C/M/S/

Law.Tax

Lawyers on Whistleblower Protection and Internal Investigations

July 2020

Contents

Click on a country to go to that page

Lawyers on Whistleblower Protection and Internal Investigations

In October 2019, when the European Union approved the Whistleblower Protection Directive, many EU jurisdictions re-examined their internal investigations systems. At the same time, an open discussion arose in business communities in the EU and around the world on the crucial importance of having effective internal investigations and Whistleblower systems in place.

With much to say on these topics, CMS joined the discussion.

It is universally agreed that the absence of proper protection and accessible disclosure channels for businesses is dangerous to their interests. It is also understood that Whistleblowers do not damage companies, but rather strengthen and protect them from disastrous prosecutions and embarrassing news headlines. Internal investigations can be arduous and unpleasant, but they are a necessary part of a company's maintenance. As there is no single internal-investigation strategy that applies to all companies and jurisdictions, the experts, authors and speakers who have compiled this manual offer a variety of solutions, sharing their hands-on experience and insights with material that reflects the diversity of the business world's many markets and the unique traditions and legislative environment of each.

Every year the CMS Employment Group organises a global webinar series. This year, marking our tenth jubilee, the series explored the topic of internal investigations and Whistleblowing. Conducted between November 2019 and May 2020, the series – organised by *Katarzyna Dulewicz*, employment partner at CMS Poland and CEE Head of Employment at CMS CMNO, and her team covered 24 jurisdictions and educated thousands of people on the key points of conducting a successful internal investigation in a way that protects both employers and employees.

Articles and podcasts based on the webinars were published after the online presentations, which we would like to share with you in this volume. We thank those of you who attended the sessions and the many participants who provided valuable feedback.

And to all the readers of this manual, we wish you good luck in applying these principles and strategies in your workplaces.

For more information on how to implement internal-investigations solutions that are best suited to your company, market and jurisdiction, do not hesitate to contact us directly or visit the insights section *Whistleblower Protection* on our website.

Caroline Froger-Michon
Partner, CMS France
Co-Head of Employment Group
E caroline.froger-michon@cms-fl.com

Chris Jordan
Partner, CMS Germany
Co-Head of Employment Group
E christopher.jordan@cms-hs.com

Austria

Click to listen to the webinar recording
Published 20 December 2019

Experts recommend businesses implement internal investigative systems ahead of whistleblower law

Outline

With Austria expected to pass a whistleblower protection law no later than December 2021, legal experts here are recommending that businesses carefully monitor the legal situation and start putting internal investigative systems in place to prevent, detect and respond to reports of misconduct.

Although Austria is now obliged to pass a whistleblower protection law within the next two years in line with a recently passed EU Directive (2019/1937), Austrian courts already preside over misconduct cases as they pertain to violations of Austrian labour law. One reason for this may also be the new sensitivity in HR-cases for data protection issues.

As there is an increasing sensitivity as to whether documentary evidence is obtained in compliance with GDPR and other regulations, businesses are advised to create systems that allow for comprehensive *ad hoc* investigations.

Ad hoc investigations

The first thing Austria-based businesses must realise is that they are legally bound to respond to any and all allegations of misconduct as part of their obligation to create a safe and secure working environment for employees.

How should a business respond if an employee reports misconduct? According to the EU Directive, if no mandatory reporting or investigative systems are in place in the firm, the whistleblower will be compelled to appeal to an outside authority (e.g. police, ombudsman, prosecutors) or might even go public with the allegation as a last resort. In these cases, businesses, at least those which are obliged to establish such systems under the EU Directive, must do everything in their power to protect these whistleblowers, no matter the substance of the allegation.

If a business has an internal system in place, management should respond to an allegation by interviewing the personnel involved. Above all, the interview process should be confidential, both to protect the privacy of individuals (particularly in cases were the allegations are unfounded) and the integrity of the inquiry.

Once interviews are under way, companies will almost always have interactions with their Works Councils, which are in-house employee committees that represent worker rights and usually exist in Austrian businesses with five employees or more. During an investigation, a Works Council representative will likely demand access to all information on the inquiry and participation in any employee interviews.

Managing directors should be aware that the rights of council reps during an ongoing *ad hoc* investigation are limited. Although these councils have the right to give input on general policies concerning a firm's work environment, they have no general legal right to represent individual staff members without their consent or obtain any information.

In the interview process, businesses should also be aware that the storing of digital records and transcripts has GDPR implications. Data protection officers should be consulted about how evidence is processed.

Employees under internal investigation

If an employee is under internal investigation, a business faces the thorny question of what do with the individual before the inquiry is

concluded. The decision to terminate or dismiss a person should be well-considered and not taken prematurely, given the high level of protection against unfair dismissal. Yet it is unwise to allow someone under investigation to remain in their position with the power to manipulate evidence or intimidate witnesses.

Under Austrian labour law, employees enjoy the "right to work" only in exceptional cases. Hence, businesses are rarely obliged to keep the subject of an investigation in the workplace as long as the staff member is being paid. As a result, many businesses solve the problem of what to do with a staff member under investigation by sending this employees on fully paid "garden leave", where he is instructed to go home until further notice and to be on call for questioning.

Investigative document searches

Aside from interviews, internal systems can include other investigative techniques, such as the hiring of private detectives, which has been accepted by courts in past misconduct cases so long as investigators do not overtly violate the privacy rights of a worker. For example, justices frown upon investigators employing round-the-clock surveillance.

Phones, laptops and email accounts of employees can also be sources of evidence. Both Austrian labour law and the GDPR allow for searches of professional email accounts and work-related documents, although businesses are advised to warn employees of the possibility of such searches when they are hired or seal agreements with Works Councils.

Austrian courts have in the past even allowed searches of private emails of employees, but only under controlled circumstances, such as searches using key words pertinent to a case.

Prevention

Experts advise, however, that the best method of dealing with misconduct is to prevent it from happening in the first place. Firms are encouraged to conduct risk analyses to determine those areas of the business most vulnerable to misconduct and to put policies in place to discourage it.

Businesses can also install whistleblower hotlines, assign personnel to act as reporting officers for allegations of misconduct and draft codes of ethical conduct. In terms of both conduct and reporting, management should show a firm commitment to the process. Leadership can set a tone that infuses and inspires the entire organisation.

Also, periodic training sessions on acceptable behaviour can make a company's standards crystal clear to all employees.

When putting any pro-active system in place, managing directors are encouraged (and sometimes obliged) to cooperate with their Works Councils, and such cooperation can only have a positive influence on corporate culture.

Companies, however, should be aware of the national whistleblower legislation that is expected to come down in the next two years. In the meantime, when crafting whistleblower policies, businesses are encouraged to study the recently issued EU Directive.

If you have further questions, contact your regular CMS source or local CMS experts:

Daniela Krömer
Of Counsel, CMS Austria
E daniela.kroemer@cms-rrh.com

Miriam Mitschka
Senior Associate, CMS Austria
E miriam.mitschka@cms-rrh.com

Belgium

Click to listen to the webinar recording
Published 24 February 2020

Case law and regulations governing Belgian internal investigations

In Belgium, the laws surrounding internal investigations are not conclusive, and Belgian companies planning to draw up procedures for in-house inquiries are urged to consider both regulations and case law. Belgian legal theory may be clear, but companies must consider the practical world of court precedent when developing policies.

In short, developing internal investigation and whistleblower policies within a Belgian company centres around this question: if you suspect that an employee is guilty of corruption (e.g. sharing information with competitors, falsifying a timesheet), what can your company do to investigate and if necessary issue corrective measures that are an appropriate response and consistent with Belgian regulations and case law?

Below is a high-level summary of the most important legal principles that could apply in case of an internal HR investigation, and our general recommendations:

First of all, it must be remembered that no laws exist in Belgium that oblige companies to establish a whistleblowing or internal compliance programme. Establishing such policies, however, is recommended to combat internal wrongdoing and to allow a company to respond to any corrupt activities that might be taking place among its ranks.

A good first step for any company implementing its own whistleblowing procedures is to create an Internal Compliance Programme. In addition to appointing a manager to implement this programme, internal compliance should also include the drafting of clear guidelines that set down the company's policies and defines both acceptable and unacceptable behaviour.

The employer must ensure that all employees are aware of these guidelines by, for example, asking personnel to sign a copy of these policies.

To assist in employee education and to create a positive corporate culture, businesses are also encouraged to conduct regular trainings on good conduct in the workplace and the consequences of non-compliance. To ensure that the legal ramifications of these issues are clear to all, it may be advisable to have either an in-house counsel or an outside lawyer participate in the trainings.

Setting up whistleblowing procedures in a company is complicated by the fact that no legal framework for this exists in Belgium other than the 2019 EU Whistleblowing Directive. This legal vacuum, however, does give businesses the freedom to choose the policies (e.g. should reports be filed anonymously? will the company offer immunity in exchange for cooperation?) that management considers most efficient.

Particular attention should be paid to the following two points:

1. all internal investigation procedures must comply with data-privacy regulations as set down by Belgian law and the EU's GDPR;
2. companies cannot enact policies claiming to immunise whistleblowers from dismissal.

According to Belgian law, companies are not obliged to inform either whistleblowers or employees about an investigation nor are they required to alert works councils or representative bodies. Nonetheless, specific information obligations regarding the employees could arise depending upon the investigative measures (see below).

Generally, we advise that all internal investigations include employee interviews in the appropriate official language (Dutch or French depending upon the place of work). It is recommended that minutes be taken of each interview, which the employee should be asked to review and sign. Furthermore, companies are advised to allow employees to seek the support of union representatives during the interview process. Having lawyers present during interviews is not always advisable since some employees might view this as intimidation.

In principle, interviews cannot be recorded in audio or visual form unless the employee gives his explicit permission. In addition, companies are advised to seek the approval of employees before searching their workstations (e.g. offices, desks, company vehicles) since these areas may contain personal articles that would fall under either data-protection or Belgian privacy laws. When asking permission to conduct a search, the company should specify a clear goal, detailing what it is looking for and why.

When searching laptops and mobile phones, a raft of Belgian regulations and case law apply, such as CBA 81, Electronic Communications Act and Article 314bis of the Criminal Code. Given the legal sensitivity of these searches, we advise that companies strictly comply with rules contained in the regulations described above.

In terms of other investigation techniques, surveillance cameras can be used in the work place. Again, strict formalities apply for camera surveillance to be legal. For example, in line with labour and data-protection regulations, employees should, among other details, be informed of their presence, and the cameras should not be placed in areas like employee lunchrooms where work is not conducted.

Companies should indeed protect themselves from the possibility of having the results of their internal probe overturned later in the courts.

Yet even if mistakes were made in an internal investigation and evidence was collected contrary to regulations, all is not necessarily lost. According to the "Antigoon" precedent in case law, illegally obtained evidence may be accepted in court if it doesn't obstruct the rights of the accused to a fair trial, if the evidence is reliable, and if there is no violation of a formal requirement sanctioned with nullity.

As for employee rights, are workers entitled to withhold cooperation in an internal investigation? Here a fine balance must be struck. According to Belgian law, employees have a "loyalty obligation" that could serve as a basis for employers to request collaboration. However, employees as citizens have the right to reject any request that may lead to self-incrimination.

Generally speaking, employers can request the cooperation of their workers so long as their investigation procedures are not invasive and respect employee rights.

Since former workers are not bound by Belgian law to cooperate with internal investigations, employers could consider including a post-employment cooperation obligation in all employee contracts.

When an investigation has been concluded, Belgian companies have various options at their disposal for meting out sanctions. For relatively minor infractions, companies could consider giving workers oral warnings, written warnings or fines (sanctions to be included in the work rules of the company and to be imposed on the first working day following the infringement or the conclusion of the investigation).

For more serious offences, a termination of the employment contract can be considered. Termination can come after a notice period has been performed or with immediate effect in which a cash payment compensates for the absence of notice.

In cases of termination, employers are not obliged by law to consider a rebuttal argument from an employee, although giving the employee a forum to respond is recommended as protection against any subsequent court action.

In more complex situations, employers can try to reach termination settlements.

In case of serious misconduct such as theft, fraud or corporate espionage, companies can terminate an employee immediately, as stated in Article 35 on the Belgian law overseeing employment contracts.

In this case, termination must take place within a three-workday period following the date on which the company has sufficient knowledge of the facts, and in instances of fraud or serious negligence, the fired employee may be liable for damages.

In conclusion, in order to ensure its protection in case of employee misconduct, a company is advised to implement appropriate measures and to act sooner rather than later.

For more information on internal investigations in Belgium, contact your regular CMS advisor or local CMS experts:

Katrien Leijnen
Senior Associate, CMS Belgium
E katrien.leijnen@cms-db.com

Géraldine Lemaire
Senior Associate, CMS Belgium
E geraldine.lemaire@cms-db.com

Bulgaria

Click to listen to the webinar recording
Published 24 February 2020

Bulgarian internal investigations regulated by collection of laws and best practices until passage of whistleblower act before end of 2021

No single law governs how an internal corporate investigation of corruption or wrongdoing can be conducted in Bulgaria. Yet when faced with allegations of wrongdoing in its ranks, a Bulgarian-based company has options at its disposal through various regulations, some case-law and the best practices currently being employed.

What exactly are these options?

Stage one of the process is the report, originating from a whistleblower or through an internal audit, that a wrongdoing has taken place. In certain circumstances, Bulgarian law requires that a company take immediate action.

For example, according to Bulgaria's *Protection Against Discrimination Act*, if an employee is being harassed or bullied in the workplace, the company must implement measures immediately to stop this harassment and investigate the case.

This may entail separating the harassed employee from his alleged harasser. Or it could require that the suspect be put on leave while an investigation is conducted.

But it should be noted that suspending an employee from work can be problematic under Bulgarian law, which does not explicitly address this issue. By law, employees can only be suspended if they arrive at the workplace in a "state" that does not allow them to complete their duties (e.g. under the influence of drugs or alcohol). In this case, they are suspended as long as they are unable to work and during this period they are not paid.

Although "garden leave" – suspending an employee while an investigation is ongoing – is not recognised in Bulgaria, it is accepted by many foreign jurisdictions where Bulgarian multinational companies are based. Hence, a multinational may need to exercise "garden leave" if this is recognised in the country where the company is based and reflects in its internal policies.

But in this case, these employees must be paid while they are not in the office, mainly to protect the Bulgarian company from any future court action.

To avoid other legal risks, in cases of garden leave, companies must ensure that there are no personal items belonging to the suspended employee left in on the worksite. If this occurs, this could be interpreted as denying an employee access to private property and – crucially – personal data, if the property in question includes a laptop, tablet or storage drive.

In terms of the actual investigation, many companies have whistleblowing procedures in place that employees can use to report wrongdoing or harassment. But whether or not a company has internal policies in place to report grievances, a firm is still obliged to respond if wrongdoing is uncovered.

Clearly, procedures can vary from company to company, but can include the following processes: a careful collection of evidence through interviews, reviews of business emails and company messaging services, an inspection of company phone records and computer usage,

inspections of CCTV video (if available) and physical searches of the working area.

Of these investigation techniques, interviews are the most common and effective. To hold interviews, companies usually create an interview commission, which should be made up of one or more senior managers, an HR official and a legal counsel. Depending on the alleged wrongdoings, it may be advisable to add the company compliance officer or the line manager.

The number of staff to be interviewed depends on the case. Minor offences may require the interview of only one person: namely, the accused. More serious offences, particularly those that could incur legal liability to the company, may require a more exhaustive round of interviews to bring all the facts to light.

When a suspect is being interviewed, he does not possess the right to have legal representation present, although a company – in the spirit of fairness and to protect itself from future court challenges – may allow it. Representative bodies, such as trade unions or works councils, need not be officially informed that the interviews will take place. But again, a company may choose to do so.

During interviews, minutes of the proceedings should be taken, either by a stenographer or a committee member. After each interview, these notes should be reviewed by commission members and the interviewees, and signed by all involved to certify their accuracy.

Interviewees may choose not to sit before a commission, but answer questions in writing. This is an acceptable practice and at times preferable, since written responses may be more revealing.

Once the interviews are completed, the commission should draft and release a report summarising the proceedings and analysing the evidence it collected.

In terms of email and text-messaging scans, any data searches of electronic devices and computers must comply with the EU's GDPR, Bulgaria's data protection law and Bulgarian and EU human rights legislation. In terms of GDPR compliance, companies should ensure its digital search procedures are completely transparent and focused only on data that is directly related to the investigation. Every effort should be made to protect the privacy of the data scanned and collected.

Bulgaria's data protection act states that companies should have GDPR-compliant internal investigation procedures in place for data collection and that employees should be well aware of these processes. Furthermore, companies must establish clear guidelines regarding any private use of company email and messaging systems, which include the types of communications that may be monitored by the company.

In short, a balance must be struck: the company should establish policies that allow for an investigation of its communication systems, but also exhibit GDPR-compliant respect for personal privacy. A 2017 case adjudicated by the European Court of Human Rights explored the legal implications of data collection in the Romanian workplace. This decision can be studied in detail when drafting internal data-collection rules.

After an investigation is complete, it may be necessary to report findings to outside sources. Multinational companies may need to report these findings to law enforcement or judicial authorities in the countries where their head offices are located (e.g. the US Justice Department).

If the investigation proves that an employee was guilty of a disciplinary wrongdoing, it may want to hand down disciplinary sanctions, such as a reprimand, warning of dismissal or dismissal.

Whatever disciplinary penalty an employer issues, it must be handed down no more than two months after learning of the breach and no more than one year after the breach has been committed.

In addition, companies should then look at ways to prevent similar abuses from occurring in the future, and implement all necessary reforms. In cases of harassment and bullying, this could include adopting a code of conduct and staff training that counsels against such behaviour. Reforms could also include enhanced whistleblowing systems, employee communication channels, and in-house investigation procedures that can better identify wrongdoing and arrive at the facts faster.

Bulgaria's legislative vacuum surrounding internal investigations will not last indefinitely. As a result of the 2019 EU Whistleblowing Directive, Bulgaria is required to adopt its own national whistleblowing legislation no later than December 2021. The EU's interest in protecting whistleblowers is borne out by the economic costs of corruption, which – within the EU's public procurement sector – results in losses of between EUR 5.8bn and EUR 9.6bn annually.

Bulgarian companies that are reviewing, revising or drafting whistleblowing and internal investigation procedures are encouraged to study this directive and insure that all their internal policies comply, since these regulations will soon be reflected in the law of the land.

For more information on internal investigations in Bulgaria and the upcoming whistleblower legislation, contact your regular CMS advisor or local CMS experts

Iveta Manolova
Senior Associate, CMS Bulgaria
E iveta.manolova@cms-cmno.com

Maria Harizanova
Associate, CMS Bulgaria
E maria.harizanova@cms-rrh.com

China

Click to listen to the webinar recording
Published 26 May 2020

China boasts strong tradition in conducting internal investigations

The Chinese economy may be young and growing, but its business community already boasts an established and sophisticated tradition for conducting internal investigations.

These traditions may be rooted in the international character of its corporate culture: the fact that many Chinese corporations conduct business with international partners based in countries that have their own systems for internal investigations and Whistleblowing.

Whatever the reason, internal investigations in Chinese companies are used in response to the same types of misconduct that occur in other jurisdictions: reports of breaches of national laws and regulations (e.g. fraud and bribery), violations of company polices and rules (e.g. breaching trade secrets), and breaking internal policies established to protect employee rights.

And like in other countries, Chinese companies usually become aware of a wrongdoing through the following ways: a report from a Whistleblower inside or outside of the firm, an internal audit, or as a result of a random discovery.

In regard to Whistleblowing: although some countries require firms to set up Whistleblower protocols, China has no such requirement. Nevertheless, many companies operating in China have recognised the benefits of having such reporting systems in place and have created channels (such as a hotline or an e-mail account) for employees, managers or clients to make a report, anonymously or not. Some companies consider these reporting systems so valuable, they have set up anonymous reporting systems that focus on specific wrongdoings, such as bribery.

Initiating an investigation

When a company receives a report of possible misconduct and has policies in place to respond with an in-house inquiry, it is advisable to proceed in the following way. Firstly, the company's management should quickly decide whether the report is credible and the charge warrants an internal investigation (i.e. does the allegation directly implicate or involve the company). A company may well decide that the evidence is too weak to warrant an investigation or that the allegations are not applicable to its business activities.

If the decision is made to conduct an investigation, the company's management will select an official (often from the company's HR or legal departments) to oversee the inquiry process. At this time, the firm will also determine whether it should also seek the help of outside experts to conduct the investigation. Normally, involving the company's trade union is not necessary. Also note that if a company decides that it lacks the in-house expertise to conduct a proper investigation, responsibility for the inquiry can be contracted to outside experts, such as a law firm or chartered accountancy with direct experience in these matters.

Once an investigation official is appointed, he should draft a plan for probing the allegations, which include the individuals to be interviewed, the exact topic to be investigated, the timeline for conducting the inquiry and whether immediate action is necessary to prevent the alleged misconduct from recurring or to stop further damage, etc.

A company and its investigation team will have to make quick decisions on protecting the integrity of the investigation, particularly during

the interview process. In short, to prevent witnesses from being harassed and evidence from being manipulated, a company may decide to place the employee who is the target of the investigation on paid furlough (i.e. "garden leave") to remove him from the workplace and separate him from other workers until the investigation is concluded.

Once the policies and procedures for the investigation have been established, one important question remains: what are the company's limitations when conducting an inquiry? In terms of collecting evidence against individuals, companies in China are legally permitted to investigate employees suspected of wrongdoing and can expand their queries to include employees who may have evidence but are not directly involved in the alleged misconduct.

A company has a number of techniques at its disposal that it can employ to collect evidence. These include the physical inspection of files and documents; examining pertinent electronic communications, such as email and mobile phone text messages; checking company computers and smartphones for files pertinent to the investigation; gathering information from any third parties (e.g. suppliers, costumers) and interviewing employees.

Companies, however, also have responsibilities to their employees. When conducting an investigation, a company must not violate – through its searches, interviews and treatment – the personal rights of any employee. The protections that must be safeguarded include an employee's right to personal privacy, to freedom and to data protection.

As for personal freedom, employers cannot physically restrain or search an employee. During interviews, questions should be delivered in a professional manner with the objective of gaining clarity of a given event. Employees should not be intimidated or insulted during this process.

In regard to processing employee data, the investigation must follow Chinese data-protection laws to the letter in order to protect itself from court action that could stem from any data-privacy infringements.

In addition, an investigation must limit its physical and online searches to company property, and cannot search the personal belongings (e.g. personal papers) or private data (i.e. personal files or communications, such as personal emails) of an employee without the individual's express consent.

In order to make sure an investigation follows data protection rules, investigators should take special care to identify the hardware and files that are pertinent to the query and limit their searches to company property. When it comes to company-owned phones and laptops, firms have a legal right to search these devices without employee consent. To gain access to this equipment, investigators can ask employees to surrender these devices, and if deemed necessary, investigators can conduct searches of these devices without the employee's direct knowledge.

If a company asks an employee to surrender a device, such as a company phone, and the employee refuses on the grounds that it contains personal information, the company can instruct the employee to delete this data or copy it to another personal device before surrendering the phone. The employee has no legal grounds to withhold such a device if a company requests its return.

Furthermore, to protect itself from such personal privacy issues, companies can establish a policy, communicated to all employees upon their hiring, which prohibits the use of company devices for personal use and for storing personal private information. By establishing this policy, the legal risk of infringing employee privacy and data-protection rights can be reduced when a company conducts searches of company devices. Such a policy, however, does not permit a company to ignore the employee's privacy and data-protection rights. When inspecting a company device, if investigators notice the existence of any private information in the device, the investigators must avoid accessing, copying, using and disclosing any of this private data.

Interviews

One of the most important tools for collecting evidence is interviews with employees, which raises the question: is an employee obliged to participate in interviews? The answer is yes. In addition, according to Chinese laws, a company does not need to forewarn an employee about an interview and can question employees at any time during working hours.

If the questions posed by investigators concern company matters, the employee is obliged to answer completely and truthfully.

It should be noted that given the importance of the interview process in establishing the veracity

of an allegation, investigators should first conduct document and data searches and collect detailed physical evidence before interviewing the suspect and any witnesses. The interview process can only be revealing if the investigators have fully prepared themselves and have devised lines of questioning with precise objectives in mind.

In terms of making official records of interviews, Chinese law does not prohibit investigators from making either audio or visual recordings. Also, employee consent or even awareness of these audio-visual recordings is not necessary. But because an electronic recording of an employee's interview represents a form of electronic data evidence, the authenticity and legality of the recording could be more easily challenged in court. Hence, it is recommended that a written transcript or report of every interview be created, which interviewees should verify and sign. In this way, a company can then use the signed transcript as evidence supporting any electronic recordings that have been made.

Role of trade unions

Another question is the role of trade unions in internal investigations. Chinese law does not require companies to inform or involve trade unions during internal investigations with one exception: if an inquiry directly concerns a work-related injury or issues related to employee health and hygiene.

After an investigation is completed, if an employee has been found guilty of misconduct and the company decides to respond with immediate dismissal, this decision must be communicated to the trade union.

Conclusion of an investigation

In addition, once an investigation is concluded, the investigators must then compile all the findings, analyse these facts and determine whether there is sufficient evidence to prove the allegation. If the evidence reveals that a company employee is guilty of misconduct (i.e. that he violated company regulations or the law), the investigation team must then recommend a response.

If the misconduct is deemed to be minor, the employee may be issued a warning. For more serious cases, a demotion may be called for. And in extreme cases, the employee may need to be dismissed. Such disciplinary measures must be determined and carried out according to the company's established rules and regulations.

If the misconduct carries civil liability, the employee can be asked to pay damages if the misconduct resulted in tangible losses to the company. But to seek damages from an employee, the company must have direct evidence linking the misconduct to the damages and evidence to prove the amount of damages requested.

If the investigation uncovers evidence of a crime, the company, of course, is obliged to report the employee to Chinese law enforcement. However, there is no statutory law that specifies a penalty for failure to report an employee to authorities who is deemed guilty of a crime. Hence, companies should use their own discretion, based on the severity of the crime and the evidence gathered, whether to go to authorities with the finding of an internal investigation.

Lastly, investigators are highly advised to compile a detailed report of the investigation, the evidence collected, and the judgment rendered in case the findings are later challenged in any way.

For more information on conducting internal investigations in China, contact your regular CMS advisor or local CMS experts:

Jeanette Yu
Partner, CMS China
E jeanette.yu@cmslegal.cn

Sophy Wang
Associate, CMS China
E sophy.wang@cmslegal.cn

Croatia

Click to listen to the webinar recording
Published 15 April 2020

Internal investigations in Croatia must not violate employee "dignity" and personal data protections

With the passage of the Croatian Act on the Protection of Persons Reporting Irregularities, which came into force before the 2019 release of the EU's Whistleblowing Directive, Croatia established itself as a pioneer in corporate internal investigations – or at least it might look like that at first sight.

But this law, based on early proposals for the EU's Whistleblowing Directive, has been criticised for being vague in key areas, which has created some uncertainty surrounding the legal foundations for conducting internal investigations in the Croatian business community. Furthermore, when conducting in-house inquiries, companies must ensure that they do not violate national laws protecting employee "dignity" and personal data.

Employee dignity

Croatia protects the "dignity" of employees by virtue of the law. Applicable to all companies employing 20 employees or more, the central feature of these regulations is the appointment of an official authorised to receive and act on alleged violations of workers' dignity. This official – together with the employer himself – is obliged to investigate all allegations within eight days after receiving evidence of violation of employee dignity and must implement all "necessary and appropriate measures" to stop further harassment, particularly if it is workplace harassment of a sexual or bullying nature.

Necessary and appropriate measures

An employer is under no obligation to consult the union or works council when appointing an official for protection of employee dignity.

The employer, however, is obliged to move expeditiously to ensure a safe and secure working environment, which, depending on each individual case, may entail – in cases of harassment – changing the work schedule and hours of employees in order to separate the victim and the alleged perpetrator while the investigation is ongoing. A position change of this kind is unlikely to include a demotion where an employee receives a lower salary since Croatian law requires employee consent before this can occur.

Croatian law affords employees other rights that an employer should keep in mind. After information to an employer that his rights have been violated, a Croatian employee can also file a complaint with the courts if he believes that his employer is not doing enough to stop workplace harassment.

Called the "Eight Plus Eight" rule, an employee has eight days to petition for a court action should a company fail to act within the eight-day deadline after a complaint has been filed.

An employee can also refuse to continue work until protection is guaranteed provided that he asks for protection from the competent court within the next eight days. He is also entitled to be paid while off the job. If – in the end – it is proven that the misconduct charge was unfounded, the company is entitled to be reimbursed with salaries paid to these employees, and any accompanying interests.

Employee protections

As in all EU countries, Croatian workers enjoy the protection of their personal data. Any

internal investigation launched by a company must ensure the confidentiality of employee information. Companies can be fined between EUR 4,133 and EUR 8,000 and responsible individuals within the companies between EUR 533 and EUR 800 for violations.

As for the individuals filing misconduct allegations, the Croatian Act on the Protection of Persons Reporting Irregularities offers Whistleblowers certain safeguards although critics argue that this law – drafted before the passage of the EU's 2019 Whistleblowing directive – is vague on key points.

Although the law applies to employers in both the public and private sector, it is not clear how the regulations apply to smaller firms of under 50 people. Although not obliged to do so by law, companies of less than 50 people may choose to have an internal investigation system, but the law is unclear on whether or not they must adhere to the Act.

It is also not clear how the law applies to large foreign-owned companies whose local offices may have less than 50 employees.

The law does regulate a reporting chain for corporate misconduct: internal reporting (within the company), external reporting (to outside authorities) and public disclosure (through media reporting).

According to the law, a company employing 50 or more employees must draft and implement procedures for receiving allegations of misconduct and responding to them. It must also designate a commissioner and a deputy who are responsible for receiving these reports and leading any investigations.

This may be problematic for some companies since – according to Croatian labour law – employees cannot be forced into accepting this position. Hence, filling this post is not always easy, but if a company fails to do so, it is liable to receive penalties from the competent authorities.

Once the commissioner's position is filled, he and his deputy are responsible for receiving reports of misconduct, examining the cases, taking immediate action to protect the Whistleblower (i.e. the person filing the report), and referring the charge to the competent authorities should the company prove unable to resolve the issue internally.

In this regard, the law also contains a notable inconsistency. According to the Act, a company cannot interfere with the work of its duly appointed investigations commissioner. Yet if a commissioner fails to respond to a report in a timely and responsible manner, the company is liable.

Although the law encourages misconduct reports to be resolved internally, external reporting channels, such as the ombudsman, or public exposure (i.e. direct appeals to media) is recommended if the issue at hand concerns a threat to health, life and safety; if there is a threat of significant damage; if there is a risk that evidence may be destroyed; if the company in question has no working internal-reporting system; if the Whistleblower is no longer affiliated with the company he intends to file a report about; or if irregularities and concerns exist regarding the company's internal reporting system.

The problems with these regulations are obvious. Although Croatian law urges Whistleblowers to act in good faith, providing individuals with a legal license to take misconduct charges to the media creates the risk of disgruntled employees using this opportunity to bring false charges against a company in the press.

Non-compliance with this Act can lead to fines of between EUR 133 and EUR 6,666 for employers; between EUR 133 and EUR 4,000 for competent officials within the companies; between EUR 400 and EUR 4,000 for malicious Whistleblowers issuing false reports; and between EUR 400 and EUR 4,000 for other competent persons and their deputies.

Conducting internal Investigations

If a company receives a report or uncovers evidence of misconduct, it is obliged to investigate. When investigating its employees, companies must take care when managing personal data. Under Croatian law, employee personal data can only be processed when there is a valid reason to do so. To this end, companies of 20 employees and larger are required to draft employment by-laws that specify exactly the employee data that will be processed in this situation, particularly in regard to sharing this data with third parties. Companies with 20 people or more are also required to appoint a data protection commissioner, who must be privy to (and in some situations oversee) any personal data collection connected to an investigation.

In addition, no piece of employee personal data can be processed without the permission of the company's works council provided that the employer has adopted the employment bylaw regulating the processing of employee personal data and that the works council has granted its consent. Note that the works council will not have to give its prior consent for each specific processing activity, which is an additional reason for drafting the employment bylaw in as much detail as possible.

In terms of the investigation itself, it can be conducted only by the employer or a person specifically authorised by the employer. If the investigation is conducted by a third party, the employer should issue specific authorisation to perform data processing activities to an external provider prior to the commencement of the audit or investigation.

It is extremely important to determine if there is sufficient legal basis to conduct an investigation (i.e. to process employee data), such as indications of harassment, the breach of a non-compete clause, commission of a crime or the disclosure of trade secrets. And to determine whether the basis for the inquiry is legitimate, the purpose of the investigation should be clearly identified and it should be considered if there are alternatives to the processing of employee data. In short, it should be judged whether the allegations brought forward entail sufficient risk to the company's legitimate interests to warrant the processing of employee data.

Not only should a company conduct a "legitimate interest assessment", this test needs to be clearly documented for later reference.

Performing this assessment will help define the detailed purpose and objective of the investigation, which from a legal point of view must be followed at all costs.

With a clear purpose established, an investigation strategy that is the least intrusive regarding the processing of employee data needs to be determined. What investigation techniques can be employed? Options include conducting interviews of employees, including both the target of the investigation and witnesses, inspecting employee communications, such as scanning emails, etc.

From a data protection point of view, the interview process is the least intrusive, if conducted lawfully. This means that interviewers must only ask questions directly pertinent to the objective of the investigation; and interviews themselves cannot be recorded either by audio or video unless the interview subjects give their explicit consent.

Scanning emails is more problematic from a data protection point of view. Employers can only inspect business email accounts and where possible should restrict their searches to email logs (i.e. when and to whom emails were sent). Only if the email log raises high suspicions that inappropriate communications took place can an employer read the "context" of the email.

Lastly, for companies that are part of international corporate groups, rules apply to the transfer of investigation data to other offices outside of Croatia. Such transfers are not forbidden, but when doing so all EU General Data Protection Regulation (GDPR) tenets must be followed.

Also note that companies can protect themselves by implementing bylaws in areas in which misconduct most often occurs. To protect trade secrets, ensure that all sensitive business information is labeled as such in a proper way and that any intelligence is closely guarded. Employment contracts should include sharply defined non-compete clauses and all obligations associated with these clauses must be fulfilled. And companies must establish a definite time period for the storage of employee personal data (e.g. archived emails) and ensure that data is not retained after this deadline.

In conclusion, despite vagaries in the current legislation, Croatia-based companies can employ internal investigations to protect themselves against risks. But care must be taken when drafting bylaws for these procedures and carrying them out.

For more information on conducting internal investigations in Croatia, contact your regular CMS advisor or local CMS experts:

Ana-Marija Skoko
Partner, CMS Croatia
E ana-marija.skoko@bmslegal.hr

Mia Kalajdžić
Associate, CMS Croatia
E mia.kalajdzic@bmslegal.hr

Czech Republic

Click to listen to the webinar recording
Published 25 May 2020

Czech business internal investigations

Like some countries in Europe, the Czech Republic has no laws that directly regulate corporate internal investigations.

Instead, other laws indirectly but profoundly impact how a Czech company should conduct an in-house inquiry, such as the Labour Code and laws governing data protection. Of these laws, data protection regulations, centred around the EU's General Data Protection Regulation (GDPR), is arguably the most important.

According to Jakub Kabát, an Associate in CMS Prague, before drafting any internal investigation policies, a company is advised to fully understand how Czech data and employees' privacy protection regulations might impact such a procedure. An internal investigation, no matter the alleged crime, will always affect the privacy of one or more individuals.

This fact, states CMS Prague's Kabát, is the central conflict at the heart of conducting corporate investigations in the Czech Republic: balancing the need to protect the personal privacy of individuals with a company's interest in protecting its property and assets while at the same time complying with all aspects of the Czech Labour Code and data privacy laws.

To this end, the company should perform a "balancing test" and determine whether the company's interest in, for example, protection of its property overrides an employee's right to privacy. If the test reveals that the threat to the company demands the collection of evidence, the investigation can proceed. (This test, however, should be recorded since the justification for the investigation and the decision-making leading to its creation may be challenged later).

In terms of worker rights, the Labour Code also provides a wide assortment of protections to employees (i.e. personnel who have employment contracts with their firms). Labour law, however, does afford the same recognition to company executives, who usually are not attached to their companies via employment agreements, although executives enjoy the same privacy and data-protection rights as any other person.

In terms of internal investigations, executives and employees may possess different legal rights, but experts recommend that companies use the same investigative methods no matter the suspect.

Generally, all investigations include the following procedures: an inspection of any electronic information or messaging pertaining to the alleged misconduct (e.g. emails, messaging, text messages); interviews with all suspects and witnesses; and occasionally other investigative techniques such as surveillance (e.g. via video surveillance). Once again, in regard to the latter, any surveillance techniques considered must conform with the GDPR and the Labour Code.

Furthermore, in regard to the collection of evidence, employees must be informed that their personal data may be collected in the event of an internal investigation. (Companies are advised to place this information as a boilerplate clause in all employment agreements or privacy policies to ensure that staff members fully understand).

In fact, the major challenge in conducting an internal investigation in the Czech Republic is collecting evidence as a means of protecting a company's assets and property while still complying with data and personal-privacy regulations.

It must also be remembered that according to both EU and Czech regulations, personal data applies to all information that can identity an individual, such as their email address or something as banal as a vehicle registration number. Hence, during an investigation, any evidence that contains this type of seemingly insignificant personal information must be collected and processed with care.

Basically, further to the goal of protecting personal privacy, a Czech internal investigation should be designed to adhere to the legal principle of "lawfulness, fairness and transparency". In short, the investigation should have a clearly defined mandate. Only evidence pertaining to the investigation's target should be collected. The evidence should be definitive and stored for only a specific period of time. Not only should all evidence be kept secure, the entire investigation must be held in strict confidentiality.

Data protection, however, is not a company's only concern when conducting an internal investigation. The query must also comply with the Czech Labour Code.

From an employer's points of view, the Labour Code forbids employees from using company resources (e.g. email accounts, phones, laptops) for personal use and allows the company to monitor whether employees obey this general prohibition. By cautioning employees not to use work equipment for personal use, employers can help safeguard employee privacy.

Czech labour law does allow for other types of monitoring, such as video surveillance of work areas. But for this surveillance to be implemented, there must be a concrete reason (e.g. risk of theft of company supplies) and the video surveillance should be limited to this specific threat. In short, such surveillance, if deemed necessary, must be conducted in an appropriate and proportional manner.

In addition, employees must be informed about the surveillance.

Although the Labour Code doesn't directly regulate inspections, such as the examination of email records or computer hard drives, such one-off examinations appear to be affected by the same rules governing worksite surveillance. Hence, these inspections should always be conducted in a measured way, and only if there is a valid reason to do so.

Ultimately, all reasons would stem from the employer receiving a report or evidence of misconduct. The most effective method of

receiving this information is through a Whistleblower. Hence, companies are advised to create their own Whistleblower channels so that anyone witnessing wrongdoing can report it in a way that allows for the protection of his identity.

Currently, Czech law does not directly regulate Whistleblowing, although there are some provisions for this type of reporting in bank and finance regulations. Whistleblowing, however, is indirectly governed by a series of other laws: the Labour Code's obligation for "general prevention" of misconduct on the part of employees; the Criminal Code's requirement that some crimes must be reported; and the Czech Republic's anti-money laundering provisions.

Any Whistleblower system implemented at a company must protect the individual making the report. To ensure strict confidentiality, a company can use a third party, such a law firm, to set up and manage the Whistleblowing system.

The Czech Republic has drafted legislation in the past to regulate Whistleblowing, which failed to win parliamentary support. Currently, Czech lawmakers are drafting a Whistleblowing bill that would contain the key requirements of the EU's Whistleblowing Directive, which requires member states to pass a law before December 2021.

According to the EU Directive, local legislation must allow for two types of reporting channels: internal systems within private companies of more than 50 employees and external channels. In the Directive, ensuring the safety and confidentiality of the Whistleblower is paramount.

After potential misconduct has come to light – either from a Whistleblower or an internal audit – a company should carefully consider whether an investigation is permissible in light of GDPR and Labour Code regulations. If a particular employee has been implicated in a complaint, it should be verified whether he was informed about the possibility of an investigation (i.e. whether the potential for an investigation was included in his employment contract or elsewhere, such as in the company's privacy policy).

If an investigation is called for and an employee was aware of the possibility of an investigation, the company's first decision may be to suspend the employee temporarily in order to remove him from the work environment so that his presence does not adversely affect the inquiry.

Once an investigation is underway, an appropriate forensic tool may be the interview. Both the suspect and any witnesses can be interviewed, but once again Czech law is mute on how interviews should be conducted. Nevertheless, it is recommended that Czech companies keep certain interview protocols.

For example, minutes should be taken of the interview session, which the interview subject should review and sign to confirm the transcript's accuracy. (An investigation cannot make an audio or visual recording of an interview without the subject's explicit consent). Interviews should be conducted in a question and answer format with the intention of gathering facts surrounding the case. Under no circumstances should interviewers attempt to force a subject into "confessing to a crime". In fact, the Labour Code provides a list of sensitive topics, such as past criminal records and the pregnancy status for women, which an interviewer is prohibited to ask about if the subject matter is not relevant regarding the type of work performed by the employee being interviewed.

In addition to interviews, an internal investigation may need to collect evidence from the suspect's electronic correspondence.

If a company allows employees limited personal use of company communication equipment, investigators must take great care to avoid inspections of private emails. Distinguishing between professional and private mail can be done by considering the email address used, the identification of the sender, the information in the subject line of the mail, the salutation employed at the top of the email and whether certain keywords connected with the investigation appear in a given message.

If a company has forbidden the use of company equipment for private use, employees must understand that the assumption of privacy is lower and all emails found on the company server can be considered as work-related and accessed by the investigation (unless it is clearly a private message).

In terms of company-owned hardware, such as Smartphones, laptops and computer drives, companies are entitled to inspect the contents. In these searches, the same privacy protocols must be observed. If a company decides to allow employees limited access of company equipment for personal use, the company should draft rules governing this usage, such as requiring each employee to create a specific folder where

personal information can be stored. During searches, an investigation can only open files that are work-related.

In terms of the make up of investigation team, companies can appoint officials from its compliance and HR departments to conduct any inquiries. But firms can also contract third parties to oversee the process. CMS, for example, offers a service for conducting an investigation, collecting documentary evidence, and passing this evidence on for analysis, as well as possessing software capabilities to conduct keyword searches of drives and communication servers.

Lastly, when the investigation is concluded, companies have an option of compiling a final report or protocol. Since Czech law does not require companies to produce such a report, a company – based on the results of the investigation – may decide not to do so, such as if the allegations reported by a Whistleblower turned out to be unfounded.

If the investigation discovered wrongdoing that the company must act upon (with the risk of being later challenged in court), the firm is advised to issue a report and judgment that fully describes the investigatory process, evidence collected and justification for the judgment.

The final report should be presented to the suspect who should be given the opportunity to respond to the final conclusion. Companies should be aware that this report may be used as evidence in any future court action.

In terms of sanctions, if an employee is found guilty of wrongdoing, the company has several options. Employees guilty of damaging company property can be asked to provide compensation. (This can only be done in compliance with the Labour Code, which places restrictions on employee liability in these situations).

In cases of misconduct, disciplinary action may be required. For minor misconduct, a company can issue a warning letter that can be placed in the employee's file. If the misconduct is more serious, termination of employment may be called for.

In most cases of termination, employees can be fired with notice. In highly serious cases, however, immediate termination can be ordered. In all instances of employee termination, the Czech Labour Code sets down specific procedures and requirements that must be followed.

As stated, the Labour Code does not to apply to company executives. In these cases, executives found responsible for property damage can be asked to pay compensation. In instances of serious abuse, the executive can be relieved by way of a "recall from office".

Clearly, ahead of the passage of specific Whistleblower legislation in the Czech Republic, Czech companies do have options when confronted with reports of misconduct or wrongdoing in the workplace. By following carefully considered procedures, companies can ensure that any allegations of misconduct are addressed in a way that complies with data-protection laws and the Labour Code, and protects a company from future court challenges.

For more information on conducting internal investigations in the Czech Republic, contact your regular CMS advisor or local CMS experts:

Jakub Kabát
Associate, CMS Czech Republic
E jakub.kabat@cms-cmno.com

Daniel Szpyrc
Lawyer, CMS Czech Republic
E daniel.szpyrc@cms-cmno.com

France

Click to listen to the webinar recording
Published 14 January 2020

In rooting out misconduct, French internal investigations must balance employee rights with effective management

When conducting internal investigations, a French-based company must conduct a thorough query upholding its obligation to provide a safe and well-managed work environment while at the same time protecting the personal freedom and privacy rights of its employees.

While balancing employee rights with management duties may seem like a tightrope walk between two contrasting objectives, French law is clear. Any restriction on an employee's individual freedom through an investigation must be justified and proportional to the legitimate objective pursued.

French law recognises various types of abuse cases likely to trigger a whistleblowing process, including: infringements of the individual rights of an employee, which usually falls under the category of discrimination, harassment or attempts to exert unlawful control; serious risk to an employee's health and safety through problems in the work environment, exposure to dangerous products or hazards posed by specific tools or machinery; perceived dangers to public health or the over all environment; and any threat to the economic wellbeing of a company through fraud, corruption or mismanagement.

In each case, employers are obliged under French law to respond in different ways. In situations where an employee's personal rights may be threatened, an employer must hear out the charges and launch an investigation. A failure by the employer to respond adequately could result in proceedings.

If an employee's health and safety are potentially at risk, the complaint will be officially lodged through a "dedicated register" and the employer will immediately launch in investigation. An emergency meeting must then be organised within 24 hours, and if a disagreement between the Whistleblower and company persists concerning the nature or gravity of the disputed facts, the Labour Inspector may be required to step in.

If an employee spots risks to public health and the environment, he must again lodge his complaint in the company's "dedicated register". If a company investigation does not uncover a risk, the company's Works Council may decide to report the case to a state prefect.

In terms of economic alerts where a company's wellbeing is at risk, the Economic and Social Council (*Comité Economique et Social*, which replaces the Works Council from 1 January 2020) will address this during its next official meeting and demand an immediate response from the company, which will be obliged to answer any and all of the Council's questions.

If the company's responses are deemed insufficient, the Council will draft a report. A chartered accountant, paid for by the company, can assist in this if the Council chooses. Ultimately, the chartered accountant's report will be forwarded to the company's board of directors and statutory auditors.

A mandatory Whistleblowing process exists in France for companies of more than 50 staff members. Based on the 2016 *Sapin 2 Act*, this

process protects the identity of a Whistleblower and the confidentiality of the information that has been disclosed.

According to the Act, the Whistleblowing procedure is as follows: the staff takes his complaint to his immediate manager, employer or some other company representative identified in the firm's internal regulations. If the company does not act on the complaint, the Whistleblower can then appeal to the courts, the Officer for Human Rights or a professional association. If these bodies fail to act (or if the complaint is deemed a public emergency), the Whistleblower can appeal to the press or social media to get the message out.

By law, an individual lodging a complaint must receive protection against retaliation in the workplace, although to be protected a Whistleblower must be an employee, trainee or job applicant; he must be disclosing a crime or infringement of any regulation that endangers the environment or public safety; he must be a disinterested party (who cannot benefit from the complaint) and must be acting in good faith; and he must follow the complaint process as it is set out in the law.

French case law has recognised Whistleblowing systems used by U.S. companies further to the *SOX Act* operating in France, but adopting these procedures are optional and no employee can be sanctioned for not reporting an abuse through this system.

Also, this U.S. system only refers to financial wrongdoing and corruption and does not address workplace harassment. Neither the reports nor the identity of the Whistleblower

can remain confidential, although employees making complaints are protected from retaliation (i.e. being fired for disclosing corruption) unless a later investigation proves that the employee had knowingly filed a false report.

In the French system, the law dictates that employers conduct a disciplinary investigation within two months of learning about an alleged wrongdoing. During the inquiry, the company's tactics must be transparent, adhering to established regulations on safety and employee rights. The employee under scrutiny must be informed of the scope and ramifications of the investigation and the collection of evidence must fully conform to French and EU data protection regulations.

Furthermore, any controls placed on an employee during an investigation must not violate his rights and must be justified by and proportional to the alleged wrongdoing.

Although not required by French law, bullying and harassment cases should involve staff representatives in the investigation as a gesture of respect to the employee under scrutiny and to underscore the company's commitment to fair play.

In terms of investigative techniques, a company can search any tool or item that is considered an exclusive professional asset, such as a company-owned laptop. For those assets, such as a company vehicle, that is considered to be both a professional and personal asset, searches must be conducted according to established internal rules and only in the presence of the employee.

If a company wants to search an employee's belongings, such as a personal Smartphone or a bag, it must receive the employee's consent first. The only rare exception to this is in the case of a security-related emergency, such as a bomb threat where bags and purses may need to be inspected.

Phone calls can only be recorded, based on established company policy, for training and employee evaluation purposes. As for other techniques, employees cannot be subject to surveillance or "tails" outside of the workplace. Employees can be interviewed, although French case law favours the use of this tool in bullying and harassment cases. When employees are interviewed, they must be questioned according to a carefully constructed questionnaire. The results of the interview must be transcribed, and a written report on the interview's findings must be drafted.

If an investigation finds evidence of wrongdoing, a staff member can be given one of four sanctions. He can be assessed blame, given a warning, suspended without pay or dismissed.

When levying sanctions, employers must keep in mind that they cannot sanction an employee more than once for a particular wrongdoing. The employer must confront an employee with the full charges against him, and give the staff member an opportunity to respond. And lastly, the punishment must be proportional to the wrongdoing. An employee cannot be validly dismissed for a minor transgression.

For more information on the pitfalls of conducting internal company investigations in France, contact your regular CMS source or local CMS experts:

Caroline Froger-Michon
Partner and Co-Head of Employment Group, CMS France
E caroline.froger-michon@cms-fl.com

Vincent Delage
Partner, CMS France
E vincent.delage@cms-fl.com

Germany

Click to listen to the webinar recording
Published 2 December 2019

German business awaits internal-investigation protocols in face of anticipated corporate sanctions law

With lawmakers in Berlin expected to pass the *Corporate Sanctions Law* within the coming year, German businesses are expected to adopt comprehensive protocols for internal investigations in order to comply with this new and potentially high-risk regulatory climate.

According to legal analysts, the new law will cause public prosecutors to investigate corporations if evidence of malfeasance is detected in the way of corruption, regulatory violations or financial crimes, and will dramatically increase the penalties against a business.

These penalties are expected to be onerous, including fines of 10% of annual worldwide group turnover. In addition, assets obtained from the criminal offences can be confiscated.

In response, Germany's legal community is recommending that businesses lose no time in preparing systems to investigate wrongdoing internally should evidence come to light.

Internal investigations, of course, provide corporations with the ability to better supervise their workforce and ensure compliance. But in the case of wrongdoing, a rapid and robust investigation by a company that immediately exposes any improper acts by rogue personnel and provides prosecutors with "clarification assistance" on the matter can result in significantly reduced penalties.

Specifically, if companies respond to a public prosecution with their own internal investigation that exposes wrongdoing and supplies evidence to the satisfaction of state investigators, a company will find the upper limit for sanctions reduced by one-half and no application of minimum sanctions. What is more, the court will not announce its judgment in public in the Corporate Sanctions Register.

In short, corporations that practise full disclosure with their own internal investigations stand to pay less in fines and avoid bad publicity.

But in light of German employment law and statutes governing Works Councils and data protection, what type of internal investigation can a German company implement now before the sanctions law is passed?

First and foremost, when a company's leadership uncovers evidence of wrongdoing, they can question any staff member who might have pertinent information, including potential suspects and witnesses. Questions pertaining to an employee's main role in the workplace have to be answered. Since an employee has no right to refuse to give a statement, interviewees who do not want to answer often retreat into memory gaps. Hence, questions should be carefully crafted ahead of time.

In order to collect evidence for later assessment, formal interviews should be conducted. Employees and managers concerned are obliged to take part in the questioning so long as the interviews themselves are conducted in an appropriate place and time and the queries concern their primary duties in the workplace.

Staff members being questioned should be adequately informed about the reasons for the

interview. Corporations cannot base interviews on groundless suspicion or use them as fishing expeditions for potential wrongdoing.

In terms of making records of interviews, audio or video recordings are possible, but only with the consent of all involved. And even with consent, experts warn that digital recordings of interviews can produce lengthy transcripts in which the precise meanings of statements are not always clear.

Given these considerations, some legal analysts advise that it may be more efficient to take written minutes of an interview, which the interviewee can later review, correct if necessary and ultimately sign.

Who can and should participate in these interviews? Even in a company with a Works Council installed to represent the interest of employees, these councils have no legal right to participate in interviews.

Nevertheless, Works Councils must be notified if an internal investigation is taking place and some analysts even recommend that council members be permitted to sit in on the interview in order support the staff member being questioned.

With support at hand on their side of the table, interview subjects are often more confident and forthcoming, and interviews can be more productive.

As stated, adopting a system for internal investigations into a company's corporate culture can be an invaluable asset after Germany adopts it Corporate Sanctions Law. But there are some caveats to keep in mind.

Not all internal investigations are considered equal. To be eligible for a reduction in penalties, an internal investigation must contribute significantly to clarifying an offense. In short, the investigation must reveal and provide actual evidence to prosecutors. Moreover, the internal investigation must be conducted in accordance with the fair trial rules. This means, for example, that the employees involved should be informed of a newly created right to refuse to provide information.

Companies can use outside help in their internal investigations, such as employing law firms that have partners and digital resources that specialize in such inquiries. But lawmakers demand that "Chinese walls" be erected in these investigations, and that lawyers investigating wrongdoings not serve as defense attorneys representing the company during court proceedings. A single law firm can do both jobs, but a firm must allocate its staff accordingly so that investigators are not also leading the defense.

For more information on Germany's Corporate Sanctions Law, CMS digital resources for corporate inquires and how CMS can assist any corporation wishing to launch an internal investigation, contact your regular CMS source or local CMS experts:

Martin Lutzeler
Partner, CMS Germany
E martin.lutzeler@cms-hs.com

Laura Blumhoff
Counsel, CMS Germany
E laura.blumhoff@cms-hs.com

Hungary

Click to listen to the webinar recording
Published 2 December 2019

Hungarian companies turn to internal investigations to reduce liability

When developing polices on conducting internal investigations within your company, it is important to understand who may need to be investigated should evidence of wrongdoing surface. That any employee no matter his responsibilities can be the target of a probe is widely understood. But executives (e.g. Executive Directors, Members of the Board of Directors and Members of the Supervisory Board) can also find themselves under investigation even though they are in a civil-law (and not an employment law) relationship with the company.

When conducting an investigation, companies have a variety of methods at their disposal, which include:

— Inspecting the electronic communications of the target (e.g. emails, text messages) on company smartphones, laptops and computers, or the hard drives of these devices.

— Directly questioning the person under investigation regarding evidence or allegations of wrongdoing.

— Interviewing other employees or company executives who are witnesses to the wrongdoing.

— Conducting surveillance of various kinds of the person under investigation.

In Hungary, any investigatory tool that is not prohibited by law can be used to collect evidence in an internal investigation as part of the Hungarian legal concept of "free evidence". But the actual techniques used will depend on the unique characteristics of a given case and the outcome that investigators are attempting to achieve. For example, if an alleged wrongdoing has labour-law consequences, the investigatory techniques used may be different than situations where there are civil-law consequences.

Companies can learn of a compliance issue from various sources: the police, which might uncover it in an investigation; a rudimentary company audit; or a Whistleblower report. No matter how a wrongdoing comes to light, the type of misconduct usually dictates the method to be used to investigate it.

Financial irregularities, for example, are usually investigated through inspections of communications and records, and interviews with suspects and witnesses. If funds have been misappropriated, these techniques along with video surveillance can be employed.

In all cases, internal investigations require preparation. This includes forming an investigatory team that is made up of members who are seen as both unbiased and competent to probe the subject matter at hand. (For example, financial misconduct would require investigators with an understanding of accounting and financial procedures). In addition, the team will need to identify and acquire any and all tools needed for the probe. Companies must understand that the work done preparing for an inquiry is as important as how the investigation is conducted. Sound preparation will not only ensure an effective investigation, but it will also help investigators comply with all regulatory requirements, such as data protection rules and employee privacy rights.

This last point is essential. If an investigation is conducted in a way that violates employee rights or privacy regulations, a company could later be sanctioned by the competent data protection authority and challenged in court as a result.

To protect themselves against liability, companies should understand that employees generally have the following rights:

— Before employees are interviewed, they should be reminded of their data protection rights under Hungarian law and the EU's General Data Protection Regulation (GDPR).

— When questioned in an investigation, an employee has the right to have a lawyer present.

— Interviews cannot be recorded without the consent of the person being interviewed.

— Interviews and questioning must be conducted in a way that is not perceived as bullying or harassing. In short, care must be taken when interviewing suspected employees in order to spare the company any risk of liability. As further protection, more than one investigator should take part interviews so that there is a witness at hand to contest charges of harassment.

— After questioning is completed, minutes of the interview should be drafted, given to the employee to review, and – preferably – signed by the interview subject if deemed accurate.

Apart from interviews, the search of electronic communications and the company's digital storage facilities is a highly effected method in any investigation. But it is a method that requires the appropriate tools, such as advanced AI software. One such software solution is "CMS Evidence", which is a fully integrated evidence-collection system operated by specially trained experts that can be applied to company computers or communication systems and can both collect pertinent documents and perform a forensic analysis. In addition, the software "Brainspace" can conduct searches of large documents, communication systems or servers and can retrieve evidence based on keywords, user names, and other criteria.

Any searches of employee communications or work files raise the issue of data protection, which is regulated in Hungary by three laws: the EU's GDPR, which provides general protection regarding the processing of personal data; the Hungarian Labour Code (Act 1 of 2021), which offers some regulation of data processing in the workplace; and the Hungarian Whistleblowing Act (Act CLXV of 2013), which allows companies to establish a specific reporting infrastructure, such as dedicated telephone "hotlines" for filing reports.

It should be noted that the GDPR and the Labour Code apply to almost all information garnered in an investigation pertaining to an individual employee. In regard to evidence collection, important principles to remember include: only a minimum amount of information directly applicable to the investigation should be processed, and a reasonable time limit should be placed on its storage; data protection considerations should be applied to all personal data processed, including any data from witnesses or suspects outside the company; and investigations that have criminal-law implications have specific data-processing requirements. In addition, if any evidence collected is to be shared with third parties, due diligence should be conducted regarding their data-protection systems so that employee personal data is not compromised as a result of the transfer.

If a highly sensitive company document is collected as evidence and the company wishes to protect this document from disclosure, an exception known as the "legal advice privilege" can be invoked, but this exemption should be used carefully and sparingly.

Data protection regulations also require due notification. According to Articles 13 and 14 of the GDPR, evidence and information cannot be collected unless the company issues a notice to employees and affected third parties that their data may be processed in the investigation, which is about to commence.

But it may not be clear what data constitutes legitimate evidence. In this case, pertinent information can be identified beforehand by conducting a "legitimate interest test", in which a company carefully weighs its interests against the personal privacy interests of employees and third parties. Through this process, only information deemed essential to the investigation is identified for processing.

Other documents and notices that should be issued in order to be compliant with GDPR and other regulations include a data protection impact assessment, operational rules and privacy notices for the maintenance of Whistleblower hotlines, and internal policies on how to conduct and record an investigation.

Privacy regulations also have an impact on digital searches of company devices and message systems. When searching communications and files, investigators must distinguish between work-related and personal employee information, and avoid processing any private data.

Employees should be instructed to protect their personal data by labeling private emails and files storing them in clearly marked folders.

Investigators can also arrive at conclusions and find personal data by studying the ebb and flow of data traffic logs; and they can note the recipients and subject lines of all emails as well as the names and formats of files. Investigators can also use Internet history to record the websites that suspects have visited and the time spent at these sites.

Another important element of internal investigations is Whistleblowing. As already stated, Hungary currently has a Whistleblowing law, but this statute will change in the near future as a result of a directive on Whistleblowing that was issued by the EU in 2019. According to this directive, by 17 December 2021 EU member states must pass national legislation on Whistleblowing that introduces minimum standards for Whistleblowing protection, allows Whistleblowers to issue reports within their company or to an outside authority, obliges companies with 50 employees or more to put in place Whistleblowing systems and investigation procedures for acting on any reports, and creates in-house safeguards that protect the identity of Whistleblowers and the confidentiality of their information.

Companies must appoint officials to act on these reports and recommend solutions should the misconduct reported prove accurate.

Feedback on a report will have to be provided in a timely fashion. Internal reporting channels for Whistleblowers must meet certain standards in terms of independence and autonomy. Safeguards to Whistleblowers must include protection against retaliatory action for filing

a report (e.g. threats to a Whistleblower's job security for disclosing embarrassing information). Whistleblowers cannot be punished for the methods used to access the reported information unless the methods were unlawful.

It should be noted that non-compliance with regulations on data-processing vis-à-vis internal investigations and Whistleblowing has resulted in the levying of fines of between EUR 1,500 and EUR 30,000 in Hungary. The GDPR, on the other hand, permits fines of up to EUR 20m for infringements of privacy and data protection. Hence, the costs of breaching these regulations can be onerously high.

Once an investigation has been completed, a detailed report of the inquiry and its findings should be produced. This report should be carefully written and thorough since it may be used as evidence should the investigation's findings be challenged in court. A copy of the report should be presented to the accused so that he can read it and – if he so chooses – respond.

If the report determines that the accused is guilty, a company can proceed in various ways. An employee can be issued a written warning. For a more serious offence, an employee can be terminated, but in this situation termination must be concluded in line with Hungarian Labour Code requirements. If an employee's misconduct resulted in damage to the company, the individual can be asked to pay compensation, but again this must be sought according to labour law procedures.

Executives found guilty of misconduct can be recalled from office or asked to pay compensation. In this situation, civil law (and not labour law) applies.

An individual found guilty of misconduct can appeal the findings according to a process set down in employment law.

If an individual believes his personal data has been processed unlawfully during the investigation, he can also file a complaint to Hungary's data protection authority.

Finally, if a terminated employee considers his punishment unwarranted, he can file suit against the company for "unlawful termination" and seek damages for any harm incurred. Compensation can be granted for material damages (e.g. loss of wages, salary) and for "non-pecuniary harm" (e.g. personal trauma, damage to an individual's professional reputation).

But the best way to deal with an internal investigation is to create policies designed to prevent wrongdoing from ever happening. Companies can be pro-active by drafting internal by-laws that inform employees that they may be monitored in the workplace and should adhere to a detailed code of conduct. Employees should also be informed about the possibility of internal investigations and Whistleblowing systems. Company by-laws should also:

- Prohibit the use of company devices for personal use.
- Create a Whistleblowing system for employees and third parties (e.g. clients, contractors, etc.).
- Create checks to ensure that companies comply with all regulatory obligations.
- And before any investigation of misconduct, ensure there is sufficient justification to launch a probe in which the collection of evidence will necessarily infringe on the privacy of individuals.

For more information on how to conduct internal investigations in Hungary and details on the investigation tools CMS Evidence and Brainspace, contact your regular CMS advisor or local experts:

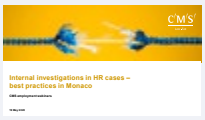
Gabriella Ormai
Partner, CMS Hungary
E gabriella.ormai@cms-cmno.com

József Kohl
Associate lawyer, CMS Hungary
E jozsef.kohl@cms-cmno.com

Márton Domokos
Senior Counsel, CMS Hungary
E marton.domokos@cms-cmno.com

György Bálint
Senior Counsel, CMS Hungary
E gyorgy.balint@cms-cmno.com

Monaco



Click to listen to the webinar recording
Published 16 June 2020

Monaco business community turns to corporate internal investigations

For an internal investigation in Monaco, the specific type of allegation will – in many cases – determine how an inquiry should be conducted.

For example, if an employee is alleged to be working while under the influence of alcohol, he can be subject to testing only accordingto a procedure outlined in a ministerial ruling under the laws of Monaco, and only if the *règlement intérieur* of the Company provides for it.

If an employee is alleged to be working under the influence of drugs or narcotics, it is not mandatory, but highly recommended that the testing be conducted according to Monegasque rulings and to be provided in the *règlement intérieur*.

For other allegations of wrongdoing or misconduct, however, companies are not required to follow these rules and can conduct procedures according to best practices and the unique demands of each particular case.

How does a Monaco-based company learn of a case of misconduct that might become the target of an internal investigation?

Like in other parts of the EU, misconduct is often communicated to company management through Whistleblower reports or alerts. In these instances, a worker witnessing a wrongdoing that it is either a contravention of company regulations or Monegasque law reports this misconduct to company management or its HR office.

In other instances, company managers either stumble upon an infraction or discover it through an internal audit.

For harassment issues specifically, any company with a headcount of over 10 employees must implement a specific policy to prevent harassment and violent behavior in the workplace, which includes the designation of a "referent". Failing to do so, the employer is exposed to criminal and civil sanctions.

For more general issues, there is no specific obligation towards the Monegasque employer, which must investigate according to its duties.

In this respect, even if Monegasque law does not demand action for a particular type of wrongdoing, a company is advised to investigate when it has knowledge of an alert / a behavior. Indeed, companies should establish policies and procedures for conducting the various inquires they may face in the future: reports of alcohol or drug abuse in the workplace; and all other types of wrongdoing from fraud to corruption.

Indeed, many companies, further to an EU Directive on the matter, have implemented Whistleblowing systems or channels, which provide an email address or hotline where reports of wrongdoing can be made. These companies also have Whistleblowing procedures in place, which should specify exactly when and how a report can be made, and the company's response when they receive such an alert.

Also, before an allegation is ever made, companies could name an official who is responsible for overseeing investigations and establish general policies on the collection of evidence.

If a company has investigation procedures like this in place, they are able to act the moment a Whistleblower alert is reported or wrongdoing

is uncovered by other means. How an investigation proceeds now depends on the severity of the misconduct.

If the allegation is serious and the investigators believe there is a danger that witnesses can be influenced or evidence tampered with, it may be advisable to place the accused employee on temporary furlough to extract him from the work place. It should be made clear that when an employee is placed on furlough, the suspension is temporary and merely a function of the investigation. It is neither punishment nor a supposition of guilt.

Monaco-based companies lacking a history of internal investigations may wonder if it is necessary to have *ad hoc* investigation procedures in place to probe misconduct that is not mandated by law.

In our opinion, company executives should actively pursue investigations as part of its commitment to internal security, employee welfare, and to reduce the risks to the company. Without a commitment to internal investigations, a company risks legal threats regarding its civil and criminal liability in addition to damage to its brand and reputation.

When a company resolves to conduct an investigation, it's vital that this responsibility be placed in the hands of a representative of the employer, who has the legal power to do so. The employer can opt to have an outside entity (e.g. a law firm with experience in corporate investigations) oversee an inquiry, but it is usually not necessary to outsource the investigations.

Once the company has selected a manager or outside party to lead the probe, the investigation can begin. But all investigations should adhere to several basic principles. First of all, a detailed record should be kept of the investigation, including the employees who are interviewed (along with the details of their testimony) and the evidence collected.

When collecting evidence that directly impacts employees (e.g. pertaining to company email and messaging services), the investigation must take care to follow all Monegasque regulations pertaining to privacy and data protection.

Furthermore, an investigation must ensure the confidentiality of both employee data and all information surrounding a probe, including investigation strategy. Employees can be informed about the general aims of an investigation, but a company is under no obligation to share details and must endure that a system is in place to protect the integrity of the investigation and the evidence it collects.

Perhaps the most important stage of the investigation will be employee interviews where the investigation's target (i.e. the employee accused of wrongdoing) and witnesses are questioned. As stated, interviews should be held in secure surroundings where witnesses can speak freely. Minutes should be taken of each interview that accurately record the testimony.

The current pandemic, which has prompted many Monaco-based companies to close offices and assign staff to work remotely from home, creates clear difficulties for the execution of internal investigations. Not only is documentary evidence more difficult to access, employees are unavailable for face-to-face interviews.

How should a company conduct an investigation during the current pandemic while remote working is in place? If the alleged misconduct is not overly serious and there is little risk to the company, the investigation can be postponed until the crisis is over. But in more serious cases, the investigation can continue with interviews conducted over video conferencing. For the sake of confidentiality, the investigation will have to find technical solutions to ensure that the interviews are secure and private. But there is no reason to delay an investigation vital to a company's interests even during the current crisis, although with much of Europe slowly reopening its economies, business may soon be back to normal (within certain limitations).

Once all the interviews are conducted and the evidence collected, the investigators will arrive at a decision as to whether the allegation has been confirmed or should be dismissed due to lack of proof.

If the allegation of misconduct is confirmed, the investigatory team should issue a formal letter to the employee found guilty of wrongdoing outlining the charge and findings of the probe. The letter will also inform the employee of the disciplinary action he is to receive, which can be – in simple cases – a warning. For more serious wrongdoings, temporary suspension or full dismissal may be called for.

The investigators will also have to determine if the wrongdoing breaks any civil or criminal laws. If this is the case, the company should discuss with legal counsel any obligation it may have to report its findings to authorities.

Clearly, by having Whistleblower and internal-investigation policies and procedures in place, a company can provided needed protection to employees and its own interests.

For more information on conducting internal investigations in Monaco, contact your regular CMS advisor or local CMS experts:

Sophie Marquet
Partner, CMS Monaco
E sophie.marquet@cms-pcm.com

Sophia Bernardi
Middle Associate, CMS Monaco
E sophia.bernardi@cms-pcm.com

North Macedonia

Click to listen to the webinar recording
Published 16 June 2020

Macedonian Whistleblowing law stresses anonymity and protection

As world economies and multinational corporations enact policies and procedures on corporate investigations and Whistleblowing, North Macedonia is following suit: implementing laws and regulations that regulate internal investigations and the recognition and protection of Whistleblowers in both the public and private sectors.

From a legal point of view, North Macedonian law indirectly regulates corporate internal investigations through its Labour Law, which includes three main types of disciplinary measures or penalties for corporate wrongdoing on the part of employees and managers. The legal system offers more direct regulation through the Whistleblowing Act, which protects individuals who report wrongdoing and provides guidelines for internal corporate investigations.

The following article outlines the laws and business practices regulating internal investigations and whistleblowing in North Macedonia.

Internal Investigations

Any internal investigation conducted within a Macedonian company must have clearly stated objectives. Although some objectives may vary from sector to sector, a company's investigative goals should include: collecting evidence in such a way to ensure the prosecution of any employees guilty of criminal misconduct; recovering any company assets lost or stolen as a result of corruption; identifying all employees guilty of misconduct and removing them from their positions; identifying any weaknesses in business operations that allowed the misconduct to take place; implementing reforms so the wrongdoing is not repeated in the future; doing everything possible to minimise risks to the business; preparing the company for future civil or criminal litigation; and protecting the company's brand and reputation.

Only by focusing on clearly stated goals can the investigation be successful. But what procedures should a company implement to execute these goals? In North Macedonia, there are two common approaches. The first is the "orthodox approach", which is made up of three basic steps. An internal investigation committee (usually made up of HR personnel) is created to respond to a wrongdoing. The committee then identifies suspects and interviews these individuals. Where possible, the committee also interviews potential witnesses.

Although the orthodox approach allows for suspects and witnesses to be questioned directly to get to the heart of any allegation, this approach does not always result in uncovering sufficient evidence, particularly if the suspect is uncooperative.

In order to obtain more evidence, businesses in North Macedonia can consider taking the more proactive "contemporary approach", which includes researching business emails, business phone records, internet histories and files contained on company computers or laptops and company smartphones.

Such an approach can uncover direct evidence of wrongdoing, but when using more invasive techniques great care must be taken when handling employee personal data to ensure that the investigation does not violate the employee's data protection and constitutional rights to privacy.

Some Macedonian businesses have been able to implement investigation procedures that are not regulated by Macedonian law. Despite these precedents, any company considering a contemporary approach to internal investigations should discuss its implications with legal experts.

Disciplinary procedures

Assuming that your investigation has uncovered misconduct and identified a guilty party, what disciplinary actions are you able to implement? The decision on what type of penalty to hand out is usually made by an authorised company official, such as the HR manager, who assesses the evidence and decides on the disciplinary measure. Labour law includes three main types of disciplinary measures: monetary fines, work suspension and employment termination.

When issuing a fine, the amount must be balanced between three factors: the severity of the violation, the consequences of the violation and how the employee performed his work duties. The fine, however, cannot be more than 15% of the last paid monthly salary to the employee and it must be imposed within six months of the decision.

In regard to suspensions, a worker can be suspended while the employer considers whether the wrongdoing warrants termination. In this case, the suspended employee is entitled to receive 50% of the salary received the previous month for the duration of the suspension.

The employee can only be suspended if found guilty of one of the following four acts: endangering the life or health of other personnel or causing high-value damage; having a negative influence on the employer's operations; hindering the investigation in wrongdoing in the company; and being charged with a crime for acts committed in the workplace. It should be noted that an employee can be terminated for incurring repeated fines for wrongdoing.

As for termination, there are two types: termination with notice and termination without notice.

Employees can be terminated with notice for violating workplace order and discipline, failing to fulfil employment obligations, not carrying out the duties and obligations of their positions, not respecting working hours, acting negligently in the operation and care of equipment, causing damage on the jobsite and failing to notify employers of any damage.

For termination without notice, employees must be found guilty of committing any of the following acts: violating workplace order and discipline, particularly in cases where an employee is absent from work for three consecutive days; abusing sick leave; failing to observe regulations on health and safety in the workplace; arriving at work under the influence of alcohol or narcotics and performing negligent acts that lead to injuries, death or extreme damage.

After a disciplinary action has been handed out, the sanctioned employee can file a complaint contesting the verdict with the employer's "governing body". By law, a sanctioned employee has eight days after receiving notification of the disciplinary decision to lodge an appeal.

Whistleblowing legislation

The face of internal investigations in North Macedonia began changing after the 2015 adoption of new legislation on Whistleblowing, which was implemented to create a culture of transparency in Macedonian business and politics.

This law protects Whistleblowers in three key areas: the public sphere (e.g. government and politics), state-owned or private companies, and the employees who report wrongdoings to external authorities, such as police or prosecutors.

A Whistleblower is any individual who reports misconduct or wrongdoing. But who exactly can make such a report? According to the law, a Whistleblower can be an employee of a company or office; a service provider; a candidate for employment (i.e. a job applicant); a trainee or even a volunteer within the organisation; anyone with a current or past business relationship with the company or office; or anyone who has used the services of the company or office.

Regardless of the Whistleblower's profile, the moment the Whistleblower steps forward, the Whistleblower's identity must be protected.

In terms of Whistleblower's acting internally within an organisation, the law sets down general rules. Companies with ten or more employees must create a Whistleblowing "rulebook" in which the rights and protections of Whistleblowers are clearly articulated. In addition, these companies are required to appoint a liaison officer who Whistleblowers can reach out to with reports of wrongdoing, even though – in practice – many Whistleblowers are reluctant to go to company officials with embarrassing disclosures.

By law, all liaison officers must act immediately when they receive a report. Firstly, they must initiate steps to protect the Whistleblower's identity. (If the liaison officer fails to do this and a Whistleblower's anonymity is compromised, the individual by law can seek protection from the courts and damages from the company for any hardships incurred as a result of the company's failure to protect his identity.)

Regarding this, the liaison officer must report back to the Whistleblower about the company's response to the allegations of misconduct no later than 15 days after the initial report was received.

For more information on the laws and practices regulating internal investigations in North Macedonia and its Whistleblowing law, contact your regular CMS advisor or local CMS experts:

Marija Filipovska
Partner, CMS North Macedonia
E marija.filipovska@cms-rrh.com

Dusan Bosiljanov
Associate, CMS North Macedonia
E dusan.bosiljanov@cms-rrh.com

The Netherlands

Click to listen to the webinar recording
Published 17 December 2020

Dutch experts cite preparation as best strategy against corporate misconduct

A company's best response to charges of misconduct is to ensure that systems are fully in place to both prevent and uproot any wrongdoing long before a complaint has been officially lodged, declare internal investigation experts in the Netherlands.

As logic dictates, the best response is preparation, insuring that all companies doing business in the Netherlands begin their corporate lives with the following four systems in place: a code of conduct for employees and management; an investigation regulation; a sanction regulation; and a Whistleblower Regulation, which is mandatory for firms with 50 or more employees.

What exactly are these systems?

Code of Conduct

A code of conduct is a written document that clearly defines the manner of personal and professional conduct that a company expects of its staff in the workplace. In order for such a code to be unambiguous to all, it should state precise guidelines for acceptable behavior and fully articulate the company's values and commitments.

For the sake of clarity, codes can specifically draw attention to examples of improper acts, such as discrimination, bullying, harassment, bribery and fraud.

Investigation Regulation

Precise Rules on Procedure should be put in place that can be executed the moment there is a suspension or evidence of misconduct. These procedures, which should be fully and clearly expressed to all employees, should include: how complaints should be made and the precise office or company official they should be made to; the team or committee that is mandated to review all complaints; and the possible investigative techniques to be used in response (i.e. CCTV surveillance, interviews, and data searches of documents, phones and laptops, etc.)

Just as employees should be made aware of a company's Code of Conduct and the parameters of its internal investigation protocol, they should also be made to understand that in the event of a misconduct investigation, their data (e.g. phone records, emails, internet history and usage) can be scrutinized.

For their part, companies must be aware that any internal investigation resulting in the processing of the personal data of an employee (or contractor, client, customer or any other person) must fully adhere to the EU's General Data Protection Regulation (GDPR).

Companies are also urged to cooperate with its Works Council – which by law is required for every firm made up of 50 employees or more – in drafting an investigation regulation.

Whistleblower Regulation

Aside from Codes of Conduct and the information on Investigation Regulations that a firm makes available to its staff, a firm should implement a Whistleblower Regulation when it employs 50 or more employees, and each firm should consult its Works Council when drafting this Regulation.

A Whistleblower Regulation should include how to respond in a timely fashion to any Whistleblower report, and a system must be in place to protect the identity of the Whistleblower. Efficiency is of the essence. Dutch law gives Whistleblowers the right to take their complaint to an authority outside of the workplace if a company does not respond in a timely manner to a complaint.

During and following an investigation

If a serious allegation has been made against an employee, the firm may decide to send the staff member home until the internal investigation is complete. But in these cases, firms are advised to carefully document their reasons for suspending an employee in case a court is later called upon to review the matter.

An employee charged with misconduct should be interviewed and allowed to state his case. In addition, in compliance with the law, fair practice and GDPR, he should be given the findings of the investigation and sufficient details on its scope.

Sanction Regulation

When an investigation has been concluded, companies should decide what sanction is necessary given the outcome. Responses can vary from no sanction to an official warning or even immediate dismissal for urgent cause.

Whatever course a company decides to take, it is crucial that all possible sanctions are clearly defined in company policy, communicated to all staff members and consistently enforced. This last point is crucial.

For more information on protecting your firm against internal misconduct or wrongdoing, contact your regular CMS source or local CMS experts:

Katja van Kranenburg-Hanspians
Partner, CMS Netherlands
E katja.vankranenburg@cms-dsb.com

Fleur van Assendelft de Coningh
Associate, CMS Netherlands
E fleur.vanassendelftdeconingh@cms-dsb.com

Poland

Click to listen to the webinar recording
Published 10 March 2020

Corporate culture in Poland offers best practices for conducting internal investigations

CEOS and managers seeking guidance on formulating procedures and policies for conducting internal investigations in Poland should not look for direct guidance from the state.

Polish law does not directly regulate internal investigations. In addition, there are no laws regulating grievance procedures when employees step forward with allegations of misconduct and no regulations that directly determine how employees should be interviewed and questioned over these allegations.

But companies facing this issue are not working in a complete legal vacuum. Laws governing data protection (in line with the EU's General Data Protection Regulation or GDPR), harassment, equal treatment and confidentiality offer managers some guidance on how to best conduct in-house inquiries in Poland.

Also, as more and more companies in Poland turn to internal investigations as a means of maintaining order and reducing their risks of legal liability, the Polish business community has developed a series of best practices that are in line with the nation's exiting laws and corporate culture. In light of all of this, what are the recommended procedures for conducting internal investigations in Poland?

For starters, we recommend that internal investigations be divided into three areas: a preparatory stage, the investigation itself and a follow-up, which involves disciplinary action if an employee was found guilty.

Preparation

Before an investigation is launched, a company must decide on the official who will oversee the process.

The best candidates are HR managers, compliance officers, or external experts such as a law firm with experience in these matters. Once appointed, this official must receive signed written authorisation to conduct the investigation from responsible company officials (i.e. management board members) and – in line with data protection laws – receive special authorisation to process the data of any employees.

Lastly, before launching the inquiry, the investigation commissioner should be fully acquainted with whatever procedures and policies regulating internal investigations are in place at the company so that evidence is collected and interviews conducted in line with these bylaws.

In terms of practices to avoid, we recommend that investigators do not release specifics about the investigation while evidence and testimony are being collected. Also, during the stage when witnesses are being questioned, we recommend not letting witnesses communicate with each other between their interviews so that they are not able to influence one another, reveal the nature of investigation, get their stories straight, etc.

Interviews

When questioning witnesses, we recommend that investigators inform all involved of the purpose and scope of the investigation without,

of course, revealing details on any findings or the identity of the whistleblower who revealed the breach.

Before being interviewed, witnesses should agree to testify by their own free will, and should sign consent forms attesting to this. This will prevent witnesses from being able to withdraw their testimony later.

In addition, all witnesses must be told that the investigation is highly confidential and should be asked to sign non-disclosure agreements relating to it.

When interviewing subjects, witnesses should not be bullied, restrained (e.g. prevented from leaving the interview room) or placed under undue pressure. Questions should not reveal details of the original allegation or compromise the personal data of any employee.

When conducting questioning, the investigation is under no legal obligation to allow witnesses to have friends or supporters in the interview room with them. This can be allowed if internal rules provide otherwise.

As for the recording method for interviews, we recommend that the minutes be taken. Recording interviews digitally is not advised, and investigators should take care to ensure that interviewees are not themselves making clandestine recordings of the proceedings.

If a company insists on making an audio or audio-visual recording, all data protection and GDPR regulations must be followed. In line with this, all witnesses should agree in writing that they consent to be recorded.

After the interviews are completed, investigators should compile a report that summarises the findings. This report both collates any evidence and proves that an investigation was actually conducted. Also, once this stage of the investigation is over, the whistleblower or complainant should be informed.

Neither the whistleblower nor the interview subjects are entitled to see this summary. Employers are under no obligation to share the investigation's findings.

Disciplinary actions

If an investigation proves that an employee is guilty of misconduct, a company will need to consider meting out disciplinary measures.

The first form of discipline is the admonition or reprimand, which will be communicated by a written warning letter, a copy of which is kept in the employee's file.

In terms deadlines, this penalty must be assessed no later than two weeks after the company learns of the misconduct, but not later than three months after the misconduct.

A penalty is handed out for fairly basic infractions, such as ignoring or disobeying essential work orders or being under the influence of alcohol or drugs on the job.

The company must invite the employee to a meeting during which he will be given the opportunity to discuss the case. During the meeting, the employee must have a chance to submit his explanations in relation to the misconduct, circumstances and motives. After the hearing, the company must reflect on the situation. It can either refrain from imposing a penalty or impose a sanction. The company must issue the warning letter in writing.

The employee can also challenge the outcome of the investigation, but he must do so in writing within seven days of receiving the verdict. This letter must be addressed to the company, which – when considering this appeal – must consult with the company's trade union (if a union is present at the company).

If the company decides not to amend the decision, the employee has a right to take the matter to labour court, but the employee must do this within 14 days of receiving the company's final decision.

A penalty is not the only form of punishment. Employees can be terminated with notice for more serious infractions, including breach of duties. In this case, a written notice of termination is presented to the employee and his labour union, if any, should be consulted. An employee can appeal this type of termination to the courts, citing generally unfair dismissal or a similar defense, but such a filing must be made within 21 days of receiving the notice.

If the courts rule in favour of the employee's motion, they can demand that the company pay compensation to the employee equal to up to three months' salary. Alternatively, the employee can be reinstated to his previous job position (together with a salary) for up to two months.

Also, companies cannot issue termination with notice to employees while they are on holidays, maternity leave, parental leave or absent due to illness. Employees approaching retirement age and trade union representatives are also afforded special protection from termination.

For highly serious misconduct, companies can dismiss employees without notice. Such termination is with immediate affect, and is reserved for serious breaches when an employee's actions have adversely affected the company's interests. In dismissals without notice, companies must serve these decisions to employees in writing no later than one month after learning of the misconduct.

Also, in these situations, a company does not need to hear an employee's version of events, but should consult with the employee's trade union (if any).

Following a dismissal without notice, an employee has 21 days to challenge this judgment in labour court. Finally, those protections mentioned above that insulate employees from termination with notice do not apply to dismissals.

In summary, although Polish law does not directly regulate internal investigations, Polish companies have options at their disposal to respond to allegations of misconduct and protect both their interests and the wellbeing of their employees.

For more information on conducting internal investigations in Poland, contact your regular CMS advisor or local CMS experts:

Katarzyna Dulewicz
Partner, CEE Head of Employment at CMS CMNO
E katarzyna.dulewicz@cms-cmno.com

Agnieszka Kałwa
Associate, CMS Poland
E agnieszka.kalwa@cms-cmno.com

Aleksandra Nowakowska
Associate, CMS Poland
E aleksandra.nowakowska@cms-cmno.com

Portugal

Click to listen to the webinar recording
Published 3 February 2020

Data protection and corporate laws regulate internal investigations while Portuguese lawmakers draft whistleblowing bill

With lawmakers in Lisbon currently drafting legislation on corporate internal investigations, Portugal can expect to have legislation soon that transposes the 2019 EU Directive on Whistleblowing.

But during this transposition process, Portugal is not in a legal vacuum when it comes to internal investigations in the corporate world. The Portuguese Data Protection Supervisory Authority (CNPD) promulgated two resolutions that directly apply to the collection of employee data during an in-house inquiry. One ruling (Resolution 765/2009) concerns the processing or collection of personal data for the purposes of internal communication and the other (Resolution 1638/2013) concerns the processing of personal data derived from information and communication technology in the workplace.

Specifically, the resolution regarding the processing of personal data for internal communication expressly prohibits the posting of anonymous reports, requiring accountability in the process in order to discourage slander and discrimination. But the ruling demands that individuals reporting abuse should have their identities protected. In addition, the resolution prohibits an employer from retaliating against a whistleblower by demoting, firing or sanctioning him even if the disclosures contain information that brings embarrassment to the company and its management.

The resolution also regulates the rights of the accused person in an investigation, giving him the right to access any and all information from the data controller about the accusation made against him, and the purposes of this data processing. The accused can also have access to any of his collected data.

The whistleblower also has rights. After a report is filed, the data controller must report back to the whistleblower and verify if an investigation is taking place, its purpose and its scope.

Data protection regulations in Portugal, however, do not regulate investigation procedures, which begs the question: without an *ad hoc* law in place, are Portuguese companies permitted to conduct internal inquiries when wrongdoing has been brought to their attention?

The answer is yes. As a result of a 2018 Corporate Governance Code issued by the Securities Market Commission, companies must adopt mechanisms for detecting abuses and a whistleblowing policy that guarantees a response to any reports of irregularities and protections for those exposing wrongdoing.

Based on the experiences of companies in the Portuguese banking sector, which has been progressive in creating such policies, a comprehensive internal investigations system should contain the following features: full definitions of what constitutes wrongdoing, corruption and a whistleblowing report; clear communication channels for reporting abuse; a process for conducting internal investigations and a body (i.e. committee) responsible for carrying them out; policies that encourage all misconduct to be reported, making it clear that anyone filing a report must identify himself and that anonymous allegations will not be accepted; policies that protect a whistleblower's identity and safeguard him against harassment; and

policies that ensure that the personal data of all employees involved are safeguarded.

No matter what internal procedures are in place, if wrongdoing is exposed, a Portuguese firm must initiate "disciplinary proceedings" as defined by the Portuguese labour code in order to be able to take action against an employee.

A crucial part of disciplinary proceedings is its deadlines. In general terms, a company must initiate disciplinary proceedings within 60 days after a violation has been revealed. This means that the clock begins ticking as soon as the employer becomes aware of the infraction and – presumably – the identity of the wrongdoer. A company's right to discipline an employee expires one year after the wrongdoing has been exposed.

As far as the structure of disciplinary proceedings is concerned, the Portuguese labour code sets down some basic requirements.

The code allows for an evidence-collection period, which it calls the "Prior Inquiry Procedure". During this time, evidence should be gathered with the aim of issuing a Notice of Fault (*Nota de Culpa*) against an employee by fully investigating the circumstances of an abuse and the events leading to it. Note that the deadlines for disciplinary proceedings can be interrupted during the Prior Inquiry Procedure, which means the clock stops ticking on these deadlines if the inquiry procedure begins within 30 days of the allegation and is expeditiously carried out, resulting in a Notice of Fault against an employee, which in turn is issued within 30 days since the conclusion of the Prior Inquiry Procedure.

Once the Notice of Fault has been presented, the disciplinary proceedings, led by the employer or individuals delegated this responsibility (e.g. outside legal advisors), can get underway.

During these proceedings, the labour code affords accused employees certain rights, such as access to any and all documents that are being used in the proceedings. (Failure to respect this right this could endanger an employer's ability to sanction an employee after the proceedings have been concluded.)

In addition, an accused employee can introduce his own exculpatory witnesses and documentation. An employer can only refuse the accused this right if it deems the request dilatory and unfounded. But in this event, the firm must fully explain its reasoning in writing. If an employer doesn't justify such a refusal in writing, this could result in an "irregularity of procedure" where the employee is eligible for compensation. (In this case, compensation traditionally amounts to approximately half the damages usually received for unlawful dismissal, but never includes reinstatement.)

As a general rule for all witnesses, testimony should be recorded in written form in case the courts must later adjudicate on the proceedings.

An exploration of an accused employee's rights must also include the privileges he does not have. Significantly, the accused does not need to be consulted for documents or any other evidence to be entered into disciplinary proceedings.

Also, an employee can be suspended from work for the duration of the proceedings if the company deems that his presence may adversely affect the investigation. A suspension can be ordered after the Notice of Fault has been issued, and should be recorded in writing. Crucially, even under suspension, an employee is entitled to his full salary.

When collecting evidence for the proceedings, a company can examine an employee's digital communications, but only as a last resort. When accessing employee data, the employer must adhere to all privacy regulations. Employers, for example, cannot download communication lists or control communication records. Instead, employers are only able to analyse the timing and duration of digital communications, and during this examination, the employee who owns the data (or a representative) must be present.

If the company successfully conducts and concludes disciplinary proceedings within the deadlines, it has the right to render sanctions against an employee, so long as the punishment is proportional to the seriousness of the offence and the degree of guilt; no more than one sanction is levied for a single offence; and the sanction is carried out within three months after the final decision is rendered.

But employers should be aware that the Portuguese labour code prohibits punishment it considers abusive, such as sanctions that were handed out against employees who voice legitimate and reasonable complaints about deficient working conditions; who refuse to carry out orders for tasks, which they are not responsible for; who are part of or applying to be part of a company works council or union; or if they have been the victim of assault or a witness to assault in a court action.

For more information on conducting internal investigations in Portugal, contact local CMS experts:

Susana Afonso
Partner, CMS Portugal
E susana.afonso@cms-rpa.com

Tiago de Magalhães
Associate, CMS Portugal
E tiago.magalhaes@cms-rpa.com

Romania

Click to listen to the webinar recording
Published June 2020

Romanian businesses increasingly turn to internal investigations

When establishing the general legal framework for a company's investigation procedures, managers must consider the following general principles: data privacy, confidentiality, anti-discrimination and the obligation to ensure transparency and effective communication channels in regard to any allegation of misconduct by any employee.

A manager that fails to address these general principles could create risks for his company, particularly if the results of an internal investigation are later challenged in court.

In terms of data privacy, all internal investigation procedures must adhere to Romanian data privacy laws and the EU's General Data Protection Regulation (GDPR). To ensure that an investigation does not infringe on the personal rights of any employee, an investigation must adopt a policy of strict confidentiality where the identity of Whistleblowers are protected, evidence is safeguarded, and in the spirit of legal fairness, everyone involved (especially the accused) is treated even-handedly and fully informed about the objective and scope of the investigation.

Note that investigators do not have an obligation to inform the accused and witnesses are not entitled to details on the investigation's charges, evidence or strategy, except where specifically required by law (as further detailed below).

In addition to adopting these principles, Romanian companies should have specific policies in place that clearly define employee inappropriate behaviour and misconduct that could trigger an internal investigation.

Occasionally, company managers will encounter evidence of misconduct by chance, or a wrongdoing will be uncovered during an audit. In most cases, however, a company will learn of a misdemeanour through a "complaint" reported by a member of staff. Such a complaint could concern straight-out misconduct; negligent behaviour in the work place; an allegation of bullying, harassment or fraud; or any breach of company policies in the areas of work safety, employee code of conduct, etc.

Complaints concerning minor issues need not trigger a full-blown investigation, and can be resolved by the appropriate manager in dialogue with the employees involved. Other issues falling short of misconduct can be remedied via administrative or HR measures, such as reassigning certain employees to other offices, modifying company procedures, initiating employee training sessions or advising specific employees on improving communication skills or changing their workplace behaviour.

Conducting internal investigations

For internal investigations that could potentially lead to disciplinary conduct, the Romanian Labour Code sets down specific rules that must be followed. A company must appoint a "disciplinary commission" to investigate the allegation and recommend a disciplinary sanction. Once evidence has been collected, the commission should hold a disciplinary hearing with the accused employee in attendance, providing the employee details in relation to the alleged disciplinary misconduct. During this hearing, the employee should be given the opportunity to present his case and a defence against such allegations.

The Labour Code does not specify deadlines and a time frame for an investigation. However, the law does specify time frames for issuing a disciplinary sanction, which will influence the timing of any investigation. For example, a disciplinary sanction against an employee must be issued no more than 30 calendar days after the company became aware of the misconduct. Furthermore, a disciplinary sanction cannot be issued more than six months after the misconduct was originally committed.

Although Romanian law does not specify details on how to conduct an internal investigation, best practices in Romania offer the following recommendations:

— Before an investigation ever takes place, a company should define in its internal policies what it considers inappropriate behaviour and the disciplinary sanction for this behaviour;

— Ensure all sanctions are consistent with Romanian law;

— Ensure that company procedures on conducting internal investigations include the "mandatory steps" set down in the Labour Code;

— Ensure that investigation procedures are sufficiently flexible (within the boundaries of the Labour Code) to respond to the challenges of a specific case; and

— Ensure that a company's disciplinary commission thoroughly documents the investigation process, retains transcripts of all testimony, and keeps a record of all evidence.

For investigations of poor performance or negligence on the job, companies should ensure that they regularly conduct professional assessments of employees in order to identify any potential problems with employees early. Such assessments are mandatory under the Labour Code, although it gives no details on how the assessments should be conducted.

To fully protect a company's interests, we recommend that prior performance assessments include clear, transparent and fair evaluation criteria that apply directly to an employee's professional responsibilities in accordance with the principles reflected in employment law. (The company's counsel or outside legal experts should be consulted for this).

If an assessment suggests that an employee is performing poorly on the job, the assessment should contain continuous documentation on the employee, including a record of regular feedback on his day-to-day performance and regular reviews conducted on a yearly or quarterly basis.

In line with these assessments, accurate and thorough job descriptions should be compiled for every employee, which should include a list of each worker's professional responsibilities.

In addition, the team conducting the assessments should be carefully selected, and no team member should have a conflict of interest or be perceived as biased.

For other types of investigations, there are no rules mandated by the Labour Code or Romanian law. These inquiries can be conducted according to the company's internal-investigation procedures, which should be carefully established. The exact procedures can vary depending on company policy and culture. But whatever your procedures are, we recommend that they be set down in clearly defined steps understandable to both investigators and employees. These procedures should include thorough documentation so that there is a detailed record of each investigation.

As stated earlier, the investigation should be confidential. Although the process should be transparent, the investigation team should not divulge any information about the details of a probe. Every effort should be made to protect the identity of Whistleblowers. In addition, employment contracts should include confidentiality agreements that apply to any internal investigation an employee may be involved in at the company.

Preparing for a specific investigation

If misconduct has been alleged and an investigation is to be launched, the company should identify all rules and provisions (e.g. laws, internal regulations, provisions specified in an employment agreement) that must be adhered to during the inquiry. With these rules in mind, the company should draft an investigation plan and select an investigation team. Again, team members should be perceived as having no conflicts of interest or biases vis-à-vis the subject matter of the investigation or anyone involved.

Conducting the investigation

Once the plan is drafted and the team assembled, the investigation can get underway. At this time, team members should carefully collect evidence, documenting both it and any other actions that the investigators take during the course of the probe.

Arguably, some of the most important evidence will come from interviews with the accused and witnesses. Personal and data privacy rules should be observed during interviews and detailed minutes of the testimony should be taken.

Employees should not be permitted to make recordings of interviews.

If an investigation team wants to make either an audio or video record of a worker's testimony, the employee must give his consent in writing. Any and all recordings should adhere to the EU's GDPR and Romanian privacy laws.

Internal investigations during lockdown and work from home

The fact that many Romanian companies were locked down during the pandemic with employees working from home raises the question: can an internal investigation be conducted virtually and remotely? The answer is: yes.

Before embarking on a remote investigation, however, a company should consider whether an investigation can be postponed. The ability to collect evidence at a later date and the legal risks of delay should be weighed carefully. If the company decides that the investigation cannot be rescheduled, it must then confirm whether it possesses the appropriate resources to conduct a remote inquiry with the same accuracy and care as a regular probe.

While this assessment is going on, a company can take immediate steps – albeit interim measures – to address the incident, and ensure that staff members are protected and risks to the company are mitigated.

When conducting a remote investigation, a company will have to adjust its procedures accordingly. Interviews, for example, will have to be conducted by video conferencing. (In addition, it's recommended that all video interviews include specific information on their date, time and duration. If any employee refuses to be interviewed in this way, this fact should also be documented).

Also, in order to conduct video interviews, companies will have to get the expressed consent of employees first since this procedure will entail the processing of personal data.

The investigation's conclusion

Whether performed remotely or not, when the investigation is completed, the team must then prepare a report, which documents the probe in detail, listing evidence, testimony, and explaining the team's final conclusions about the initial allegations.

The report should also include any and all details required by the Labour Code, and be reviewed and approved by the company's corporate leadership and compliance officers.

If the accused is deemed to be guilty of wrongdoing, the company must decide whether disciplinary action is warranted. Discipline could include a warning, demotion, reduction of salary rights or termination, depending on the severity of the misconduct.

Lastly, the company should determine whether the misconduct breaks any criminal or corporate laws or violates state regulations (e.g. data privacy, workplace safety, environmental protection), and whether the company is obliged to report the offence to state authorities. (This decision should always be considered in consultation with the company's counsel or outside legal advisors).

For more information on conducting internal investigations in Romania, contact your regular CMS advisor or local CMS experts:

Horia Draghici
Partner, CMS Romania
E horia.draghici@cms-cmno.com

Ruxandra Georgescu
Associate, CMS Romania
E ruxandra.georgescu@cms-cmno.com

Russia

Click to listen to the webinar recording
Published 3 June 2020

Russian business able to implement internal investigations despite no state laws governing it

Although Russian law contains no specific statutory regulations on conducting internal corporate investigations, these types of inquiries are common in the Russian business sector with the framework borrowed indirectly from other statutes such as employment law, criminal law, and best practices currently being used in the corporate sector.

Like many other countries in the world, Russian businesses are able to protect employees, assets, brands and reputations by responding immediately to any reports of misconduct with effective investigatory procedures.

Generally, the procedures practiced in Russian business apply to incidences of misconduct that include violations of federal law, violations of internal corporate regulations, fraudulent employment law claims, discrimination in the work place, and – quite rarely in Russia – charges of harassment.

Although Russian companies are not required to create policies and procedures on internal investigations, businesses can adopt them and doing so is highly advisable. Establishing and entrenching policies on internal investigations can send an important signal to staff regarding their conduct and the penalties that might occur for inappropriate behaviour.

To this end, it is also highly advisable to make it absolutely transparent to employees what acceptable and non-acceptable behaviour is by establishing a well-advertised "Code of Conduct" in the company's compliance policies. Having such a code in place will make it far easier to launch an investigation and issue penalties should the investigation reveal any wrongdoing.

Although it is not common, some Russian companies have Whistleblower hotlines in place through which employees can report allegations of misconduct, explains lawyer Valery Fedoreev, a Partner with CMS Russia. But because these hotlines are a rarity, most complaints in the Russian business sector originate as written statements sent to management.

If such a letter is received, a Russian manager should immediately define the scope of the allegation, answering the following questions: what precisely is the complaint? Who is the target? What are its ramifications?

If the complaint is related to a violation of the company's compliance policies, note that some internal corporate policies are not backed up by federal legislation. For example, many Russian companies receive complaints that former employees have violated the non-compete clauses of contacts after leaving the company. Because Russian law does not recognise non-compete clauses in contracts, little can be done in this situation.

In terms of investigators, the manager must immediately assemble an *ad hoc* team to follow up the complaint, and a chief investigator to oversee the team's activities. According to CMS's Fedoreev, a team usually contains officials from the following departments: compliance, HR and a lawyer from the counsel's office. Depending on the dynamics of the case, a manager may opt to choose outside investigators, such as a law firm specialising in compliance and labour law.

When the investigation gets under way, it is vital – further to the formalities of Russian law – that the company officially issues an internal order on initiation of an investigation. (This order need not be announced, but for official bureaucratic reasons it should be generated.)

Once the declaration is made and the investigatory team is assembled, the investigators will want to inspect all pertinent documentary evidence, and will make a quick assessment on where to obtain this information. When inspecting company documents, it is essential that the investigation team have a system in place to store and protect this data.

In order to scan messages and various documentation, it is possible in Russia to take possession of an employee's work laptop for inspection. When scanning the business emails and messages stored on an employee's computer, it is essential to avoid any personal communications that may be stored there. If personal files are found on the computer, however, these can be reviewed if the company's internal policies prohibit the use of business equipment for personal reasons.

When liaising with employees during the investigation – particularly, when conducting interviews – it is important that investigators not reveal the scope or target of the investigation. If a complaint was lodged by a whistleblower, his identity must be protected.

Depending on the severity of the allegation, the investigatory team may also want to remove the target of the investigation from the work environment to stop the misconduct, prevent evidence manipulation or the ability of the accused to intimidate witnesses. Some countries recognise the concept of "garden leave", which enables a company to send an employee home without notice for the duration of an investigation so long as he is being paid his full salary. Garden leave is not recognised in Russian law. Therefore, employers in Russia should use other legal ways to remove an employee from the work place. However, most require employee consent.

After messages and pertinent documents have been reviewed, the interview stage of the investigation should begin. It is recommended that all interviews are conducted outside of the office since this will minimise the likelihood of employees sharing information.

Prior to every interview, the employee is usually informed about the purpose of the interview, but he is not entitled to receive details of the investigation. The questions for each employee (e.g. the target of the investigation and pertinent witnesses) should be carefully drafted ahead of time. Interviews should be conducted in a sharp Question & Answer format and detailed written notes of the proceedings should be taken, which the employee should later review and sign as a confirmation of the transcript's accuracy. Having a detailed record of the interviews will make it impossible for employees to change their testimony at a later date and will support the company in any disciplinary action taken after the investigation is complete.

It is also recommended that interviews be recorded either by audio or audiovisual means. Having such records will also serve the company well during the disciplinary stage when it is necessary to justify any sanctions that have been handed out. Audiovisual recordings, however, cannot be conducted without an employee's consent.

Interviewers should take great care about what they say to employees about the investigation and any outcomes during questioning since the subject could later use these comments against the employer in court.

After the documentary evidence has been collected and the interviews conducted, the investigatory team will come to a conclusion, and will determine whether the allegation is backed up by evidence or not. The team can file a report in Russian (and English as well, if the company is foreign owned) that outlines the investigation's findings. The report or protocol should be signed and certified by all members of the investigatory team and all the evidence collected should be safely stored away in case the investigation's findings are later challenged.

This final report should not be shared with employees, and all evidence should be guarded and considered highly confidential.

If the investigation determined that the allegation was not confirmed, the team must try to decide why this happened. Was the allegation the result of a misunderstanding that can be rectified by staff training, coaching or some procedural change? The team may also determine that the Whistleblower knowingly filed a false claim in order to further a personal agenda. (The Whistleblower could be facing termination for a variety of reasons and filed the complaint to gain leverage in severance negotiations). If the

company decides that the Whistleblower's complaint was false and was issued with malicious intent, disciplinary liable actions may be brought against him if the Whistleblower's conduct is considered a disciplinary violation under the company's policies.

A company wanting to terminate a Whistleblower for making a false allegation faces difficulties since Russian law prohibits the firing of a Whistleblower for filing an unconfirmed complaint. In this case, a company would need to use the mutual agreement as grounds for dismissal, subject to the consent of the Whistleblower.

Upon the results of a compliance investigation, an employer can take other types of actions against an employee who is found to be at fault. If the employee's misconduct is a violation of Russian criminal law, a company can initiate proceedings against the individual. Such a course can be taken if the investigation uncovers evidence of bribery (especially relating to a state tender and commercial bribery), fraud, extreme abuse of managerial influence (i.e. causing damage to the company) and a violation of Russia's anti-monopoly statutes.

Note that bribery is considered a serious crime in Russia carrying penalties (depending on the severity) of up to 15 years in jail and fines of up to 70 times the amount used in the bribe. What constitutes a bribe? Currently, any gift to a state official greater than RUB 3000 (EUR 20) is prohibited. And if a state official tries to canvas a bribe from a company employee, Russian authorities have set up a Whistleblower hotline where this can be reported and where immunity is available in exchange for cooperation.

Because Russian authorities are now focused on uprooting corruption in the business sector, companies are advised to report any criminal activity they uncover to authorities. Doing so will insulate the company from any liability stemming from the misconduct.

For lesser misdeeds that fall short of criminal activity, a company can issue a reprimand or a simple warning. Whatever the disciplinary measure, however, the company must follow

an implementation procedure and be careful to respect all deadlines. (Otherwise, the measures could be challenged later in court.)

The sanction against the employee, for example, must be handed out no later than one month after the company learned of the misconduct (i.e. after the investigation team officially issued its findings.) There is a statute of limitations on misconduct: six months in general cases (e.g. for complaints lodged by a Whistleblower) and two years for violations uncovered in audits.

For investigation findings and judgments to be unassailable in court, they must be backed up with solid documentary evidence. And the grounds for the violation must be a contravention of established company policy that is (in the case of foreign-owned companies) translated into Russian and made known to all Russian employees, which they can confirm with a signature. The misconduct can also be a breach of an employee's "fixed" and stated job duty, which would create an opportunity for a "disciplinary dismissal" should the misconduct be deemed a "gross violation", such as the sharing of trade secrets.

For moderate breaches, however, disciplinary dismissals are almost always a last resort after warnings have been issued since these dismissals, which can make it difficult for the employee to find another job, are often challenged in court.

After the investigation's findings have been released, the employee must be given an opportunity to respond with a written explanation that should be received within two days after the report is completed.

The disciplinary measures a company issues is more likely to stand up to judicial scrutiny if it is measured and fair, based on an evaluation of the severity of the misconduct and takes the employee's previous conduct at the firm into account.

Lastly, the company's HR department should issue the penalty by an internal order, which should be officially confirmed by the employee with a signature. (An actual "wet" signature is a must; not a digital one.)

Other considerations when launching an internal investigation in Russia include: Russia has no Whistleblower protection laws (other than regulations that protect witnesses in criminal proceedings), although a company should do everything possible to protect a whistleblowers identity during an investigation; companies are under no legal obligation to inform the company's trade union of an investigation; and a company is also under no obligation to inform government authorities of an investigation or its results unless a state law has been violated.

For more information on conducting internal investigations in Russia, contact your regular CMS advisor or local CMS experts:

Valery Fedoreev
Partner, CMS Russia
E valery.fedoreev@cmslegal.com

Ekaterina Elekchyan
Senior Associate, CMS Russia
E ekaterina.elekchyan@cmslegal.com

Singapore

Click to listen to the webinar recording
Published June 2020

Best Practices in HR Internal Investigations

The months of March, April and May 2020 have seen most businesses in Singapore adopting remote-working or telecommuting as the "new normal". While the Singapore government recently announced that "circuit breaker" measures in the country end on 2 June 2020, the Ministry of Manpower has emphasised that employees should continuing working from home even after that date for the foreseeable future.

Even with such a large number of employees working remotely, employers continue to be exposed to the risks of misconduct in the workplace. We take a brief look at two common scenarios requiring internal investigations – workplace harassment and "whistleblower" complaints – and examine some of the best practices your organisation can adopt when conducting an internal investigation.

Workplace harassment

Workplace harassment has come to the forefront of most employers' minds in light of the global #MeToo movement, which has highlighted the prevalence of sexual harassment in the workplace and led to the fall from grace of many senior and top management executives found guilty of unprofessional conduct.

A recent study conducted in 2019 saw Singapore ranked in the second-lowest spot out of 14 countries for workplace inclusivity with 24% of workers reporting being bullied during the previous year. The survey was aimed at helping organisations understand where greater effort should be made to make workplaces more inclusive and equal.

Workplace harassment can occur in different forms and in different degrees. Broadly speaking, workplace harassment occurs when one party in the workplace demonstrates behaviour that causes or is likely to cause harassment, alarm or distress to another party. Such behaviour can violate a person's dignity or create an unfavourable work environment, posing a risk to the person's safety, health and well-being.

Workplace harassment can take place through different modes of communications, such as email, text messaging or social media. As such, even if employees continue to work from home, they remain susceptible to workplace harassment, albeit remotely. It is not uncommon for workplace harassment to occur outside of the office space, such as on business trips, company-organised events, client premises or during other work-related occasions.

The Ministry of Manpower (MOM) in Singapore has provided examples of behaviour that may be considered harassment, which include (but are not limited to) the following:

— Threatening, abusive, or insulting language, comments or other non-verbal gestures;

— Cyber bullying;

— Sexual harassment; and

— Stalking.

Harassment in and outside the workplace is an offence under the Protection from Harassment Act (POHA). POHA protects individuals from harassment and related anti-social behaviour through criminal sanctions, and also provides a range of self-help measures and civil remedies for victims of harassment.

Whistleblowing

Over the past few years, the spotlight has been shone on whistleblowing in Singapore with scandals rocking major industry players implicated in corruption and graft worth billions of dollars. Such cases raise important questions about whether whistleblower complaints are being properly dealt with in a country otherwise regarded as largely corruption-free.

Whistleblowing refers to an act where an employee exposes information on wrongdoing and misconduct to his employer. This misconduct can range from financial malfeasance or corruption to regulatory non-compliance, such as non-compliance with MOM regulations aimed at curtailing the spread of COVID-19 transmission in the workplace.

On a general level, Singapore law does not impose any statutory or regulatory requirements on how a whistleblower's complaint is to be assessed. Nor does it provide protections for whistleblowers. However, in the specific context of a complaint dealing with anti-bribery or corruption, the Prevention of Corruption Act provides that no complaints regarding a corruption offence can be admitted as evidence in any civil or criminal proceedings and no witness to any civil or criminal proceedings will be obliged or permitted to disclose the name or address of any informant or state any matter, which may lead to the informant's discovery.

Employer Do's and Don'ts during internal investigations

Do's

One of the key things an employer should do is to have a written internal investigation plan that sets out clearly and concisely what needs to be done in the event of an internal investigation. The investigation plan should be easily accessible to the staff who will be conducting investigations.

The sections of the investigation plan to be adopted in a particular situation will largely depend on the specific facts of a case. However, some common steps include data collection, evidence preservation, document review, compliance with internal protocols relating to investigations, coordination with external service providers, communication with law enforcement agencies, witness interviews and taking statements.

During the data-collection and evidence-preservation process, it is important to consider data privacy and banking secrecy laws in jurisdictions where documents may be located. This can impact whether the documents and their contents can be transferred between countries. It is also important to consider whether dealing with documents stored in other jurisdictions will have any impact on ongoing or potential investigations by local law enforcement agencies in those jurisdictions.

Email correspondence and messages exchanged on instant messaging platforms are increasingly regarded as key types of documentary evidence for internal investigations. As investigations may involve allegations of false or manipulated documentation, it is important to retain "soft" or digital copies of relevant documents so that metadata information and properties can be examined.

Don'ts

One common pitfall that employers may commit in the rush to conclude an investigation is to conduct an inquiry without transparency and then terminate an employee based solely on the findings of such an internal investigation. Even though the statutes and regulations in Singapore do not prescribe a fixed procedure for internal investigations, MOM has advised that as a general guide the following principles should be adopted:

— Firstly, the employee under investigation should be told of his alleged misconduct.

— Secondly, the employee should be given the opportunity to present his case.

— Thirdly, the person or persons hearing the inquiry should not be in a position, which suggests bias.

Another common pitfall relates to informal record-keeping. The more informal the process of an inquiry, the more likely it will be that the local courts will decide that a "due inquiry" has not been undertaken.

Some of the things that a prudent employer could do include:

— keep contemporaneous written records of the investigation, including witness statements that should be signed by an employee after an interview; and

— ensure that a letter of termination (if it comes to that) clearly states all the reasons for the employee's dismissal and also that a formal inquiry had been undertaken by the organisation.

Matters that employees should note during internal investigations

Employees should carefully review internal policies and guidelines and the terms of their employment contract to fully understand their rights and obligations. While Singapore law doesn't impose specific obligations on an employee to cooperate with an internal investigation, depending on the terms of their employment contract his non-participation may amount to a disciplinary breach, which could potentially provide grounds for termination.

Employees should note that while there is no legal obligation for an employer to arrange for an employee to have legal representation during an investigation interview, an employee should not be prevented from seeking legal advice before signing off on any statements or agreements.

Best practices for organisations

The following are some (non-exhaustive) best practices organisations can consider adopting:

— Employers should develop formal policies, which prohibit harassment and encourage whistleblowing if they are not already in place. These policies should, among other things, ensure recourse in the case of harassment and ensure confidentiality and protection in the case of whistleblowing.

— An organisation's policies should take into account the actual situation on the ground. It is recommended that organisations develop their policies in consultation with a committee of employees and their trade union (if any).

— Harassment prevention and whistleblowing policies are key corporate governance documents, which should be communicated clearly to all levels of the organisation. The management of an organisation should discuss and reinforce these messages regularly at staff meetings or training sessions to demonstrate its commitment to upholding these policies.

— Employers should create a safe environment for reporting and ensure that whistleblowers or those suffering from workplace harassment will not be penalized by, for example:

  - Creating multiple reporting channels, which can include a higher authority or a neutral party within the organisation if the harasser or subject of the whistleblowing complaint happens to be the victim's immediate supervisor or manager; and
  - Setting up anonymous whistleblowing mechanisms, which will allow employees to report grievances without being identified, such as external hotlines as an additional channel for employees to make reports.

— Organisations should ensure transparency throughout the process of the investigation (e.g. regarding timelines, updates on progress, providing an avenue for appeal) until the closure of each case. Proper closure of a harassment incident or whistleblower complaint can help prevent recurrence. It is particularly important to ensure that the parties investigated do not repeat the misconduct if they continue to work in the organisation.

For more information on conducting internal investigations in Singapore, contact your regular CMS advisor or local CMS experts

Wei Ming Tan
Senior Associate, CMS Singapore
E weiming.tan@cms-holbornasia.com

Pradeep Nair
Associate, CMS Singapore
E pradeep.nair@cms-holbornasia.com

Slovakia

Click to listen to the webinar recording
Published 25 May 2020

Slovak business embraces internal investigations

Like most countries in the EU, more and more Slovakian businesses are adopting internal regulation policies in order to encourage employees to comply with both the law and company regulations while on the job.

When should an employer seek to initiate an internal investigation? The short answer is: whenever evidence arises that a company's interests and compliance may be at risk through the actions of an employee or manager.

Slovakian companies have options at their disposal on how to manage an investigation. But every investigation must balance the company's clear interests in protecting its assets and reputation and the employee's right to personal and data privacy. Regulations protecting the personal and data rights of employees include the Slovak Constitution, the Labour Code and the EU's General Data Protection Regulation.

Companies that do not take sufficient care in respecting employee rights place themselves at risk of future court or administrative proceedings for infringing key laws. (See the Appeals section of this article).

Regarding investigations, it should be noted that different statutes protect employees and executives. Where the Slovak Labour Code offers safeguards to employees, its protections do not apply to executive directors, Board Members and Supervisory Board Members.

With this in mind, this article will focus on employee investigations only.

When investigating employees, companies can use the following techniques to collect evidence: inspect an employees digital messages, emails and files stored on company devices; interview the target of the investigation along with witnesses; and depending on the circumstances, use assorted other methods such as inspecting video should the workplace be equipped with Close Circuit Television.

As stated, the two legal sources that regulate the privacy aspects of the collection of evidence are the EU's GDPR and the Slovak Labour Code.

GDPR

Regarding the former, investigators must take great care to avoid data protection breaches when carrying out the investigation. Before commencing the investigation, investigators should review the GDPR (2016/679) and ensure that they comply fully throughout the whole process.

Furthermore, before conducting any monitoring, the company's investigation's team – working in cooperation with the company's data protection officer, if there is one – should conduct a data protection impact assessment in order to be sure that any data searches conducted within the company does not result in high risk to the rights and freedoms of the investigated persons, and if so, to mitigate this risk.

A company can prepare for an internal investigation by establishing clear policies on whether employees are permitted to use company devices, such as laptops and phones, for personal use (e.g. sending and receiving personal email).

Labour Code

The Labour Code also sets important limitations on the use of surveillance and monitoring as a means of collecting evidence in an investigation. According to Slovak labour law, employee monitoring can only be done if there is a serious reason pertaining to the specific nature of the employer's activities.

If this criterion is met and monitoring is deemed necessary, the employee must be notified in advance. Implementation of any monitoring mechanism must be done in consultation with the employee representatives (e.g. trade union, works council or employee trustee) representing the company's workers in regard to the manner, scope and duration of the surveillance. This information must also be provided to employees.

In terms of employee rights, a company must also consider how it received information about a case of possible misconduct. Some allegations of misconduct are the result of a chance finding or audit. If another employee leveled an allegation, however, then legal protocols regarding whistleblowing must be followed.

Whistleblowing regulations

Currently, Slovakia regulates whistleblowing through a law that came into force on 1 March 2019: the Act on the Protection of Whistleblowers (Act No. 54/2019 Coll.). This act, which replaced the former Act on Some Measures Related to the Reporting of Ant-Social Activities, provides increased protection for whistleblowers, establishes specific obligations for employers and created a special Office for Whistleblowers' Protection to safeguard these protections.

The Office for Whistleblowers' Protection, however, is not yet fully functional. During the transition period, the competent labour inspectorates, which were the competent authorities under the former legislation, and the Ministry of Justice, in respect to the payout of rewards, will perform the office's duties.

This law obliges companies to ensure the protection of the reporting person (whistleblower) and also people close to and working alongside the whistleblower who may be placed at risk through a report. In addition, the law also defines the types of misconduct that a whistleblower may report. Individuals are not limited to reporting crimes. If someone witnesses an offence or negligence that could have a negative impact on society, he can make a report and receive protection under the Act.

As an incentive, whistleblowers who file reports can receive a reward under certain conditions. If requested, the Ministry of Justice may provide the whistleblower who has submitted a qualified report a reward equaling up to 50 times the current minimum wage.

Whistleblowers are generally protected against the adverse actions of employers. Therefore, if the whistleblower is receiving protection in criminal or administrative proceedings and the company performs a legal act or issues a decision towards him that the employee does not agree with, the labour inspectorate must give its prior consent for this act or decision to be enforced. If no consent is given, the act is deemed void.

If protection is not granted to a whistleblower either in criminal or administrative proceedings because he submitted only an "ordinary" report, the whistleblower can request that the labour inspectorate suspend those effects of the labour law act made against him with which he does not agree.

What are the main obligations of employers? Companies with 50 employees or more must have investigation procedures and conditions for internal reporting in place (which is also strongly advised for companies with fewer than 50 employees), including an internal system of report verification and the appointment of an official who is responsible for overseeing any inquiry or report. Also, one of the channels for submitting reports must be available to employees on a 24/7 basis. Many companies have dedicated hotlines or email addresses people can file reports to quickly and securely.

Investigation procedures can vary from company to company, depending on the operations and corporate culture of each enterprise. According to Slovak law, all reports of misconduct must be investigated within 90 days of the report being made. At the conclusion of the investigation, the whistleblower must be notified about its findings.

Throughout this process, it is vitally important that the identity of the whistleblower remain confidential.

Collecting evidence

Before officially launching the inquiry, the company should also determine if evidence – for example, digital or hard records – may be in jeopardy due to the close proximity of the investigation's target. If there is any fear that

the suspect could tamper with evidence, he can be asked to hand over his company devices, and be removed from the work place by being assigned paid leave, either in the form of work suspension or garden leave, whereby he is asked to avoid the workplace and remain at home until further notice. Work suspension may be utilised if there is a reasonable suspicion of serious breach of labour discipline. In such cases, the employee is entitled to receive at least 60% of his average earnings. The rest must be paid out if the suspicion is not confirmed. Garden leave requires the employee to receive 100% of his average earnings.

Interviews

The testimony of the accused and any witnesses is gathered through interviews. Exactly how an interview should be conducted is not specified in Slovak law, but the most effective procedure is to invite the subjects into an interview room where they will be questioned by an investigator.

It is recommended that investigators take minutes of the interview and have them reviewed and signed by the interviewee at its conclusion.

Investigators cannot make an audio or video record of the interview without the expressed consent of the subject.

Inspecting company-owned devices

Investigators can also perform searches of company email and messaging systems. When reviewing digital communications, however, investigators must take care to distinguish between business mail and personal messages and avoid opening and reading the latter.

Investigators can identify personal email, for example, by inspecting the subject line, the email address of the recipient (i.e. addresses based on popular services such as yahoo, Gmail, etc. are likely to contain personal information), and the salutation used.

The hard drives of company-owned laptops and desktop computers can also be inspected, but again investigators must take care not to open personal files stored on these devices.

As stated, the process of distinguishing between personal and business files and communications

is easier in companies that have strict policies on personal use of company devices.

Final investigation protocol

When all the evidence has been collected, the company has the option of drafting a final report or protocol. Slovak law does not require that a protocol be issued, but the existence of a final report may be crucially useful should the investigation's findings be challenged in court later.

Whether or not a protocol is drafted, the whistleblower must be informed of the investigation's findings within ten days after the investigation's conclusion.

Disciplinary action

If an investigation concludes that an employee is liable for wrongdoing, a Slovak company can respond with disciplinary action. If the employee has been found liable for financial losses to the company, the company can request that the employee pay damages, although the Slovak Labour Code places restrictions on this.

In terms of discipline, a company can issue a warning letter for breach of labour discipline. Serious breaches may call for the employee to be immediately terminated, which again must be carried out in line with Slovak Labour Code requirements.

Lastly, if the investigation uncovers evidence of a crime, the company may be obliged to notify Slovak law-enforcement authorities. For its own protection, a company is advised to seek the advice of its counsel or outside lawyers to be sure that the wrongdoing meets the threshold of criminal activity and must be reported.

Appeals

In most instances, the investigation stops at this point since Slovak law does not specify an appeal process for findings of this nature.

An employee who believes that Labour Code dictates were violated during the investigation can file an official complaint with the Labour Inspectorate. If the employee believes that his personal data was violated in the collection of evidence, he can issue a complaint with Slovakia's Office for Personal Data Protection.

In addition, the employee can go to court with legal action if he believes he was unlawfully terminated or endured personal or professional harm during the investigation and seek the appropriate remedy.

Be prepared: a checklist

In review, to protect itself against such liabilities, a company should be prepared by putting in place internal investigation and whistleblowing procedures before any allegation is made, and to ensure that these polices follow all applicable Slovak and EU laws.

Companies should also set down policies on the use of company devices for personal use.

Companies should clearly communicate these policies and procedures to all employees.

When an allegation surfaces, the company and the appointed investigation's official should conduct a test to determine whether an internal investigation can be conducted in such a way that does not violate the accused personal privacy rights or data-protection rights.

In short, preparation, communication with employees, and the creation of in-house systems for reporting abuse and investigating it can protect both a Slovakian company and its employees should an internal investigation be necessary.

For more information on conducting internal investigations in Slovakia, contact your regular CMS advisor or local CMS experts:

Martina Šímová
Senior Associate, CMS Slovakia
E martina.simova@cms-cmno.com

Dominika Mislovičová
Lawyer, CMS Slovakia
E dominika.mislovicova@cms-cmno.com

Slovenia

Click to listen to the webinar recording
Published 17 February 2020

Investigation Procedures and the impact of the Whistleblowing Directive

As the new legal buzzword "whistleblowing" echoes in political and business circles and the December 2021 deadline for the transposition of the EU's Whistleblowing Directive into national law, the Slovenian lawmakers have revealed little information on what details and novelties the upcoming Whistleblowing legislation will contain.

Internal investigation procedures in absence of whistleblowing legislation

In the absence of legislation specifically dealing with whistleblowers, the employers may resort to establishing internal investigation procedures. Legal compliance for such investigations is crucial. The key pieces of Slovenian regulation that must be taken into account when setting up these kinds of procedures are: the *Employment Relationship Act*, *Health and Safety Work Act*, data protection laws, and the *Private Security Act*.

Until a dedicated whistleblower act is passed in Slovenia, these regulations – with an eye on key judgments in local case law – provide local businesses with a solid direction on how to put systems in place that protect employees from abuse and safeguard firms from the legal risks inherent in violating employee rights. Even when the respective procedures based on the Whistleblowing Directive are adopted into Slovenian law, general rules regarding internal investigations will still apply.

Key considerations for drafting internal investigation procedures

The first step before introducing internal investigations should be the adoption of an internal by-law. Before finalising these procedures, the employers should make sure they adopt the by-laws in line with statutory requirements, which also require the involvement of worker representative bodies.

Once established, all personnel should be made aware of these systems and should be able to acquaint themselves with these company by-laws at any time. Full transparency protects both the employees and the company.

What priorities should be followed when drafting these procedures?

The procedure should be:

— transparent;

— timely and efficient;

— pursuing a legitimate purpose; and

— proportionate to the alleged violations.

First and foremost, companies must conduct investigations that do not violate employee privacy at various levels, including data protection (i.e. procedures must respect Slovenian data protection legislation and the GDPR), the physical integrity of an employee's body, personal communications and private property.

By-laws addressing workplace harassment

Sexual abuse in the workplace falls under the auspices of Article 47 of the *Employee Relationship Act*, which not only outlaws sexual harassment in the workplace, but requires employers to create a working environment that protects employees from all types of harassment or abuse. One of the best practices for doing this is to adopt systems or by-laws that list examples of prohibited behaviour (e.g. sexual overtures, bullying, threats, gossip) and the

measures that have been put in place to ensure that the established rules are also carried out in practice (e.g. dissemination of harassment by-laws to all personnel, in-house training on correct conduct, and HR campaigns aimed at creating a healthy work environment).

Employers should also take into account the Slovenian Health and Safety Work Act when drafting these by-laws, which should contain measures to expose and punish anyone guilty of harassment and systems to protect victims. Once the Whistleblowing Directive is implemented, employers will have to adopt specific procedures for whistleblowers. One of the fundamental principles should be that no employee face retribution from the company or colleagues for reporting wrongdoing.

Generally, employees must be fully apprised of what to do in these situations. Firstly, if they experience workplace harassment, they should first try to resolve the wrongdoing themselves. (Some minor abuses may represent one-time behaviour that can be corrected if pointed out.) If this fails, the employee should report the abuse and together with the employer follow the established internal procedures.

By-laws regarding internal investigation procedures may also include creation of an investigation commission, consisting of independent members whose job is to respond to allegations and lead an inquiry. Procedures could also include some guidance that victims can adopt to aid an investigation, such as keeping a diary of any harassment or wrongdoings they encounter.

Investigation Techniques: dos and don'ts

The primary method for resolving a contentious situation and determining whether the allegations are founded is to conduct interviews with the subject of the investigation, the complainant and witnesses. Generally, an employee must participate in these interviews, which is in line with the basic legal requirement that employees follow the instructions of their

employers. It is advisable that detailed minutes of each interview are made, reviewed, approved and signed by the participants.

Other investigatory techniques face important restrictions.

Monitoring and scanning of emails are heavily regulated by Slovenian data protection and privacy of communication laws, and are permitted only in exceptional situations when no other recourse is available to achieve the pursued purpose and the protection of employer rights overrides an employee's right to privacy (i.e. the proportionality principle).

Companies, however, should be aware that because the Slovenian Constitution and the Criminal Code protect the privacy of email correspondence, violations of this protection could constitute a criminal act in the violation of secrecy of letters. Great care is advised when considering this course of action.

Phone taps are generally prohibited. Searches of an employee's personal property represent a severe intervention in a person's right to privacy and are likely to constitute a disproportional measure. We therefore advise employers not to carry out this kind of measure. A direct inspection of an employee by the employer is generally forbidden even if the employee gives his consent for an inspection. However, "pat downs" are possible if executed by the security guards in accordance with the *Private Security Act*.

A job site can be placed under ***video surveillance***, but only if the aim cannot be achieved by other means and is necessary to ensure people safety and protect property, classified information and commercial secrets. Employees must be given prior notice and the representative trade unions have to be consulted prior to its commencement. Video surveillance of certain locations such as change rooms, elevators and bathroom and shower facilities is banned outright.

Once all evidence has been collected, companies should render a decision in writing and inform the subjects involved.

Consequences of internal investigation procedures

A decision can result in disciplinary action or the outright termination of a staff member. In cases of employee termination, companies can protect themselves from subsequent court challenges by ensuring they adhered to all established procedures, that these procedures were well known and transparent among employees, and that the firm took care to record in writing the initial allegation, all interviews and the final report.

These considerations should also be taken into account, even after Slovenia implements the Whistleblowing Directive, which it is obliged to do by 17 December 2021. A close examination of the text of the directive will give employers a solid idea of what any future legislation will look like. Employers are highly advised to include key principles of this directive in their internal by-laws as long as these systems are consistent with the Slovenian legislation described in this article.

For more information on establishing internal investigation procedures in your company and how to best protect yourself in these circumstances, contact your regular CMS advisor or local CMS experts:

Amela Žrt
Senior Associate, CMS Slovenia
E amela.zrt@cms-rrh.com

Lučka Brunec
Associate, CMS Slovenia
E lucka.brunec@cms-rrh.com

Spain

Click to listen to the webinar recording
Published 25 May 2020

Spanish companies must balance data-privacy and CBA agreements when conducting internal investigations

In the Spanish corporate world, internal investigations are largely conducted to investigate the following types of misconduct: discrimination, harassment, violations of internal policies and criminal activity.

The scope and target of a Spanish investigation, however, greatly depends on the details of whatever collective bargaining agreement (CBA) the Spanish company applies since some agreements contain clauses that directly address internal investigations, and detail the obligations of employees throughout the process.

In short, if a Spanish company is operating under a CBA that specifies the procedures for an internal investigation and establishes a clear definition of misconduct in the workplace, a company must follow this process if faced with reports of misconduct.

If the company's CBA contains no mention of investigations, its management is free to establish investigative procedures that best suit the firm's profile. But all investigations in Spain operate under certain limitations: the details of the CBA as it pertains to employee rights (as just mentioned), personal data protection regulations centred around the EU's General Data Protection Regulation (GDPR), pertinent laws governing gender equity and labour relations and legal protections for personal rights and freedoms.

Investigatory procedures: an overview

In terms of Spanish employment law, companies are advised to implement the following procedures when launching an internal investigation. Details will be provided later in this article, but the following is a rundown.

After receiving a formal complaint of wrongdoing (or if an in-house audit reveals malfeasance), the firm should respond by initiating an internal investigation. Basically, the first thing to be done once the investigation is underway is to initiate protective measures: identify and protect possible evidence, and insure that key witnesses do not become the target of harassment or intimidation.

To do this, the suspect or affected employee alleged to have committed the wrongdoing may need to be removed from the workplace until the investigation is completed. One tool to do this is a furlough called "garden leave" where an employee can be ordered to remain at home while receiving a full salary. (More on garden leave later).

Once protective measures are in place, investigators have several ways to collect evidence and determine the accuracy of a complaint. They can conduct interviews, review documents (both hardcopy and digital records), and inspect communication records (phone, text messages and emails). After all the pertinent individuals (experts, suspects and witnesses) have been questioned and all records and documents inspected, the investigators are ready to arrive at a conclusion whether the evidence proves that a wrongdoing has taken place.

If there is sufficient evidence to prove misconduct, the company will have to respond. The first response should be to implement "corrective measures" to try to prevent this type of wrongdoing from occurring again. In cases where the wrongdoing is minor, this correction and a warning to the investigation's target may

suffice in resolving the issue. For more serious cases, punishment will have to be meted out.

Although it is advisable in terms of protecting an employee's rights and the company's interests to respond to allegations of misconduct with a disciplined internal investigation, there is no law in Spain obliging a company to have internal-investigation procedures in place.

If a company does establish procedures for internal investigations, it should ensure that they are followed to the letter if an investigation is ever conducted. It should be noted that any company with internal-investigation policies in place that punishes an employee for misconduct without following its own procedures stands the risk of having these sanctions later challenged in court and declared unfair.

Whistleblowing

Another crucial consideration is Whistleblowing. Spanish companies are currently not required to have Whistleblowing systems in place, such as a hotline, a Whistleblowing commissioner and policies that encourage employees to use this channel to report misconduct with assurances that all reports will be confidential. This legislative vacuum, however, will not last for long. As a result of EU's recently passed Whistleblowing Directive (2019/1937), member states like Spain are required to pass their own national legislation on Whistleblowing by December 2021.

Even before this deadline, companies should implement their own Whistleblowing procedures in order to reduce the criminal liability of its directors, advises Maria Jose Ramos, an Associate Lawyer with CMS Spain.

According to Ramos, if a company decides to establish procedures for internal investigations and Whistleblowing, it is obliged to consult with employee representatives or labour unions before finalising its policies. Employee representatives views should also be sought out before drafting a company Code of Conduct, and once formalised, employees should be trained on how to adhere to these regulations and what to do should they witness infringements.

In terms of consultation and employee rights, a company is not obliged to inform an employee's legal representative should he become the target of an investigation, unless the applicable collective bargaining agreement requires it. However, if an employee under investigation requests the presence of an employee representative during any investigation-related interviews, it is advisable – for the sake of fair play – to consent. Lastly, if an investigation uncovers a serious infringement by an employee that is a member of a trade union, the company should consult with the employee's union before handing down an official judgment.

Spanish companies are under no obligation to inform state labour authorities of an internal investigation they are conducting. If the investigation, however, uncovers criminal activity, the firm could inform the police or prosecutors.

Lastly, as touched upon above, it may be prudent to remove an employee under investigation from the workplace until the inquiry is concluded. This will diminish the risk of evidence tampering and witness intimidation. Under Spanish law, such a removal can be done easily and effectively by granting "garden leave" whereby an employee is asked to remain at home on call to provide answers to the investigators while receiving a full salary.

Conducting interviews

In any internal investigation, the most important method of collecting evidence is the interview process. This allows investigators to directly question the suspect and all witnesses. Spanish law includes deadlines for the completion of an investigation so that every employee under investigation is guaranteed speedy justice. (These deadlines are explained in detail at the end of the article.)

As for interviews, the questions asked and the information collected must be considered highly confidential. To protect the security of the interview process, interviews can be strategically scheduled to reduce the possibility of leaks of information.

Interviews cannot be recorded by audio or audio-visual means unless the employee gives his explicit consent. But a written record (i.e. minutes) of the interview should be produced. This record or formal protocol should be shown to the interview subject, and ultimately signed by him to confirm the accuracy of the transcript. All interview transcripts (along with all the evidence gathered in the investigation) should be retained and stored by an HR official or relevant manager for later reference.

The primary consideration, when conducting interviews, is to ensure that the fundamental rights of employees are not violated. Interviews should not be overly aggressive, punitive or designed to intimidate. Interviews are straightforward and highly effective fact-finding tools, and should be treated as such.

Interviews, however, must be structured according to the legal status of the individual to be questioned. When interviewing employees, investigators must consider and follow the firm's policies and all applicable labour code regulations, and if issuing sanctions against an employee, the company must respect any limitations present in the CBA.

Contract employees, however, are another matter. Although technically they are not subject to the same disciplinary actions as regular employees, a contactor – who is the target of an investigation – may claim the same rights and protections as an employee if he follows the same routine as regular employees: keeping regular office hours, reporting to a manager, etc. To avoid this, a company is advised not to initiate a standard internal investigation if it involves a contractor. Any potential misconduct should be investigated, but different procedures may be applied to ensure that the contractor cannot claim the status of an employee.

Data collection

When collecting evidence outside of the interview process, investigators can access "company resources" such as company phones, email servers and the Internet history of company laptops. Further to EU and Spanish data-protection laws, investigators cannot read private emails or search the contents of an employee's personal phone.

Investigation protocol

When the evidence has been collected and considered, the investigation team is obliged to issue a report or protocol detailing the inquiry's findings. The importance of issuing a comprehensive report cannot be stressed enough.

"It's very important to have an extremely complete final protocol," explained Alejandro Gil Murillo, an Associate Lawyer with CMS Spain.

According to Gil, the protocol must include the following: the allegations made by the Whistleblower or "affected employee" (particularly important in harassment cases), all the documentary evidence, and the findings of the interviews of both the subject and any witnesses. The report can also contain feedback from the union or works council representing the subject and any evidence culled from external participants, such as clients and contractors.

After the report is finalised, it should be presented to the suspect of the investigation, who should have an opportunity to respond. Copies of the final report, however, should also be given to any legal representatives of the employee or to the affected employee's union if the CBA requires it.

Lastly, it should be understood that the report will become evidence in court if the employee presents a legal challenge. Hence, the company should retain a copy of the investigation's findings in both hard copy and digital format.

But this raises the question: how final is the final protocol? After being reviewed by the suspect, can the report's findings be appealed if the suspect maintains that the conclusions are flawed or that key evidence has been overlooked?

The answer depends on each company's individual policies on internal investigations: whether a company has built an appeal process into its investigation procedures. If lacking an established appellate process, companies are under no legal requirement to entertain an appeal. In this case, if a company considers an appeal, they do so voluntarily out of a sense of fair play that could strengthen the company's legal position should the matter later go to court.

Corrective actions

If the investigation finds that the suspect is guilty of misconduct, the company is obliged to respond. In addition to any changes made to company policies that might prevent such a wrongdoing from taking place in the future, the company is obliged to apply corrective measures to the guilty employee.

Basically, the response to be made falls under three categories according to Spanish labour regulations: minor offences, serious offences, and offences categorised as very serious. Employees revealed to be guilty of minor offences can be served a written or verbal warning. Under Spanish law and the applicable Collective Bargaining Agreement (CBA), these employees can also be suspended without pay for up to three days.

For more serious offences, employees can be suspected, depending on the applicable CBA, up to 15 days without pay or prohibited from receiving a promotion for up to three months.

In cases of extremely serious misconduct, an employee can be suspended for up to 60 days (again, depending on the CBA). He can also permanently lose the right of promotion within the company. As a last resort, the employee can be dismissed.

Whatever corrective measures are issued, the company must (as stated earlier) adhere to strict deadlines for the rendering of judgments. For minor offences, companies must issue their decisions within ten days. The deadline for serious offences is 20 days. For extremely serious offences, companies must investigate and render a judgment within six months from the date the misconduct occurred. In addition, a company has 60 days from the moment it learned of the misconduct to complete the investigation and render a final decision.

Also note, because Spanish law does not mandate internal investigations, those companies without established policies requiring internal investigations can implement corrective measures as soon as an allegation of misconduct comes to light.

In the end, companies are encouraged to approach allegations of employee misconduct with the utmost care and consideration since any investigation and judgment may be challenged in court. If called upon to review a judgment and corrective measures, a labour court may do any of the following: confirm a sanction, partially revoke a sanction, totally revoke a sanction or render a company's judgment null and void. To avoid the latter, companies are advised to ensure that their response to any misconduct adheres to Spanish labour law, gender equity laws, data protection regulations, an employee's personal and civil rights, all pertinent clauses of the CBA and a general sense of fairness.

In short, companies are advised to be fully prepared for allegations by establishing internal investigation systems, a clear channel for Whistleblowers to report wrongdoing, and a strict and well-publicised corporate Code of Conduct that addresses key issues such as bullying, discrimination, harassment and corruption.

For more information on conducting internal investigations in Spain, contact your regular CMS advisor or local CMS experts:

Maria Jose Ramos
Associate Lawyer, CMS Spain
E mariajose.ramos@cms-asl.com

Alejandro Gil Murillo
Associate, CMS Spain
E alejandro.gil@cms-asl.com

Switzerland

Click to listen to the webinar recording
Published June 2020

Internal investigations on the rise in Switzerland

What you need to know about best practices and how to protect your company from liability

Although Swiss case law affirms that it is crucially important companies conduct internal investigations in certain situations, the rights and obligations of both employers and employees when allegations of misconduct arise are still not clear to everyone. Swiss law does not specifically address internal investigations.

According to Christian Gersbach, a partner with CMS Erlach Poncet AG, even though Swiss law doesn't specifically address internal investigations, "certain fundamental principles of Swiss employment law apply to the conduct of such investigations and also the mutual rights and duties of the parties."

One of the most important statutes in this regard is the employer's duty of care, outlined in art. 328 of the Swiss Code of Obligations (CO), which serves as a "general guideline" for company conduct during an internal investigation. This law obliges an employer to "act in good faith" and do everything possible to protect the employee's personality rights. Hence, if an allegation of abuse against an employee arises, this law compels the employer to act, but to do so in a way that protects all employees involved – the victim, the accused and any witnesses.

The law governing the employer's right to give instructions (art. 321 CO), enables a company to be able to launch an investigation and guarantee the cooperation of employees, who in turn have a "fiduciary duty" to conduct themselves in a honest and lawful manner vis-à-vis the employer's funds and assets (art 321a CO). Switzerland's data protection legislation governs how an employer can collect data considered evidence.

According to these provisions, a company can only investigate an employee for alleged misconduct performed on the job. (An employee cannot be investigated for conduct the company may find embarrassing during private hours away from the workplace, such as comments made over social media). Furthermore, the employer does not have the same right as, for example, a state prosecutor (e.g. if the employee does not participate in an investigation or makes false statements). As a result, the measures that the employer may take during an investigation – and as a result of such an investigation – are strictly limited to employment law. On the other hand, according to case law, the employer does not have to grant the same rights to the subject of an investigation as guaranteed by – for example – penal procedural law. In particular, while the employee must have a right to be heard, these employee rights are less far-reaching than the ones in a criminal investigation conducted by a public prosecutor.

The employer, however, does enjoy certain rights. He has both a right and duty to conduct an internal investigation if confronted with the proof of misconduct. But when specifically is an investigation called for? Because judgments in the Swiss high court have increasingly demanded documented justification for the termination of employees, CMS's Sarah Keller advises that thorough internal investigation procedures be implemented whenever serious allegations of employee misconduct or misappropriation arise so that any termination that follows cannot be challenged in court.

In fact, the employer has a series of duties it must adhere to should allegations be reported: a duty to conduct an internal investigation that establishes the facts since any penalties that an employer levies against a worker could be challenged if there is insufficient evidence backing it up. The employer also has a duty to establish all the relevant facts before responding to allegations of harassment in the workplace.

In terms of corporate liability, financial regulations in industries like banking demand that the facts behind any allegation of misappropriation be clearly and formally established.

Furthermore, it may be necessary to investigate the conduct of managers or directors to establish their liability for certain actions. In this case, an investigation might result in recommendations on how to establish institutional checks within a company.

Employees also have duties in connection with internal investigations. First of all, as stated, they have a duty and right to participate in any investigation that is launched. Different from criminal law in many jurisdictions that afford citizens the right to remain silent and not incriminate themselves in an investigation, employees have no right to refuse cooperation. Indeed, they have the duty to give complete and accurate information when questioned, even if their testimony is self-incriminating.

The employee does have a right to be heard during an investigation. But it is unclear based on case law whether an employee has the right to have a lawyer present during questioning. Many Swiss legal analysts argue that employees do not have this right, but CMS's Christian Gersbach recommends that companies allow the presence of a lawyer if requested by an employee since this could facilitate his cooperation and bolster the investigation's overall atmosphere of fairness.

If a lawyer is retained, who pays for this representation? The employee generally is responsible for these costs except for rare circumstances where company procedures and policies may be under investigation. In other instances, the company may have insurance policies for personnel that could cover these expenses.

What can trigger an internal investigation?

Several types of allegations can compel a company to initiate an internal investigation. In Switzerland, perhaps one of the most common accusations is expense fraud. Bullying and harassment are also reported. Whatever the allegation, the ultimate decision to launch an investigation lays with management.

In this instance, a company should mandate an independent unit to respond and investigate allegations. This team could be made up of personnel from the company's compliance or human resources office. But it is also possible to hire an experienced and impartial external body to respond, such as a law firm, accountancy office or corporate investigations agency specialising in HR issues.

When an investigation begins, discretion is paramount, but companies are not advised to keep an investigation totally secret from employees since the staff will undoubtedly be aware that something is going on. So the investigatory team and management will have to be sure to measure its response: to communicate the investigation's existence without revealing information that might violate the rights of employees or compromise the inquiry. This communication must be formulated as a strategy and drafted with utmost care.

In terms of communication, the investigators must also insure that in harassment cases, witnesses or the victim are not subject to further abuse. If deemed necessary, the accused could be removed from the work environment until the facts are established. A useful tool for this is to send him home on "garden leave" where the employee receives full salary, but is asked to remain at home and on call for possible questioning. If garden leave is ordered, this must not reflect adversely on the employee and any communication strategy the company devises for its staff must make this clear.

Launching an investigation

The first step in any investigation is document collection and review, which is crucial because documentation almost always offers essential background. Also, documents represent documentary evidence that may be crucial when arriving at and justifying a judgment. But when collecting documented evidence, employers must distinguish between an employee's private and professional communications, such as email and phone text messages.

The basic rule is: the employer has a right to review all business communication, but under almost all circumstances cannot access an employee's private communications. And all reviews must comply fully with Swiss (and possibly EU) data protection regulations.

Interviews

After all pertinent documents have been reviewed, the next step is the interviews process. Interviewing the accused, the victim (if there is one) and any witnesses should be done by an interview team specially selected by the investigation. The interviews should be private, and before each one begins, the various members of the interview team should be introduced to the subject. The lead interviewer should then explain the purpose of the interview, the background of the investigation and the process that is underway.

The primary interviewer should also explain that the meeting will be recorded. In many cases, written notes are taken, but if all the participants agree, an audio or audiovisual recording can be made of the interview.

The employee should also be cautioned that everything that transpires at the meeting is confidential and should not be confided to colleagues or coworkers.

Regarding colleagues and coworkers, the company is obliged to protect any witnesses summoned to give testimony, especially if they are in a position of having to make a statement against a superior. In cases such as this (e.g. harassment allegations), the employer should do everything possible to avoid a highly stressful confrontation between the accused and a victim during the investigation process.

After the document review and interviews, a final report must be drafted, which should outline the evidence collected and come to a determination whether or not the allegation has been proven. Once completed, the main findings of the report (sans identification of witnesses or any other confidential information) should be shown to the accused, who should have an opportunity to respond to its findings in a written statement.

At this stage, the company should decide whether or not to levy sanctions against the accused. Penalties could include a formal warning, standard termination and in serious cases termination with immediate effect. In the case of the latter, immediate termination must be issued no more than three business days after the misconduct became known, which is to say after the findings of the internal investigation were released. In short, companies must be prepared for quick action in the worst-case scenario.

Apart from sanctions, an investigation can recommend certain corrective measures, such as specialised training or coaching for staff to resolve any communication or behavioral problems that might exist within a team.

Finally, at the end of an investigation, the company must provide a comprehensive and thoughtful summary for the staff. Employees must be told what transpired (in general terms) and what measures the company will undertake to prevent similar misconduct from occurring in the future. The staff, which will be fully aware of the investigation through the company's communications and office gossip, will want an explanation and closure.

For further information on how to conduct an internal investigation in Switzerland and assistance with any investigation your firm may now be conducting, contact your regular CMS advisor or local CMS experts:

Christian Gersbach
Partner, CMS Switzerland
E christian.gersbach@cms-vep.com

Sarah Keller
Associate, CMS Switzerland
E sarah.keller@cms-vep.com

Turkey

Click to listen to the webinar recording
Published 24 March 2020

Internal investigations in Turkey subject to litany of laws including data protection

Despite lacking a central law dictating internal investigations, Turkish companies still must adhere to clearly defined regulations contained in a list of other legislation when responding to suspected wrongdoing in their organisations. These laws include the Labour Law, Code of Obligations, Penal Code and Turkish Data Protection Law.

Experts warn that a company's failure to know the implications of these various laws and codes when conducting internal inquiries can result in serious legal and financial risks. But companies can diminish these risks by being aware of the regulatory environment and implementing policies and procedures that follow the letter of these laws.

First and foremost, a company can reduce the risks of investigating malfeasance by doing everything possible to prevent it from happening in the first place. This includes drafting and distributing an employee Code of Conduct that defines inappropriate behaviour and clearly states the penalties for exercising it.

This code and the sanctions that can be handed out for violations should also be included in employment contracts.

Other than that, companies can further protect themselves by setting down procedures and systems for responding to possible abuse in the workplace. The most important step in this direction is to identify who in the organisation will respond should allegations of wrongdoing surface. In short, a business must identify its team of investigators and establish a policy regarding third-party advisors, who may be needed to lend expertise if the alleged abuse is in a specialised area such as taxes and accounting.

These in-house investigators should receive training on how to do their jobs, particularly when it comes to technical procedures such as evidence collection.

Furthermore, a company should also set down the exact investigative tools that should be employed in an inquiry, such as employee interviews, the scanning of electronic communications and audits of financial records.

Strict protocols protecting the confidentiality of whistleblowers, witnesses and suspects should also be established. Guarding the identity of the employees involved in an inquiry not only reduces the risk of injury to their careers and reputation, it also insulates the company from future court action.

Other considerations when preparing for an internal investigation: companies should insure that collecting evidence from computers, smartphones and electronic devices do not violate Turkish data-protection laws. When harvesting evidence from electronic devices that may contain an employee's personal information, a company should take great care to use all the privacy-data tools at its disposal, such as following all privacy protocols as dictated by law, issuing search notices and gaining written consent notices before any scans or searches are carried out.

The procedures described above should be fully in place before any investigation is launched. Once an internal inquiry is underway, however,

a company should consider the following points to be high priority.

First and foremost, an ongoing internal investigation should protect any whistleblower who exposed or reported abuse by keeping his identity secret and making sure he is not the target of reprisals.

When gathering evidence, strict rules of evidence management should be maintained. For example, when employees are being questioned, written minutes should be produced, verified by the interviewees and signed.

If third-party experts have been hired to assist in the investigation, they should adhere to the same rules of evidence collection and exercise the same discipline.

Time is of the essence in any investigation. Inquiries should be launched as soon as management is made aware of any abuse and investigators should do everything possible to expedite their work. Whereas there is not a specific time restriction for an employer to take action against non-severe breaches, it is important to note that once a serious wrongdoing (i.e. a wrongdoing that gives the employee cause for termination) is established, a company has six (6) days to inform the employee and issue a formal notice of termination. At the same time, it should be noted that in case of serious wrongdoing, the limitation period is one (1) year from the date the act was committed.

All judgments should be based on a careful examination of all the evidence collected, and should include the expert advice of any third-party advisors brought onboard. Penalties against employees should reflect the sanctions that have already been set down in the company's policies and procedures and the employee's employment contract. And penalties must be issued in a timely manner. Where a serious wrongdoing is in question, as mentioned above the companies have six (6) days to hand down a termination after such wrongdoing is discovered. Again, the limitation period is one (1) year from the date on which the act was committed. If a company violates this deadline, the employee has grounds to contest the penalty, no matter how convincing the evidence against him is.

What are the options for sanctions in Turkey? For non-severe breaches, an employee can receive a formal warning, which should be issued in writing and clearly document the actions for which the warning has been issued.

Also, an employee can have his pay docked, but deductions cannot exceed two-days salary and the existence of this penalty as company policy should be clearly stated in the worker's employment contract.

Lastly, if an employee's misconduct has resulted in material loss to the employer, the company can also seek damages.

But even when wrongdoing has been proven and a penalty issued, the investigation is not over. In the aftermath, companies should take great care to ensure the continued protection of whistleblowers, guarding their anonymity and making sure they receive no internal reprisals (e.g. harassment, demotion, termination).

Furthermore, data privacy must continue to be protected. Strict adherence to data-protection laws protects companies from both administrative fines of between EUR 750 and EUR 150,000 and criminal prosecution. It also protects its staff from criminal prosecution since serious violation of data rules can bring criminal sentences of between one and five years in jail.

Also, criminal liability towards representatives of a company may arise if such company fails to notify Turkish judicial authorities about any criminal violations their internal investigations have uncovered.

As stated at the beginning of this article, employee training, including a clear articulation of the company's Code of Conduct, can do much to prevent wrongdoing from taking place. Companies can also protect themselves by putting in place whistleblowing procedures and ensuring that all personnel know what to do if they spot abuse.

Companies can also protect themselves by establishing risk-analysis systems that offer early warning of any high-risk behaviour or activities. Such systems include multi-layered approval procedures, such as joint signature protocols, which may render some forms of wrongdoing (particularly in the financial area) virtually impossible.

Based on the current legal environment, companies can also install internal controls, such as electronic monitoring, in the workplace to both influence behaviour and provide early warning of any problems. But again, while Turkish labor courts have been more relaxed and employer friendly on this issue, all electronic supervision must adhere to Turkey's data protection laws.

In the end, after an investigation has been completed, management and the investigation teams should conduct a postmortem of the inquiry, evaluate what procedures worked and what practices fell short, and implement any reforms deemed necessary.

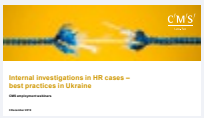
For more information on conducting internal investigations in Turkey, contact your regular CMS advisor or local CMS experts:

Döne Yalçın
Partner, CMS Turkey
E doene.yalcin@cms-rrh.com

Inci Alaloglu-Cetin
Counsel, CMS Turkey
E inci.alaloglu-cetin@cms-cmno.com

Sinan Abra
Counsel, CMS Turkey
E sinan.abra@cms-rrh.com

Ukraine



Click to listen to the webinar recording
Published 18 December 2019

Ukrainian business urged to use 'internal investigations' to fill legislative gap

With labour law in Ukraine currently unable to address many of the forms of corruption common to the corporate world, Ukrainian companies are now being urged to establish their own internal investigation procedures and police themselves in matters of internal corruption and employee wrongdoing.

According to experts, Ukraine authorities may lack the tools and resources to investigate certain types of corruption, but it is in a Ukrainian-based company's best interests to implement effective internal investigation systems that represent the best practices of the industry.

Why? Although Ukraine labour law does not include specific requirements for internal investigations, proactive action by companies to prevent and root out corruption can reduce the risk that its staff will be found guilty of violating Ukrainian law. In addition to legal risks, this policy also protects firms from financial loss and the incalculable cost of a diminished reputation.

In terms of reputation, the existence of visible and effective internal investigation procedures sends a message to the business community that the firm is committed to transparency and honest business practices. Similarly, these systems can also boost staff morale by creating an employee friendly environment where all personnel feel both secure and empowered.

But internal investigations are also necessary given the prevalence of corruption in the Ukrainian corporate world, which experts attribute to imperfect laws and a lack of investigative resources by certain authorities.

Given Ukraine's problematic legal environment, Ukrainian companies have only a few guidelines they must follow in regard to internal investigations. For example, employee sanctions are limited to only two types of actions: reprimands and dismissals.

In the case of dismissals, this action can only be executed by corporate bodies with the legal power to hire personnel: the company director or its board of directors. But there is a statute of limitations on dismissals that makes efficient and expeditious internal investigations both valuable and necessary, particularly in cases of serious breaches.

Staff members guilty of misconduct can only be sanctioned within a month of a breach, a time limit that can be extended if the employee under investigation is on leave, but cannot be extended more than six months. Furthermore, only one sanction can be issued per case.

Even though Ukrainian labour law is mum on the nuts and bolts of an internal investigation, other legal considerations makes it essential that any staff member under scrutiny must be given a full opportunity to explain his actions and refute any charges.

Companies must be aware that sanctions – mainly dismissals – can be appealed, but that Ukrainian labour law does not have a mechanism for employees to lodge grievances other than the established system of labour-dispute resolution. For companies that have labour or works councils, these bodies can be used to mediate grievances and cooperate

in investigations. But it should be noted that Ukrainian law differs from the labour codes of many western European countries in that it does not mandate works commissions. As a result, not many Ukrainian companies have them in place.

When collecting evidence as part of an in-house inquiry, companies are primarily advised to adhere to laws on data protection, since most investigations involve the collection and storage of data. Ukrainian law does not regulate the collection of data during internal investigations, but it does have strict guidelines on collecting personal data of employees. Hence, if an internal investigation is likely to impact or affect an employee's sensitive personal data, the company's data protection officer and the state data authority – the Ukrainian Parliament's Commissioner for Human Rights – should be notified.

The latter office must be informed within 30 days of the beginning of any investigation that collects sensitive personal data. The importance of adhering strictly to the general rules of data privacy and data collection regulations cannot be overstressed given that personal privacy in the Ukraine is a constitutional guarantee.

If personal data is not an issue in an investigation, companies are not required to inform authorities of a query, and may only be obliged to do so after an investigation has been concluded if evidence has been uncovered of state crimes, such as theft or fraud.

To protect themselves from data-protection restrictions in an investigation, companies are advised to warn employees at the start of an employment relationship that their professional communications (i.e. company email accounts and phone records) can be accessed in any investigation. They should be warned not to use professional accounts for personal use, and if they do so, they should mark all personal emails as "private" so that these communications can be avoided in an inquiry.

Other points to remember in an investigation: all investigations should be carefully documented and adhere to an established system and schedule; in interviews, the subject of the investigation should be informed that his professional data will be reviewed, transferred and stored and no personal data can be accessed without the employee's permission; and lastly professional email communications can be monitored so long as the personal privacy of the individual has not been violated.

In short, Ukrainian law may not demand that companies have effective internal-investigation procedures in place, but it is in a company's best interests to do so and ensure that all investigatory procedures respect every Ukrainian citizen's constitutional rights for privacy and data protection.

For more information on internal investigations in Ukraine, contact your regular CMS source or local CMS experts:

Maria Orlyk
Partner, CMS Ukraine
E maria.orlyk@cms-rrh.com

Mykola Heletiy
Associate, CMS Ukraine
E mykola.heletiy@cms-cmno.com

United Kingdom

Click to listen to the webinar recording
Published 1 June 2020

Strategic guide: internal investigations in the UK

Introduction

In recent years there has been a sharp increase in internal investigations in UK businesses. This is in part due to an increased focus on ethics and governance and, within certain sectors, increased regulatory scrutiny and a move towards a speak up, listen up culture.

These workplace investigations are as diverse in their subject matter as they are in their origins. Triggers for an investigation include whistleblower reports, workplace grievances, external complaints or regulatory enforcement action. The objectives and outputs therefore vary considerably:

At the most basic level, an organisation will want to respond to a complaint by investigating whether it has any substance. At the other end of the spectrum there may be a 'root and branch' investigation into culture. For example, where a previous investigation has hinted towards a widespread institutional problem.

Some investigations are pre-emptive, in the sense that they seek to avoid a situation where a third party such as a regulator takes matters into its own hands.

Others are reactive and focus on damage limitation.

It is critical to understand why an investigation is being carried out and to ensure that key decisions such as resourcing, legal privilege and the form of reporting are strategically aligned.

Establishing an effective investigation process will also promote confidence amongst staff and other stakeholders, including investors, that any wrongdoing will be taken seriously, and that individuals are held accountable for their actions. The internal investigation process can also root out more systemic issues such as poor risk culture or certain behavioural problems, which may not be obvious to those at a senior level.

This strategic guide focuses on practical aspects of planning and managing internal investigations. Developed alongside a webinar presented by Hannah Netherton and Steven Cochrane, partners in the CMS Employment Group, this guide contains our expert insights and advice relevant to all internal investigations in the UK workplace with a focus on the nuances unique to whistleblowing and sexual harassment investigations. Finally, given the current workplace restrictions in the UK, we look at some of the challenges when dealing with investigations in a virtual context.

Planning and Scoping

There are many key hallmarks of an effective investigation. In fact, what 'good looks like' will vary on a case by case basis. However, there are some basic considerations important to all investigations, and none more so than the planning and scoping phase.

The appropriate breadth and depth of an investigation will depend on a number of internal and external factors. These factors should be considered upfront and the scope of the investigation agreed upon (bearing in mind that a degree of flexibility may be required to take account of potential developments, such as fresh allegations coming to light during the investigation).

It will also be crucially important for the investigator to understand the scope of the investigation, the wider strategy and their own role in the process. In situations where the HR team is investigating a relatively routine employee relations issue, this ought not to be particularly difficult. However, with larger or more complex investigations, such as those involving specially formed investigation committees or external investigators, it will be extremely important to articulate all of these points in a formal terms of reference. For more complex investigations the terms of reference should address issues such as the scope of the investigation, the nature of the allegations/issues being investigated, the authority under which the investigation is being conducted and the intended form of output (e.g. a formal written report, presentation to key stakeholders, written recommendations). Again, it is always sensible to ensure that the terms of reference are clear but flexible, so as to accommodate any further material developments that arise during the investigation.

Proportionality

A proportionate response is key to an effective investigation. A well thought through scope and terms of reference will focus minds and help ensure that the investigation remains on track. Certain investigations demand only a light touch response, with relatively few interviews or documents to review. Conversely, other investigations will require a more rigorous approach with multiple witness interviews and a complex and time-consuming document review exercise. Generally, the level of investigation will depend on the seriousness or complexity of the allegations (as well as the potential for external scrutiny or collateral litigation). However, it Is important to exercise judgement in deciding what is proportionate to the facts of the investigation and to avoid an overly superficial investigation (which could appear to be whitewashing the issue) or conversely a heavy handed approach that is more invasive than is necessary. This can often be a delicate balancing act and requires careful consideration at an early stage of the process.

Confidentiality

The importance of confidentiality in internal investigations cannot be overstated. There are multiple reasons for ensuring that confidentiality is a key focus. From a PR perspective, robust information barriers are an important measure to mitigate the risk of an information leak and information and documentation should generally only be shared on a ‘need to know’ basis.

Confidentiality is also vitally important in terms of maintaining trust in the process. Internally, trust

will be severely damaged if confidentiality is not respected. In whistleblowing cases in particular, unnecessary sharing of information can increase the risk (or at least the perceived risk) of whistleblowers or witnesses being subjected to retaliatory treatment or detriment. Externally, regulators and law enforcement agencies will generally hold an internal investigation in higher regard where confidentiality protections have been robust. In certain sectors this may mean the difference between third parties, such as regulators, accepting the internal response or being dissatisfied and commencing their own external investigation.

Another compelling reason for ensuring confidentiality exists where an investigation (or part of it) is intended to be protected by legal privilege. While the law on privilege is in a state of flux in the UK, it is fair to say that privilege is unlikely to attach to all documents produced, created or collated as part of an investigation. However, where the company is looking to maintain a claim for legal privilege over some or all of an investigation (e.g. its outcome), loss of confidentiality will almost always lead to a loss of privilege. This could be a devastating outcome, particularly where the potential cost of adverse publicity is high or where there is a risk of disclosure requests by or obligations to third parties (for example in the context of collateral litigation).

However, as important as confidentiality is, it is not absolute. The need or desire for confidentiality must be balanced with other considerations such as the need for fairness, in particular vis-à-vis the individual subjects of allegations. As a general rule witnesses or complainants should not be given guaranteed confidentiality or anonymity as this could be considered unfair to those under investigation. Similarly, it will not always be possible to guarantee confidentiality or anonymity and it may be necessary to disclose certain details of an investigation (including the identity of individuals), for example in the context of regulatory enforcement action or disclosure in litigation. The key will be ensuring that reluctant witnesses' fears and anxieties are understood and that, where possible. reasonable reassurance is provided.

Who should investigate?

By choosing the right individual to lead an investigation, the company can do much to ensure its success. Multiple factors should be considered including skills, experience, independence and the risk of perceived conflicts of interest. In certain investigations, even where no actual or perceived conflict exists, the sensitive nature of the allegations may mean that it would be preferable (in terms of overall optics) to have the investigation carried out by persons with particular experience or background.

- **Independence and perceived conflicts of interest.** This issue frequently arises where the subject(s) of the allegation(s) are particularly senior, for example a member of the board or executive committee, or senior management more generally. Where this is the case it can be difficult to create actual and perceived impartiality without appointing an external investigator. Depending on the circumstances this could be an external HR consultant, or senior representatives from another group company. In certain circumstances the Chairman of the Board supported by other independent non-executive directors may be appropriate. Where maintain legal privilege is of particular importance it may be preferential to appoint external counsel to manage or support the investigation.
- **Skills and experience are extremely important.** This covers both requisite experience in investigation skills (for example interviewing witnesses) and, where particularly technical or complex allegations are at play, experience and knowledge of the underlying subject matter. It can be very difficult for an investigator to meaningfully engage in a complex allegation about industry specific or technical matters if they do not have a good grasp of these matters.
- **Lastly, optics will always be important.** This is particularly significant where the investigation is likely to be subject to external scrutiny. It is often the case when dealing with high profile and/or serious regulatory allegations of wrongdoing that external investigators such as lawyers or consultants are appointed. A decision not to appoint external independent experts would need to be carefully thought through and be capable of being justified, as choosing not to make these appointments may appear inappropriate to regulators. In other investigations, particularly those involving serious allegations of discrimination and harassment, it may appear insensitive or inappropriate to appoint a lead investigator who does not share some of the same characteristics as the victim (for example, appointing an investigation committee comprised of three white males is likely to be inappropriate where the complaint is a black female complaining of racism and sexual harassment).

Policies and sources of guidance

Although it may seem obvious to establish and follow sound internal policies, doing so is not always straightforward. Misconduct allegations are rarely cut and dry, and some organisations develop separate policies for handling harassment and bullying, alongside their standard grievance policy. Employers should also consider at the outset whether the matter is captured by a company whistleblowing policy. Ideally, these policies will align alongside each other. However, since these types of documents are regularly updated, both the appointed investigator and HR should read and reread the relevant policies before an investigation starts.

The investigator (and of course HR) should also be familiar with other sources of guidance for investigations, including the ACAS Code of Practice on disciplinary and grievances, which sets the minimum standard of fairness in the workplace in the UK, and the ACAS Guide to Investigations.

If the employee operates in a regulated environment, then any additional layers of compliance should be considered according to the relevant rules. Where harassment is in scope, an investigator should familiarise themselves with the Technical Guidance on Sexual harassment and harassment at work issued by the UK's Equalities and Human Rights Commission (EHRC).

Interim safeguards

Investigators, as well as HR staff assisting in an investigation, should consider at the outset whether any other interim safeguards are required and, in particular, whether any further action is needed to protect evidence and the investigation's integrity. This might include decisions around suspension of alleged wrongdoers from the workplace pending investigation in order to prevent contact between witnesses or the undermining of evidence during an investigation.

Investigators may also look to put a document preservation system in place to protect evidence. This might include suspending any existing IT procedures on the deletion of emails from the company servers following a determined period, to prevent any potentially important records being lost.

The investigation must also comply with data protection legislation including the UK's Data Protection Act 2018 and the GDPR. Where it becomes clear that an investigation will require a substantial search of employee communications, the company should consider whether a Data Privacy Impact Assessment (DPIA) should be completed before the processing of any personal data takes place. Failure to do so could lead to investigation, criticism and/or enforcement action from the UK's data regulator, the ICO, as well as potential collateral litigation from any data subjects whose personal data is not processed lawfully. If a DPIA is deemed unnecessary, it is advisable to document the rationale for this in writing, to ensure there is an audit trail should that decision subsequently need to be justified.

Whistleblowing

Focus on … whistleblowing investigations

Generally speaking, the best practices discussed above should be equally applicable to most whistleblowing cases. However, there are specific nuances in whistleblowing investigations that merit further consideration.

In certain sectors, such as financial services, whistleblowing and the need to have a 'speak up, listen up' environment is part of the regulators' broader agenda on culture. Regulators such as the Financial Conduct Authority have made it clear that psychological safety and an open environment, where people are empowered to call out problems without the fear of reprisal, is a regulatory requirement rather than a 'nice to have'. As such most financial institutions have relatively sophisticated whistleblowing frameworks, including policies, escalation procedures and multiple internal and external channels for the reporting of wrongdoing. But the recognition of this need and this framework for a healthy workplace culture and sound risk management is not unique to the financial services industry.

Clearly, maintaining a robust and well communicated 'speak up' infrastructure is key. However, this is only the beginning and, without the correct mindset throughout the organisation, this infrastructure becomes impotent. Businesses need to follow through on their promises and ensure that values and corporate commitments around whistleblowing do not become mere platitudes.

Confidentiality and anonymity will be particularly important in the whistleblowing context, as the cornerstone of any good regime will be protection of whistleblowers against detriment and victimisation. This can only exist where whistleblowers are able to come forward on an anonymous basis or where high levels of confidentiality and trust exist.

It is also crucial for those that investigate whistleblowing to wear a 'purpose blind' lens, focusing on the allegations and the fact finding and avoiding the trap of focusing too much (if at all) on the potential motives of the complainant. Doing so, whilst perfectly natural, can severely undermine the perceived impartiality and neutrality of the investigator and in turn, the integrity of the whole investigation.

Sexual harassment

Focus on … sexual harassment investigations

Whether triggered by a direct complaint or concerns about the culture in a particular business area, many current corporate investigations involve sexual harassment allegations, reflecting the global #Metoo movement that has focused on tackling this type of workplace issue.

Investigators should be fully acquainted with the latest EHRC Technical Guidance before carrying out the investigation, bearing in mind that this guidance offers recommendations and is not a statutory code.

Where harassment has been alleged, investigators should be sensitive to the delicacy of this issue and conduct themselves appropriately. As discussed above, the decision around the identity of the investigator, together with their skills and background, are crucial. When interviewing victims of sexual harassment, investigators should choose their words and approach carefully in order to ensure both a fair outcome and that the complaint has been heard. Sexual harassment investigations also require the investigator to ask about subjective feelings and not purely objective facts, as an integral part of the process is to obtain an understanding of the impact on the individual. This will obviously be a sensitive but important process for an investigator to tackle.

Investigators may also decide that it is in the best interests of the person bringing the complaint that they are accompanied to interviews for emotional support. This may already be a requirement under the relevant workplace policy but this is often limited to a colleague or union representative only. Additional discretion may well be appropriate here in allowing the individual to bring a person of their choice for support.

Investigators may face situations where it becomes difficult for an investigation of this type to proceed. For example, the person making a complaint does not want an investigation to take place, or the person accused resigns after a complaint has been made. In these situations, even though it may be tempting for the organisation not to investigate, it will often be prudent to continue. There are a number of good reasons to do so, not least that a failure to act could be perceived as a cover-up or lack of interest in tackling an underlying cultural issue.

Further considerations are necessary where an individual concerned in the investigation leaves the company. This could be the complainant, the accused or a witness, and they might leave for all manner of reasons. However, where they have left under terms of a settlement agreement, the company should carefully consider whether it is appropriate to insist that the employee signs a non-disclosure agreement (NDA) as part of the settlement terms. While these have become entirely standard in UK settlement agreements, both the EHRC and the Law Society of England and Wales have published important guidance and practice notes on the use of NDAs in discrimination and harassment cases. Both legal and HR advisers should carefully consider these obligations and the impact of an absence of confidentiality obligations as part of any exit discussions.

While much of the business world is locked down during the COVID-19 pandemic, a central question is: how can internal investigations – particularly highly sensitive ones – be conducted while employees are working remotely?

Investigations, particularly workplace investigations, tend to be largely 'people' focused. The fact-finding exercise is typically based on witness evidence rather than extensive document review exercises. Emotional connection and the ability to ready body language, build rapport and empathy are critical. All of these things are undeniably more difficult in the context of a remote or 'virtual' interview. However not all complex or sensitive investigations can or should be put on hold until the current lockdown restrictions are eased.

Whilst creating an emotional connection in a virtual world is a challenge, it is not insurmountable. Perceptions around the use of technology have dramatically changed since lockdown was implemented in the UK. We have seen courts and tribunals successfully manage virtual hearings and emotionally charged settlement discussions. Mediations have successfully played out using video technology.

A successful remote investigation is therefore achievable.

Certain issues will need to be given special or additional consideration (for example the right to be accompanied, the need to give witnesses access to highly restricted documents during the interview or confidentiality – which may be difficult depending on the participants' home-working environment). However, in most cases, with careful consideration and planning the investigation can proceed without face to face interaction. Generally speaking, the benefits of proceeding with the investigation (as opposed to putting on hold indefinitely) will outweigh the downsides or challenges attaching to doing so virtually.

Key takeaways

In summary, internal investigations can be carried out successfully where companies remain focused on the following:

- Planning is key. A clear scope and terms of reference will help ensure that the investigation remains on track. A considered strategy will help to pre-empt potential unintended consequences before they occur.
- Selecting an appropriate investigator will be essential to the investigation running smoothly. An investigator without the requisite investigative skills, technical/subject matter knowledge or perceived independence can undermine the integrity of the whole process.
- Confidentiality must be maintained so far as possible. Information should generally be shared on a 'need to know' basis. A lack of confidentiality increases the risk of information leaks (as well as loss of legal privilege, if claimed) and erodes internal and external confidence in the process.
- Understand the limitations of legal privilege and decide on your strategy upfront.
- Remember to act proportionately. Not all investigations demand a 'root and branch' fact finding exercise. Conversely, a light touch investigation will be inappropriate in relation to serious allegations and may result in allegations of 'whitewashing' or avoidable intervention by law enforcement agencies and/or regulators.
- Make sure the investigator and company are fully versed on company policies, rules of the relevant regulatory body and the most recent guidance from ACAS and the EHRC.
- Ensure that all decisions as the investigation progresses are based on the evidence collected.
- Manage the risk of collateral disputes or litigation and adhere to data protection law when collecting and storing evidence.
- Ensure that the investigation is carried out in a manner that is consistent with the company's culture, particularly regarding fairness and equality.

For more information on conducting internal investigations in the UK, contact your regular CMS advisor or local CMS experts:

Hannah Netherton
Partner, CMS UK
E hannah.netherton@cms-cmno.com

Steven Cochrane
Partner, CMS UK
E steven.cochrane@cms-cmno.com

C/M/S/ Law-Now™

Law . Tax

Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.
cms-lawnow.com

CMS locations:
Aberdeen, Algiers, Amsterdam, Antwerp, Barcelona, Beijing, Belgrade, Berlin, Bogotá, Bratislava, Bristol, Brussels, Bucharest, Budapest, Casablanca, Cologne, Dubai, Duesseldorf, Edinburgh, Frankfurt, Funchal, Geneva, Glasgow, Hamburg, Hong Kong, Istanbul, Johannesburg, Kyiv, Leipzig, Lima, Lisbon, Ljubljana, London, Luanda, Luxembourg, Lyon, Madrid, Manchester, Mexico City, Milan, Mombasa, Monaco, Moscow, Munich, Muscat, Nairobi, Paris, Podgorica, Poznan, Prague, Reading, Rio de Janeiro, Riyadh, Rome, Santiago de Chile, Sarajevo, Seville, Shanghai, Sheffield, Singapore, Skopje, Sofia, Strasbourg, Stuttgart, Tirana, Utrecht, Vienna, Warsaw, Zagreb and Zurich.

---

cms.law