Guidelines for internal investigations

Two landmark decisions by the German Federal Labor Court

By Dr. Daniel Klösel and Dr. Thilo Mahnhold

Corruption, antitrust violations, fraud, data theft, theft of company assets, the betrayal of company secrets: The list of potential breaches of contract and, in most cases, criminal offenses in the workplace seems to be never-ending. The development of sophisticated compliance strategies to reduce the risk of such violations or mitigate their liabilities if the inevitable occurs is no longer unique to multinationals. Investigating potential cases of such criminal offenses is an important element of compliance strategies and – in some jurisdictions – is key to the reduction of administrative fines. But what if it is not the suspect but the investigator who is the actual source of potential liabilities? The EU General Data Protection Regulation (GDPR), which will come into force on May 25, 2018, is accompanied by administrative fines of up to 4% of the total annual worldwide turnover of a corporate group. In addition, individuals who suffer material or nonmaterial damage as a result of an infringement of the GDPR are entitled to compensation. Because data protection laws "hide what is hidden" and investigators "hate what is hidden", it stands to reason that there will be a conflict of interests. This makes it even more important to be aware of what investigators can do without violating data privacy laws and exposing the employer to risks such as administrative fines, damage claims and, in some instances, even criminal liability and the inadmissibility of evidence in court.

Employers should make sure that pursuing a private investigation is warranted.

The German Federal Labor Court has now issued guidance for internal investigations in two landmark decisions. Although they refer to the current German Data Protection Act, which will be replaced by the GDPR and a revised version of the German Data Protection Act on May 25, 2018, both decisions give some indication of how courts could rule in the future.

The German Federal Labor Court on private investigators

In its decision of June 29, 2017 (2 AZR 597/16), the German Federal Labor Court clarified the legal framework for the deployment of a private investigator. The previous instance, the Appellate Court of Baden-Württemberg, had decided that the deployment was not justified as the private investigator was only investigating a single breach of contract and not a criminal offense. In this case, the employer had received an e-mail (addressed to a customer) which mentioned that the employee was working for a competitor. The employer then consulted a private investigator who ultimately saw the employee working for the competitor. The Appellate Court of Baden-Württemberg came to the conclusion that the dismissal without notice was invalid as the evidence →

collected by the private investigator was inadmissible in court and therefore gross misconduct had not been proven.

The Federal Labor Court overruled this decision with unmistakable clarity. Although the decision of the Appellate Court of Baden-Württemberg was based on a strong argument – specifically, the wording of section 32 (1) Data Protection Act which only referred to criminal offenses - the Federal Labor Court ruled that there was no legal argument to interpret section 32 (1) Data Protection Act as the appellate court had. According to the Federal Labor Court, this interpretation would be in contravention of European law as it would not reasonably weigh the employee's right to privacy against the employer's interest. Furthermore, the court assumed that when section 32 Data Protection Act came into effect in 2009, it was not intended to modify the rulings of the Federal Labor Court, which had allowed covert investigations under certain conditions.

Against this background, the Federal Labor Court states that the (covert) surveillance of an employee by a private investigator is justified in general if the following rules are observed:

- there is a (simple) suspicion of gross misconduct, which does not necessarily have to be a criminal offense;
- the suspicion is based on specific facts (to be documented);
- no less intrusive investigative measures exist ("need to know");
- the investigative measure is reasonable (balance of interests).

It should be noted that German case law applies a strict interpretation of these principles. The steps that can be taken must be selected in accordance with the circumstances of the specific case. In particular the "need to know" principle must be closely observed. If, for example, a measure that is less intrusive than using a private investigator does not exist, the scope and length of the investigation must nevertheless be limited, for instance only a few hours a day and not every day. It is also crucial that a weighing of the respective interests has taken place.

The German Federal Labor Court on keylogger programs

The second decision of the German Federal Labor Court concerned keyloggers, which track all keyboard entries regardless of content, from business to online banking to personal correspondence. The employer in this case had decided to take this step after rumors that the employee in question was using his work computer for private business during working time. It was also reported to the employer that the employee had hastily closed "heavily pictured" windows on his computer in at least one case. In its decision of July 27, 2017 (2 AZR 681/16), the Federal Labor Court compared keylogging to covert video surveillance, which it had already deemed to be justified under strict requirements. The court also considered the aforementioned principles, which lay down the legal framework for the deployment of private investigators, video surveillance and other covert investigative measures. With regard to the case at hand, however, the court held that the use of a keylogger failed to meet even the first prerequisite of a simple suspicion of gross misconduct based on specific facts. Rumors and the one-time closing of a "heavily pictured" window are simply not sufficient. The court also highlights that keylogging is highly intrusive and contravenes the right to privacy as it provides a comprehensive and complete profile of computer use. The court explicitly states that the use of a keylogger in this specific case was excessive.

Even in light of this ruling, keylogging is not a no-go per se but is definitely a last resort with very limited areas of application. Its use must be clearly restricted in scope and time, and a careful weighing of interests must take place to ensure that its use is not excessive. The Federal Labor Court even gives an example for a less intrusive and permissible surveillance measure: Recording process data for use of the internet browser for a limited period. Evaluation of this kind of data on a random basis can be the preferred option for monitoring compliance with company policies on Internet use. This is good news from the employer's perspective, as the court clearly acknowledges the employer's interest in warranting compliance with internal policies and protecting company assets and IT systems.

Relevance under the GDPR

What will these landmark decisions be worth when the GDPR and the new German Data Protection Act come into force? In all relevant aspects, the new section 26 (1) of the German Data Protection Act is identical to section 32 (1) of the current Data Protection Act. The aforementioned decisions are based on an argumentation which allows the Federal Labor Court to continue to uphold both decisions even under the new laws. Even if →

it remains speculation, there is good reason to believe that this is the purpose of the two carefully drafted decisions. Nevertheless, there is one crucial and unanswered question that the German courts have to deal with under the GDPR and the Data Protection Act: According to article 13 (1) GDPR, the data subject, that is the employee, must be informed at the time that personal data is being obtained directly. It is irrelevant whether this entails video surveillance, private investigators, keylogging or GPS tracking if the data is obtained directly from the subject. If the employer or investigator is obliged to simultaneously notify the employee about these tools or measures, covert investigations would be impossible. In light of this, a recent decision by the European Court of Human Rights (ECHR, judgment of September 5, 2017, Bărbulescu v. Romania, no. 61496/08) is also noteworthy. It advises local courts to take into account that employees should be notified in advance of the possibility that their employer might take measures to monitor correspondence (in the case at hand, this was a messenger service). Although the ECHR has justified the use of covert investigative measures such as video surveillance in the past, this is another hurdle to be overcome if the German Federal Labor Court wants to uphold its two landmark decisions.

All in all, there is good reason to believe that the German Federal Labor Court will not be forced to alter its decisions. The ECHR ruling only influences the interpretation of German laws and German courts decide at their own discretion how to observe such rulings. Although the GDPR is binding, there is reason to assume that it does not aim to abolish reasonable covert investigative measures as this would otherwise be an overzealous interpretation of the right to privacy. In addition, article 14, which addresses duties to inform when data is not collected from the data subject, provides for an explicit exemption from the duty to inform if the information in question seriously impairs the achievement of data processing objectives. It is merely logical to apply this exemption to situations in which the data is obtained directly from the subject or employee (see Byers, NZA 2017, 1086, 1090).

What needs to be done?

Because the GDPR and the new Data Protection Act are currently driving many employers to revise their data protection policies, there is good reason to consider whether the mere possibility of specific (covert) investigative measures should be disclosed as part of a revised data protection concept. Policies on IT security, the use of telecommunications, data protection policies or compliance policies in a broader sense could be an appropriate place for these disclosures. For employers with works councils, master works agreements on data protection or individual works agreements regarding the tools that are subject to codetermination (for example video surveillance) could be another smart option when taking precautionary steps. In light of all the unknown factors, one thing is certain: The implementation of the GDPR is a challenge, not only for employers but also for the courts. ←

Dr. Thilo Mahnhold,
Rechtsanwalt, Partner, Fachanwalt für Arbeitsrecht,
JUSTEM Rechtsanwälte, Frankfurt/Main

t.mahnhold@justem.de

Dr. Daniel Klösel,
Rechtsanwalt, Associate, JUSTEM Rechtsanwälte,
Frankfurt/Main

d.kloesel@justem.de

www.justem.de