos Aires, New Delhi, Peking, Tokio.

### VERLAG

CASTON GmbH, Law & Business Information  
Luisenstr. 5, D-30159 Hannover,  
Fon 0511 - 30756-50 Fax 0511 - 30756-60  
Mail [info@caston.info](mailto:info@caston.info); Web [www.caston.info](http://www.caston.info)

Alle Angaben erfolgen nach bestem Wissen; die Haftung ist auf Vorsatz und grobe Fahrlässigkeit beschränkt. Wiedergabe, auch auszugsweise, nur mit Genehmigung der Herausgeber.