



Interne Ermittlungen im Unternehmen

Unternehmens- und Reputationsschutz durch „internal investigation“
Reihe „Schacht Arbeitsrecht“

© Rechtsanwalt Stefan Schröter, Gunzenhausen

Internal Investigations: Arbeitsrecht und Datenschutz im Unternehmen

© Rechtsanwalt Stefan Schröter, Gunzenhausen, Gunzenhausen

Was hat ein milliarden schwerer Korruptionsfall mit dem mutmaßlichen Diebstahl eines Pfandbonds im Wert von 1,43 Euro zu tun?

Big Brother scheint Einzug zu halten in die heiligen Hallen des Deutschen Unternehmertums. Unternehmensinterne Verfehlungen lösen nicht nur lokal fristlose Kündigungen, einen weltweiten Reputationsschaden und eine schwere interne Vertrauenskrise aus, sondern auch einen regelmäßigen medialen Overkill über Ethik, Verhältnismäßigkeit und Rechtsnormen im Deutschen Unternehmertum.

Diese ungebremsste öffentliche Neugier in Verbindung mit gesellschaftlichen Neidpotenzialen verändert nachhaltig die Kultur von Unternehmen jeder Größe.

Compliance auch in der Großindustrie ein Zukunftsthema

Ein milliarden schwerer Korruptionsfall veranlasste Siemens, eine eigene Compliance-Risikostruktur aufzubauen, unter Einsatz von mehr als 500 Compliance-Officern, bis hin zum Aufbau einer eigenen Compliance-Risikostruktur.

Notwendigkeiten und Hindernisse interner Überwachung am Arbeitsplatz

Ich nutze diesen Aufsatz, um aus Rechtssicht über Notwendigkeiten und Hindernisse interner Überwachung am Arbeitsplatz zu informieren. Ich habe diese Kapitel gewählt:

- I. Schäden durch unternehmensinterne Verfehlungen
- II. Kontrollmotive des Arbeitgebers für heimliche Überwachung am Arbeitsplatz
- III. Formen von Mitarbeiterkontrollen
 - Video
 - Privatdetektiv
 - Handy, GPS, RFID, Keylogger
 - E-Mail-Auswertung
- IV. Verdachtskündigungen
- V. Fazit

I. Schäden durch unternehmensinterne Verfehlungen

Studien zufolge entstehen deutschen Unternehmen jährlich Gesamtschäden in Höhe von 2,5 bis 17,5 Mrd. Euro durch Straftaten eigener Arbeitnehmer^[1]. Diese Schäden entstehen unter anderem durch

- Mitarbeiterdiebstähle
- Verrat von Geschäftsgeheimnissen
- Compliance Verstöße (z. B. Vorenthalten und Veruntreuen von Arbeitsentgelt, § 266 a StGB)
- Verstöße gegen Bestimmungen der EU-DS-GVO und des BDSG
- Haftung für fehlerhafte Zolldanmeldung durch Arbeitnehmer
- Verstöße gegen Arbeitsschutzvorschriften
- Verstöße gegen das MiLoG

II. Kontrollmotive des Arbeitgebers für heimliche Überwachung am Arbeitsplatz

Unternehmen haben daher ein nachvollziehbares Interesse, bereits begangene Straftaten aufzuklären.

Der Arbeitgeber kann häufig solche Straftaten nur durch verdeckte Ermittlungsmaßnahmen verfolgen.

Gerade bei trickreichen Tätern sind Kontrollmaßnahmen, die mit Kenntnis der Mitarbeiter erfolgen, oftmals kein taugliches Aufklärungsmittel.

Unternehmen führen daher heimliche Mitarbeiterkontrollen regelmäßig zu repressiven Zwecken durch.^[2]

III. Formen heimlicher Mitarbeiterkontrollen

Verschiedene Formen heimlicher Kontrollmaßnahmen werden eingesetzt, die unterschiedlich stark in das Persönlichkeitsrecht der überwachten Arbeitnehmer eingreifen.

1. Videokontrollen

Der Einsatz von Videokameras breitet sich nicht nur auf öffentlichen Plätzen, sondern auch in Betrieben aus. In einem größeren Hannoveraner Modegeschäft waren insgesamt 128 Videokameras installiert, bevor es dem neugegründeten Betriebsrat gelang, ihre Zahl im Wege der Mitbestimmung auf 67 zu reduzieren^[3]

Eine solche Observationstechnik besitzt auch nach Meinung des Gesetzgebers eine besondere Eingriffsqualität (so der Bericht des Innenausschusses Bundestags Drucksache 14/5793, 61), die bei heimlicher Vorgehensweise noch erheblich gesteigert wird (LAG Hamm, ZD 2014, 204).

Der Betroffene wird in seiner Verhaltensweise, einschließlich seiner Bewegungen und seiner jeweiligen Stimmungen weitestgehend erfasst.

Bereits die offene Videoüberwachung im Unternehmen löst, unter Berücksichtigung der Bestimmungen der EU-Datenschutzgrundverordnung, deutlich ausgeweitete Informationspflichten des Arbeitgebers aus. Es müssen unter anderem

- zusätzlich die Kontaktdaten des betrieblichen Datenschutzbeauftragten, des für die Videoüberwachung Verantwortlichen und dessen Vertreter genannt werden.
- weitere Informationen durch den Arbeitgeber mitgeteilt werden, etwa Zweck, Rechtsgrundlagen, sowie die berechtigten Interessen der Videoüberwachung.
- Angaben zur Speicherdauer, sowie zu Auskunfts- und Lösungsrechten gemacht werden.

Umso dringender müssen die konkreten Verdachtsmomente eines strafbaren und/oder pflichtwidrigen Fehlverhaltens gegenüber einem heimlich videoüberwachten Arbeitnehmers sein.

Der Fall Lidl

Im Fall Lidl spielten verdeckte Kameras eine zentrale Rolle. Entgegen des Anspruchs des Bundesverfassungsgerichts und dem Transparenzgebot des Artikel 5, Abs. 1 a DS-GVO wird für den Einzelnen völlig unklar, wer was und bei welcher Gelegenheit über ihn weiß^[4]

Videokontrolle in öffentlich zugänglichen Räumen:

Befindet sich der Arbeitsplatz in einem öffentlich zugänglichen Raum (z.B. Laden, Tankstelle, Bankfiliale), muss der Betreiber seit dem 25.05.2018 eine Interessenabwägung zwischen dem Kontrollinteresse des Arbeitgebers und dem Persönlichkeitsrecht des Mitarbeiters vornehmen.

Vor dem Einsatz der Anlage muss ihr Zweck konkret festgelegt werden, um die Rechtmäßigkeit des Videoeinsatzes überprüfbar zu machen^[5].

Zulässig ist die Überwachung des öffentlichen Raums durch Videokameras, wenn

- sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist
- keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

- sie strafbare Handlungen zu verhindern hilft.

Schutzwürdige Interessen der Betroffenen können überwiegen

Der Zweck, strafbare Handlungen zu verhindern, darf z.B. nicht die Überwachung von Toiletten und Umkleieräumen rechtfertigen, da die schutzwürdigen Interessen der betroffenen Personen höher gestellt ist.

Überwachte Bereiche müssen auf das Notwendige beschränkt sein.

Videokontrolle von Mitarbeitern in öffentlich begehbaren Räumen

Arbeitnehmer, die in öffentlich zugänglichen Räumen als Verkäufer, Bankangestellte, Museumwärter usw. beschäftigt sind, müssen

- sich in einen nichtüberwachten Raum entziehen können
- Anlass gegeben haben, die Videoüberwachung durchzuführen. Ohne einen solchen Anlass ist die Videoüberwachung verboten.

Der Eingriff in das allgemeine Persönlichkeitsrecht ist dann besonders gravierend, wenn

- die Überwachung kontinuierlich erfolgt
- der Einzelne ihr nicht ausweichen kann.

Voraussetzung ist deshalb immer, dass ohne eine solche Maßnahme gravierende Nachteile drohen, die durch eine Stichprobenkontrolle nicht verhindert werden können.

Kamera-Attrappen

Auch das Installieren einer bloßen Kamera-Attrappe wird rechtlich dem Aufstellen einer realen Kamera gleichgestellt^[6], sodass auch ohne das effektive Festhalten und Speichern von Daten ein rechtswidriger Eingriff in Persönlichkeitsrechte vorliegen kann.

Heimliche Video-Kontrollen in nicht öffentlich zugänglichen Räumen:

Versteckte Kameras, deren Existenz dem betroffenen Arbeitnehmer nicht bekannt sind, sind grundsätzlich unzulässig^[7].

Sie gelten als übermäßiger Eingriff in das allgemeine Persönlichkeitsrecht.

Auch eine offen eingesetzte - ausschließlich der Kontrolle des Arbeitsverhaltens dienende - Videotechnik wird als Verstoß gegen die Menschenwürde und damit als unzulässig gewertet^[8].

- Ausnahme:
Vorliegen eines „überwiegend, schutzwürdigen Interesse des Arbeitgebers“.
Zulässig ist die Situation nur dann, wenn ein überwiegendes schutzwürdiges Interesse des Arbeitgebers für eine Überwachung spricht, weil sich beispielsweise erhebliche Warenverluste nur auf diese Weise aufklären lassen^[9].
Richtet sich der Verdacht gegen ein Gruppenmitglied, so kann sogar vorübergehend die gesamte Gruppe observiert werden, sofern es sich nicht nur um den Verdacht einer relativ geringfügigen Verfehlung handelt.

Generalverdacht löst keine rechtmäßige Videoüberwachung aus

Kommen Gegenstände abhanden, ohne dass sich ein konkreter Verdacht gegen bestimmte Personen ergibt, so kann nicht die ganze Belegschaft unter Beobachtung gestellt werden; vielmehr ist auf die Torkontrolle als milderes Mittel zurückzugreifen^[10]

Problematik der Zufallsfunde in Videoaufnahmen:

Zufallsfunde bei Videoüberwachungen sind in einem Prozess dann verwertbar, wenn das Beweisinteresse des Arbeitgebers im Zuge einer durchzuführenden Interessenabwägung höher zu gewichten ist, als das Interesse des Arbeitnehmers an der Achtung seines allgemeinen Persönlichkeitsrechts.

Arbeitsgerichte verwerten Videos zur Beweissicherung

Häufig verwerten Arbeitsgerichte das Videomaterial, wenn dadurch entweder strafbare Handlungen oder schwerwiegende Pflichtverletzungen bewiesen werden können und der Arbeitgeber ein nachvollziehbares, überwiegendes Interesse hat, Missstände in seinem Unternehmen aufzudecken und in Zukunft zu unterbinden.

- Beispiel legaler Videoüberwachung:
Gerichte würden die heimlich aufgenommene Misshandlung einer Patientin durch eine Pflegekraft in einer Pflegeeinrichtung verwerten, wenn dadurch Taten bewiesen werden können.

2. Einsatz von Privatdetektiven

Der Einsatz von Detektiven kann nur zu repressiven Zwecken erfolgen.

Es muss der konkrete Verdacht einer Straftat zu Lasten des Arbeitgebers gegen einen abgrenzbaren Kreis an Mitarbeitern vorliegen.

Wird ein Privatdetektiv eingesetzt, so werden die Beobachteten in der Regel bewusst im Unklaren gelassen, dass eine Kontrollmaßnahme stattfindet.

Nach der bisherigen Rechtslage lassen sich auch verdeckte Observationen durch Privatdetektive in engen Ausnahmefällen legitimieren.

Ist der Privatdetektiv-Einsatz „verhältnismäßig“?

Der Detektiveinsatz muss das letzte Mittel zur Aufklärung darstellen und darf nicht unverhältnismäßig sein^[11]. Verhältnismäßig ist er nur, wenn

- der Observationseinsatz zeitlich begrenzt wird.
- die Privatsphäre des Arbeitnehmers geschützt bleibt.

Wann ist eine heimliche Überwachung von Mitarbeitern zulässig?

Eine Interessenabwägung im Einzelfall stellt fest, ob die Kontrollinteressen des Arbeitgebers gegenüber dem Persönlichkeitsschutz der Mitarbeiter überwiegen. Nur dann wäre eine heimliche Überwachung zulässig.

• Beispielsfall¹

Eine Münsteraner Sekretärin, 50, war sieben Monaten im Unternehmen, als es zum Streit mit ihrem Chef kam. Dieser kritisierte, dass sie ihm Unterlagen nicht schnell genug vorlege. Sie verteidigte sich, doch der Konflikt blieb ungelöst. 15 Tage später meldete sich die Mitarbeiterin plötzlich krank und erscheint dann über 2 Monate nicht zum Dienst. Der Vorgesetzte vermutete, dass seine Sekretärin nicht krank ist, sondern „krank feiert“.

Er engagierte eine Detektei, die heimlich Filmaufnahme anfertigte. Die heimliche Observierung mittels Detektiv und das heimliche Filmen erfolgte nach Ansicht des BAG rechtswidrig, weil der Anlass für die Überwachung nur auf Vermutungen fußte. Die Videoaufnahmen waren damit erst recht nicht rechtmäßig, daher stand der Frau Schmerzensgeld zu.

Die Sekretärin forderte 10.500,00 € Schmerzensgeld. Das Landesarbeitsgericht, wie auch die Vorinstanz, hat ihr lediglich 1.000,00 € Schmerzensgeld zugesprochen.

Anlass für die Beauftragung des Detektives war aus Sicht des Arbeitgebers die Übermittlung einer Erstbescheinigung während des Winterurlaubs wegen der Diagnose schwere Bronchitis mit Rippenfellentzündung.

Es folgten weitere Arbeitsunfähigkeitsbescheinigungen. Der Detektiv verfolgte die Kranke und hielt in einem Bericht fest, dass die Frau keinesfalls bewegungsunfähig

¹ Bundesarbeitsgericht Az. 8 AZR 1007/13.

war. Es wurde beobachtet, wie zwei leere Mülltonnen vom Fußweg Richtung Wohnhaus geschoben wurden, wie sie sich bückte, um einen Hund zu begrüßen. Filmaufnahmen erfolgten auch im Waschsalon.

- Kommentar: Überführte Blaumacher müssen unter Umständen auch die Detektivkosten tragen.

3. Handy, GPS, RFID, Keylogger, E-Mail-Auswertung

Der Chef beobachtet Mitarbeiter und macht Beweisfotos mit seinem Handy. Darf er diese verwerten?

Beobachtet ein Vorgesetzter zufällig in seiner Freizeit einen krankgeschriebenen Mitarbeiter, wie er seinen PKW in der Autowaschanlage reinigt, so kann er dies nach Auffassung des LAG Rheinlandpfalz mit seinem Fotohandy im Bild festhalten^[13]

Detektiv nutzt GPS Technik. Ist das erlaubt?

Detektive machen sich strafbar, die heimlich an LKWs GPS-Sensoren anbringen, um auf diese Weise ein Bewegungsprofil der Fahrer zu erstellen.

Nach neuem Datenschutz-Recht ist wegen unerlaubter Datenerhebung zumindest ein erhebliches Bußgeld nach Artikel 83 DS-GVO fällig.

Bewegungsprofile mit Hilfe von GPS zur Arbeitsorganisation unnötig

Für den Arbeitgeber kann es interessant sein, wer sich zu welchem Zeitpunkt an welchem Ort aufhält. Dies gilt insbesondere für Außendienstmitarbeiter und Fahrer, die ggf. umdirigiert werden können, um einen eben eingegangenen Auftrag zu erledigen. Technisch lässt sich dies unschwer mit Hilfe von GPS und Handyortung bewerkstelligen.

Grundsätzlich sind derartige Eingriffe in die Persönlichkeitssphäre nicht erforderlich, weil der Arbeitgeber seine Mitarbeiter verpflichten kann, während der Fahrt auf Handy erreichbar zu sein.

Durch ein kurzes Gespräch kann er dann den Standort erfragen und ggf. die Route neu bestimmen, weil es noch Zusätzliches zu erledigen gibt.

RFID (radio-frequency identification)

RFID² ist derzeit auf dem Vormarsch und in Deutschland als Kontrollinstrument unzulässig. Die Technik besteht aus zwei Komponenten. Bisher wird diese Technik insbesondere zur Verbesserung der logistischen Steuerung, etwa des Warenflusses oder des Koffertransports auf Flughäfen eingesetzt.

Keylogger^[14]- Ist die Überwachung der Internetnutzung am Arbeitsplatz erlaubt?

Der Unternehmer hat ein Interesse daran zu erfahren, wie oft, wie lange und wie intensiv seine Mitarbeiter privat das Internet während der Arbeitszeit nutzen.

In den Arbeitsverträgen ist meist geregelt, dass der Arbeitnehmer Hard- und Software aus Gründen der informationstechnischen Sicherheit ausschließlich zur Erfüllung der vereinbarten Aufgaben nutzt.

² Technische Erklärung von RFID: Anders als bei einem Barcode ist dafür keine unmittelbare Nähe mehr erforderlich. Theoretisch könnte man die Lesegeräte so einstellen, dass das Auftauchen von Tags noch in 30 Metern Entfernung registriert würde.

Der Marburger Bund der angestellten Ärztinnen und Ärzte hat dem BMAS im Rahmen der Diskussion um Arbeit 4.0 mitgeteilt, Dienstkleidung werde zunehmend mit RFID Technologie ausgestattet, wodurch sich ein detailliertes Bewegungsprofil von Ärzten erstellen lasse.

Viele andere Anwendungen sind jedoch denkbar. Soweit eine relativ dichte Infrastruktur von Lesegeräten besteht, können über einzelne Mitmenschen, in deren Kleidung sich Tags befinden, unschwer Bewegungsprofile erstellt werden. Dies kann in der Regel unbemerkt geschehen, da weder Tag noch Lesegerät auffallen, wenn sie der Betroffene nicht systematisch sucht.

Auf einer Ware oder auf der gekauften Kleidung eines Menschen ist ein Tag, ein sogenannter batterieloser Transponder angebracht. Er enthält einen Mikrochip, der bestimmte Daten gespeichert hat und sie bei Annäherung an ein Lesegerät (die zweite Komponente) an dieses übermittelt.

- Fall:

In einer Mail an alle Mitarbeiter informiert der Arbeitgeber über die Überwachung und Speicherung der Tastaturredaten und kündigt Konsequenzen im Fall der Zuwiderhandlung an:

Hallo Liebes ...-Team,

es ist so weit, die Telekom hat es endlich geschafft, uns einen schnellen Internetanschluss bereitzustellen. Dieses möchte ich natürlich euch nicht vorenthalten. Aus diesem Grund erhaltet Ihr freien Zugang zum WLAN. Da bei Missbrauch, z.B. Download von illegalen Filmen etc. der Betreiber zur Verantwortung gezogen wird, muss der Traffic mit geloggt werden. Da ein rechtlicher Missbrauch natürlich dann auf denjenigen zurückfallen soll, der verantwortlich dafür war.

Somit: Hiermit informier ich Euch offiziell, dass sämtlicher Internet Traffic und die Benutzung der Systeme mitgeloggt und dauerhaft gespeichert wird. Solltet ihr damit nicht einverstanden sein, bitte ich mir dieses innerhalb dieser Woche mitzuteilen.

Der Kläger widersprach nicht. Die Beklagte installierte auf dem Dienst-PC des Klägers eine Software, die alle Tastatureingabe protokollierte und regelmäßige Screenshots fertigte (Keylogger).

In einem Gespräch mit dem Kläger gab dieser zu, seinen Dienstrechner während der Arbeitszeit privat genutzt zu haben. Er gab genaue Zeiten und Abläufe und Gründe an für sein Verhalten (3 Stunden für das, 10 Minuten täglich für das Logistikunternehmen seines Vaters, etc.)

Die daraufhin von der Beklagten auf Arbeitszeitbetrug gestützte Kündigung war in allen Instanzen erfolglos.

Unsere Rechtskommentare zu diesem Fall:

1. Das Nichtwidersprechen stellt keine notwendige Einwilligung dar.
Keylogger-Einsatz erfordert den konkreten Anfangsverdacht einer Straftat oder einer anderen schweren Pflichtverletzung. Dies war hier nicht der Fall.
2. Der Einsatz von Keyloggern ist nicht per se unzulässig.
Ermittlungsmaßnahmen gemäß § 32 Abs. 1 BDSG erfordern keinen Straftatverdacht, sondern sind auch bei Verdachtsmomenten nur bezüglich einer Pflichtverletzung erlaubt. Als Verdachtsgrad reicht ein Anfangsverdacht.
3. Die Einwilligung des Arbeitnehmers ist erforderlich.
Es ist eine wirksame Einwilligung der betroffenen Arbeitnehmer nach detaillierter Aufklärung über Art und Umfang der Kontrollmaßnahme zwingend erforderlich.

E-Mailauswertung – Was darf der Arbeitgeber? Was darf er nicht?

Volkswirtschaftlich entsteht durch die private Nutzung von geschäftlichen Mail-Accounts sowie durch privaten Mailverkehr vom privaten Account des Mitarbeiters während der Arbeitszeit ein immenser Schaden.

Leider wird dieser nicht kleiner, wenn Bestimmungen im Arbeitsvertrag dazu fehlen.

Wie und wann darf der Arbeitgeber private Mailkontakte kontrollieren?

Der Arbeitgeber darf die Nutzung des betrieblichen E-Mailkontos für private Zwecke kontrollieren, wenn dies im Rahmen des Arbeitsvertrages ausdrücklich vereinbart wurde und der Betroffene in Kontrollen vertraglich eingewilligt hat

Lösung: Holen Sie schriftliche Einwilligungen zur E-Mailauswertung ein!

Klarheit für den Arbeitnehmer und Rechtssicherheit für den Arbeitgeber stellen Sie durch schriftliches Einverständnis Ihrer Mitarbeiter mit Ihren Kontrollmaßnahmen her.

Um den datenschutzrechtlichen Transparenzgebot zu genügen, muss die Einwilligungserklärung so sein:

- klar
- schriftlich
- verständlich
- aussagekräftig

Der Arbeitnehmer muss dabei

- über den genauen Umfang und Zweck der Erhebung informiert sein
- über Verarbeitung und Nutzung seiner personenbezogenen Daten informiert werden
- über die namentlichen Empfänger der Daten informiert werden.
- in der schriftlichen Einwilligungserklärung ausreichende Bestimmtheit^[15] vorfinden.
- die Tragweite seines Einverständnisses erkennen können.
- freiwillig und nicht aus einer Drucksituation heraus erfolgen.
- seine Einwilligung jederzeit und ohne Begründung widerrufen können

Unser Tipp:

Wegen des letzten Punktes sollten Arbeitgeber in der Einwilligungserklärung auf ebenfalls einschlägige, gesetzliche Erlaubnistatbestände für die Datenverarbeitung zurückzugreifen.

Ist eine Einwilligung erteilt, darf der Arbeitgeber die E-Mails im Rahmen der definierten Grenzen nutzen.

IV. Wenn sich der Verdacht im Zuge der internen Ermittlungen erhärtet - Verdachtskündigung

Der Verdacht, der Vertragspartner könne eine strafbare Handlung oder schwerwiegende Pflichtverletzung begangen haben, kann nach ständiger Rechtsprechung des BAG einen wichtigen Grund für eine außerordentliche Kündigung bilden^[16].

Gerade der Verdacht ruiniert das notwendige Vertrauen des Arbeitgebers in die Redlichkeit des Arbeitnehmers und wird zu einer unerträglichen Belastung des Arbeitsverhältnisses^[17].

Verdachtskündigung: ein eigenständiger Tatbestand

Die Kündigung wegen Verdachts stellt neben der Kündigung wegen der Tat einen eigenständigen Tatbestand dar.

Bei der Tatkündigung ist für den Kündigungsentschluss maßgebend, dass

- der Arbeitnehmer nach der Überzeugung des Arbeitgebers die strafbare Handlung tatsächlich begangen hat
- dem Arbeitgeber aus diesem Grund die Fortsetzung des Arbeitsverhältnisses unzumutbar ist.

Zerrüttetes Vertrauen als Kündigungsgrund

Nicht das pflichtwidrige Fehlverhalten des Arbeitnehmers muss der Unternehmer vor Gericht beweisen, sondern Verdachtsmomente, die das Vertrauen erschüttern.

Der Arbeitgeber kann wegen desselben Sachkomplexes sowohl eine Tat- als auch eine Verdachtskündigung aussprechen.

Der Arbeitgeber profitiert bei einer Verdachtskündigung von Beweiserleichterungen.

V. Fazit in elf Erkenntnissen

1. Eine heimliche Überwachung von Mitarbeitern ist nicht generell rechtswidrig.
2. Heimliche Videoüberwachung ist nur dann zulässig, wenn ein überwiegendes schutzwürdiges Interesse des Arbeitgebers für eine Überwachung spricht.

3. Ohne Vorliegen konkreter Verdachtsmomente ist eine heimliche Videoüberwachung unzulässig.
4. Zufallsfunde in Videoaufnahmen sind aber nicht generell unverwertbar.
5. Auch neue Überwachungsmethoden, wie z. B. Keylogger sind nicht per se unzulässig.
6. Wirksame Einwilligungen der Betroffenen nach detaillierter Aufklärung über Art und Umfang der Kontrollmaßnahme sind Grundlage für eine legale Überwachung.
7. Keyloggern oder E-Mailauswertungen müssen Arbeitnehmer schriftlich zustimmen.
8. Bei der Anhörung des verdächtigten Arbeitnehmers ist ein Wortprotokoll anzufertigen. Der Untersuchungsführer ist niemals der Protokollführer.
9. Wenn sich der Verdacht im Zuge der internen Ermittlungen erhärtet, ist zwingend an die Möglichkeit einer Verdachtskündigung zu denken.
10. Die internen Ermittlungen sind zügig, aber nicht mit hektischer Eile durchzuführen. Während der Anhörung des betroffenen Arbeitnehmers ist die zweiwöchige Kündigungserklärungsfrist gehemmt.
11. Bei einer Verdachtskündigung muss der Unternehmer vor Gericht nicht das pflichtwidrige Fehlverhalten beweisen, sondern das Vorliegen dringender Verdachtsmomente, die das Vertrauen erschüttern. Insofern gelten Beweiserleichterungen.

Ich freue mich auf Ihre Fragen!



Rechtsanwalt Stefan Schröter

Fachanwalt für Arbeitsrecht

Fachanwalt für Medizinrecht

Fachanwalt für Versicherungsrecht

Telefon: 09831 6707-14/-15 (Assistenz: Frau Julia Reiser und Frau Lisa Zier)

Mail: s.schroeter@dres-schacht.de

www.schacht-unternehmeranwaelte.de