

„Compliance akut“- Internal Investigations zwischen Licht und Schatten

INTERVIEW mit Ass. jur. Paul H. Malberg



Die öffentliche Wahrnehmung von internen Ermittlungen ist immer spannungsgeladen. Die Perzeption betrifft überwiegend solche Fälle, bei denen im Verlauf der Recherchen gegen Datenschutzvorschriften und Arbeitnehmerrechte verstoßen wurde oder die Rechtsprechung den gesetzgeberischen Willen und die Reichweite des Erlaubten definieren und sanktionieren muss. Was also ist die Best Practice und wie sehen die Ermittlungen der Zukunft aus?



Rechtsassessor Paul H. Malberg
ist Geschäftsführer der Detektei PROOF-MANAGEMENT GmbH,
Hamburg, Düsseldorf, Frankfurt/M., Köln.

ZAU: Herr Malberg, das LAG Düsseldorf (vom 26.04.2023 – 12 Sa 18/23) hatte zuletzt einem Arbeitnehmer wegen einer illegalen Überwachung durch eine Detektei eine Entschädigung i.H.v. 1.500 € zugesprochen. Sollten Arbeitgeber bei Verdacht auf Straftaten überhaupt noch ermitteln (lassen) und wie können sich Arbeitgeber davor schützen, dass sie einem Boomerang erliegen?

Malberg: Das zitierte Urteil zeigt in den Gründen die Schattenseiten und Risiken der Sachverhaltsklärung auf. Es ändert aber nichts an der Notwendigkeit, auf Verdachtsmomente zu reagieren und Licht ins Dunkel zu bringen.

Jeden Tag ermitteln Unternehmen und spezialisierte Ermittler klärungsbedürftige Sachverhalte sauber aus. Nur werden sie in aller Regel von der Öffentlichkeit nicht wahrgenommen. Zu den Ausnahmen gehören im Wesentlichen nur die Fälle, in denen Compliance-Fälle medial bereits nach außen gedrungen sind und die Unternehmen sich durch eine „lückenlose Aufklärung“ reinwaschen.

Bei jeder kritischen Meldung, die eine Maßnahme der Aufklärung moniert, ist es ratsam, die Hintergründe zu beleuchten.

Ohne im Detail auf die konkrete Entscheidung des LG Düsseldorf einzugehen, fällt zu diesem Themengebiet nach Studium der Rechtsprechung ins Auge, dass im Wesentlichen drei Fehler zur Angreifbarkeit von investigativen Maßnahmen führen.

1. In einer Vielzahl der Fälle fehlt es bereits an einem Anfangsverdacht i.S.d. § 26 Abs. 1 Satz 2 BDSG, um Daten von Beschäftigten zu erheben. Nehmen wir z.B. den typischen Fall eines Mitarbeiters, bei dem lediglich aus einem Bauchgefühl heraus Lohnfortzahlungsbetrug oder Sozialleistungsbetrug vermutet wird. In nahezu allen Anfragen dieser Art – und sie kommen nicht selten – müssen wir von Ermittlungen abraten, da bereits der Anfangsverdacht des § 26 Abs. 1 Satz 2 BDSG nicht sauber begründet werden kann. Denn der Regelfall ist, dass das Unternehmen die Gründe, die zur Arbeitsunfähigkeitsbescheinigung geführt haben, nicht kennt. Und

wie wollen Sie den Beweiswert einer Arbeitsunfähigkeit erschüttern, wenn Ihnen die Hintergründe der Arbeitsunfähigkeit gänzlich unbekannt sind? Und selbst, wenn Sie Anhaltspunkte für eine psychische Erkrankung haben, sind in diesen Fällen dem Erlaubten fast keine Grenzen gesetzt. Es lässt sich auf dieser löchrigen Basis schwerlich einschätzen, welches Verhalten des arbeitsunfähigen Mitarbeitenden genesungswidrig und welches konform ist. Und damit sind wir beim zweiten Fehler.

2. Die notwendige Verhältnismäßigkeit der Datenerhebungen scheidet oft schon an der Geeignetheit. Bei einem arbeitsunfähigen Mitarbeitenden setzt die Geeignetheit einer Beobachtung aber voraus, dass durch die Beobachtung seiner Person der Beweiswert der Arbeitsunfähigkeit tatsächlich erschüttert werden kann. Wenn Sie aber nicht wissen, nach welchem regelwidrigen Verhalten Sie Ausschau halten sollen, wird schon die Geeignetheit kaum konstatiert werden können. Zur Prüfung der nachfolgenden Erforderlichkeit und Angemessenheit kommen Sie da gar nicht mehr.
3. Der dritte und in meinen Augen größte Fehler ist, dass eine ordentliche und chronologisch geführte Dokumentation des Compliance-Falls ausbleibt, in der erste Hinweise und Verdachtsmomente, konkrete Personenkreise und Geschehnisse sowie weitere relevante Daten und Fakten festgehalten werden. Die Dokumentation bildet das Fundament, um im Weiteren die erforderlichen Abwägungen zu treffen und festzuhalten. Sie dient zum einen der eigenen Reflektion, Verdachtsmomente und Maßnahmen nüchtern zu analysieren, zu bewerten und die Verhältnismäßigkeit zu prüfen. Zum anderen nutzt eine vorzeigbare, lückenlos geführte Kladde als glaubwürdige argumentative Stütze im etwaigen Kündigungsschutzprozess.

ZAU: Haben Unternehmen also heute kaum noch Möglichkeiten, auf vermuteten Lohnfortzahlungsbetrug zu reagieren? Und wie sieht es mit anderen Formen des Fehlverhaltens aus?

Malberg: Wie so oft – es kommt auf den Einzelfall an. Wenn mir alle relevanten Umstände mitgeteilt werden, bewerte ich mit den Entscheidern akribisch den Sachverhalt und die im Raum stehenden Verdachtsmomente. Dabei achte ich darauf, dass ein folgender Prozess von Anfang an sauber aufgesetzt wird.

Und um die Lebenswirklichkeit realistischer wiederzugeben: Wir werden nicht nur aufgrund von „Bauchgefühlen“ angesprochen. In der Mehrheit der Anfragen sind die Sachverhalte komplexer und beinhalten konkrete Hinweise, die den Weg in § 26 Abs. 1 Satz 2 BDSG und die Sachverhaltsklärung eröffnen.

Erweitern wir den Fall des vermeintlich arbeitsunfähigen Mitarbeitenden um den Umstand, dass er eine Tätigkeit in einem anderen Betrieb ausüben soll. Wird der Ort der Nebentätigkeit aufgrund eines Hinweises bereits vermutet, lässt sich eine umfassende und unverhältnismäßige Beobachtung des Mitarbeitenden vermeiden, indem z.B. lediglich der Ort der mutmaßlichen Nebentätigkeit in den Fokus genommen wird.

Nach meiner Erfahrung liegt in diesem simplifizierten Fall ein nur marginaler und vertretbarer Eingriff in das allgemeine Persönlichkeitsrecht des Mitarbeitenden. Und das kann selbst dann gelten, wenn die krankheitsbedingten Gründe für die Arbeitsunfähigkeit unbekannt sind.

Ein wesentlicher Faktor für die verhältnismäßige Überwachungsmaßnahme ist, in kurzer Zeit und mit möglichst niedriger Eingriffsintensität eine dolose Systematik festzustellen, die den Beweiswert der Arbeitsunfähigkeit erschüttert.

Ich gebe aber zu, dass der Nachweis von Lohnfortzahlungsbetrug wegen des geltenden Datenschutzes und der wenigen Informationen, die dem Arbeitgeber für gewöhnlich zur Verfügung stehen, oftmals eine besondere Herausforderung darstellt. Von daher nimmt in diesen Fällen die objektive Erstberatung durch uns sowie die Verhinderung von unüberlegten Schnellschüssen einen wichtigeren Platz ein als die ursprünglich angefragte Überwachung.

Bei anderen Arten von vermutetem Fehlverhalten sieht es da regelmäßig anders aus. Blicken Sie auf Arbeitszeitbetrug, Diebstahl, Geheimnisverrat oder andere Delikte, die mehr oder weniger in jedem Unternehmen mal Thema sind.

Ganz überwiegend finden sich hier Ansätze, um die Aufklärung rechtskonform voranzubringen, weil in diesen Fällen mehr Informationen über die Tat und den potenziellen Täterkreis bekannt geworden sind.

Das können adaptierte verdeckte Beobachtungen sein, die IT-forensische Prüfung von Betriebsrechnern und Handys oder offen geführte interne Ermittlungen in Form von z.B. Mitarbeiterinterviews. Auch datenschutzkonforme verdeckte Videoüberwachungen sind denkbar. Letztlich hängt alles von den Umständen des Einzelfalls ab.

ZAU: Können Sie uns aus der jüngeren Vergangenheit Beispiele nennen, bei denen die Aufklärung durch Sie als Externe den Unternehmen einen deutlichen Mehrwert verschafft hat?

Malberg: Im Jahr 2023 waren wir z.B. mit dem Fall betraut, dass hochwertige Materialien über Nacht aus einer Betriebsstätte in NRW gestohlen wurden. Der Schaden belief sich auf über eine Millionen Euro. Die Begutachtung des Tatorts und der Tatspuren ließ nur den Schluss zu, dass Insiderwissen vorhanden war, um die perfekt organisierte und realisierte Tat zu ermöglichen. Die internen Ermittlungen, die wir unter Einbindung der Compliance-Beauftragten des Konzerns geführt hatten, waren u.a. darauf gerichtet, die Mitarbeitenden der Betriebsstätte zu entlasten und die mindestens fahrlässig begangenen Verursachungsbeiträge herauszuarbeiten. Durch die Ermittlungen und geführten Mitarbeiterinterviews war es schließlich möglich zu konstatieren, dass eine Tatbeteiligung der allermeisten Mitarbeitenden namentlich ausgeschlossen werden konnte.

Unsere Untersuchung ergab aber auch, dass bei zwei Mitarbeitenden erhebliche Fehlleistungen zutage traten, die einen signifikanten Einfluss auf das Gelingen der Tat hatten.

So konnten wir zwar keine vorsätzliche Tatbeteiligung der beiden Mitarbeitenden abschließend belegen, aber mindestens grobe Fahrlässigkeit dokumentieren, durch die die Tat erst möglich wurde.

In einem weiteren Fall, den wir betreut haben, ging es um einen Betrug im großen Stil zu Lasten eines Geschäftspartners. Unsere Aufgabe war es, den Chefjustiziar des geschädigten Unternehmens zu unterstützen und die Rechtsposition für anstehende zivilrechtliche Verfahren durch eine Verdichtung der Beweislage zu verbessern. Bereits nach akribischem Studium der Ermittlungsakten gelang es uns, genau hierfür Ansätze zu finden, um die Ermittlungen in und um das Unternehmen strategisch klug aufzusetzen.

Schon im ersten Aufschlag, in dem wir einen zentralen Zeugen ausfindig gemacht und befragt haben, haben wir für unseren Kunden einen erheblichen Mehrwert geschaffen und die Beweiskette deutlich verbessert.

ZAU: Wie sehen Sie die Zukunft Ihrer Arbeit? Was können Sie Unternehmen mitgeben, um im Fall der Fälle richtig zu reagieren?

Malberg: Für die Zukunft sehe ich durchaus leichte Veränderungen, was die Art der Ermittlungen angeht. Während früher der Schwerpunkt unserer Arbeit die heimliche Überwachung von Mitarbeitenden war, verschiebt sich der Fokus nicht zuletzt wegen des strengeren Datenschutzes und der gewünschten Unternehmenskultur.

Compliance-Fälle werden heute offener behandelt und nicht zuletzt durch Mitarbeiterinterviews transparenter gestaltet. Darüber hinaus gewinnt die Auswertung elektronischer Daten zum Nachweis von Straftaten spürbar an Bedeutung. Daher haben wir seit 2020 den Bereich IT-Forensik und E-Discovery so etabliert, dass wir spezielle Auswertungen von Computern, Handys, Tablets und Co. vornehmen können.

Insbesondere bei Verdacht auf konspirative Absprachen, Datendiebstahl oder Datenmissbrauch ist hier das Potenzial der Beweisgewinnung nicht zuletzt aufgrund unserer IT-forensischen Softwarelösungen phänomenal. Den Unternehmen sei aber gesagt, dass sie die Voraussetzungen zur Auswertung formaljuristisch durch Betriebsvereinbarungen, IT-Richtlinien, Regelungen im Arbeitsvertrag etc. schaffen müssen.

Deswegen empfehlen wir den Compliance-Verantwortlichen, Arbeitsrechtlern und Datenschützern, die Notwendigkeiten ex tunc zu berücksichtigen, um später im Verdachtsfall die Risiken der Beweisverwertung auf ein Minimum zu reduzieren und schnell reagieren zu können.

Ein weiterer Rat stammt aus dem Lateinischen: Respice finem. Unternehmen sollten immer ihr Handeln von Beginn an reflektieren. Und sollten die Verantwortlichen allein nicht in der Lage sein, aufgrund von Erfahrung und Weitsicht routiniert mit einem plötzlich aufgepoppten Compliance-Fall umgehen zu können, ist es empfehlenswert, mit denen zu sprechen, für die dieser Ausnahmezustand zum Tagesgeschäft gehört.

Wir bieten hier bei Bedarf immer ein unverbindliches Erstgespräch an.

ZAU: Vielen Dank für das Gespräch, Herr Malberg!

Das Interview führte Silvio Fricke (BVAU e.V.).



Wir gestalten
Arbeitsrecht.

**Bundesverband der Arbeitsrechtler
in Unternehmen e.V. (BVAU)**

VR Nr.: 333686 (VR/AG Mannheim)
Steuer-Nr.: 143/236/02493 (FA München)
Vertretungsberechtigter Vorstand § 26 BGB:
Alexander R. Zumkeller (Präsident)
Dr. Nelly Gerig (Vizepräsidentin)
Christian Stadtmüller (Vizepräsident)

www.bvau.de/impressum

Drächslstraße 4
81541 München

Tel.: 089 122 54 953
info@bvau.de

Strategische Partner:

Luther.

Kliemt.
ARBEITSRECHT

CMS
law·tax·future

wtw

FOLGEN SIE UNS:



www.bvau.de

**BV
AU**

Bundesverband
der Arbeitsrechtler
in Unternehmen