INTERNAL INVESTIGATIONS

When is an employer required to conduct an internal investigation?

What are the typical subjects for employment investigations?

How quickly must the employer conduct an investigation once it is aware of the conduct?

What data privacy rules must the employer be aware of when conducting an investigation?

Must employers involve collective employee representatives?

What is best practice when using social media in an investigation?

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Must the employer provide the employee with all gathered evidence?
Summary

Austria ................................................................. 4
Belgium ............................................................... 6
Brazil ................................................................. 8
Denmark .............................................................. 10
Finland ............................................................... 12
France ................................................................. 14
Germany ............................................................. 16
Hungary ............................................................... 19
India ................................................................. 21
Ireland ............................................................... 23
Italy ................................................................. 25
Luxembourg ....................................................... 27
Mexico ............................................................... 29
Norway ............................................................... 31
Poland ............................................................... 33
Russia ............................................................... 35
Spain ................................................................. 38
Turkey ............................................................... 40
Ukraine ............................................................. 42
United Kingdom ............................................... 44
United States .................................................... 46
When is an employer required to conduct an internal investigation?

Internal investigations are conducted for suspected violations of the law (i.e. concerning antitrust, capital markets, anti-corruption, privacy, labour, environmental law, competition and anti-discrimination law) or in the course of anticipated governmental investigations. An internal investigation may also be suggested if there is an indication that corporate policies have been violated (e.g. codes of conduct), often in relation to multinational companies.

The employer has a general obligation towards its employees to appropriately investigate any allegations about anticipated or actual behaviour which could justify an intervention in terms of employee rights, until the situation is adequately clarified. This covers, in particular, allegations of defamation, assault and harassment. This general obligation can be used as legal justification for an investigation. In ordinary cases, the facts may be verified by simple enquiries, but more complex situations may give rise to an obligation to perform a formal internal investigation.

If codes of conduct exist or if whistle-blowing hotlines are set up, the employer should investigate allegations via these means promptly.

By law, where there is a company-wide investigation of a parent company, cooperating with a US authority, internal investigations in Austria are primarily conducted with the participation of an Austrian subsidiary. However, internal investigations can also be independent of the investigative activities of US authorities. Although the term ‘internal investigations’ is not explicitly used in Austrian law, in Austria, as in the US and the UK, there are generally incentives for organisations to cooperate with the authorities in investigations into unlawful behaviour.

What are the typical subjects for employment investigations?

Investigations carried out by an employer typically include allegations of:

- discrimination;
- assault;
- harassment;
- drug or alcohol use.

How quickly must the employer conduct an investigation once it is aware of the conduct?

Although under existing case law, the courts have not yet made a clear statement about timeframes, it is fair to assume that investigations should not be suspended or delayed. Even though it is not clear if ‘promptness’ is the correct legal requirement, the employer should take prompt and clear action.

This applies especially to summary dismissals, where the employer must act without undue delay after it becomes aware of the relevant facts, otherwise the dismissal may be delayed.

If the employer fails to investigate and misses the opportunity to provide an appropriate remedy, this may result in justified termination of the work contract by the employee, which in turn will trigger certain legal consequences.
example, the employer may be obliged to pay compensation for termination of the employment contract (‘Kündigungsschädigung’), depending on the extent of the employer’s failings.

What data privacy rules must the employer be aware of when conducting an investigation?

Austrian data protection law contains provisions on the use of personal data and the constitutional right to privacy. Therefore, everyone has a fundamental right to privacy of personal data, provided they have a legitimate interest. In principle, this right may only be limited to protect the overriding legitimate interests of another by using the least intrusive means possible. However, if the data subject consents to processing, the data are publicly available or only anonymous data are used (i.e. the data subject cannot be identified), this right may be limited.

Data protection principles

Under law data must:

- only be processed fairly and lawfully;
- only be collected for specified, clear and legitimate purposes and not processed in a way incompatible with those purposes;
- only be processed to the extent necessary for the purpose and not for another purpose;
- only be processed in a way that ensures the information is accurate and up-to-date;
- stored in a form that can identify individuals only for as long as required for fulfilling the purposes of collection.

Longer storage periods may be required under specific law, in particular, relating to records in archives.

Further, data must be processed only so far as the purpose and content of the data are protected by the legal competences or powers of the data controller and do not impinge on the data subject’s right to privacy.

In order to process data lawfully, they must be processed only to the extent required, using the least intrusive method and in compliance with the main principles of data protection law.

Security measures

For each organisational unit of the data controller or processor, certain data security measures must be taken. Depending on the category of data and purpose of the processing, taking into account technical and economic considerations, the controller must ensure that the data are protected from accidental or unlawful destruction and loss. It must also ensure lawful processing and protection from unauthorised access.

Must employers involve collective employee representatives?

An internal investigation does not trigger legal rights for the works council to participate in the investigation. Therefore, it must not be involved by the employer. This follows from the fact that data collection does not include a right to participation.

However, certain elements of an internal investigation, or actions resulting from an internal investigation, may require the involvement of the works council. If the internal investigation triggers certain control measures, a collective bargaining agreement must be concluded.

What is best practice when using social media in an investigation?

The employee generally determines the degree and scope of personal data that is made publicly available on social networks. Any information made publicly available by an employee can be used by third parties. Therefore, processing this information does not infringe any legitimate privacy interests.

Care must be taken, however, where the employer takes measures to monitor private data that is not publicly available and transfers the data using its systems. In this case, the employer should ensure it complies with data protection law on the processing of data.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

An internal investigation should not involve continuous surveillance, but rather ad-hoc access, as part of the investigation.

Emails contain personal data of the sender and the receiver, and the organisation’s email system is a way of using the data. Its use and control is subject to legal constraints protecting the right to privacy.

Where there is a clear suspicion of a violation of law or contract, the data subject generally cannot rely on his or her fundamental right to privacy. However, to protect the individual, appropriate safeguards must be implemented and the intrusion must be proportionate to the threat. The individual must be given the opportunity to consult with a person of trust, the works council or a data protection officer.

Camera surveillance

Video monitoring is considered acceptable if it is the least intrusive method to achieve the goal. Generally, video surveillance is permitted to protect the subject or to protect individuals from assault or attack.

However, video surveillance is expressly prohibited for the purposes of employee control or supervision in the workplace. This is because it is assumed that effective control can be achieved by less intrusive means. Nevertheless, video surveillance is permitted, for example, for the monitoring of cash rooms or hazardous machinery, to protect the health of employees. The monitoring of personal areas such as dressing rooms and restrooms is strictly prohibited.

As well as data protection restrictions on conducting video surveillance, specific labour law restrictions must be observed. The installation of video cameras is considered a control measure affecting human dignity if the cameras, even occasionally, capture images of the employee’s workspace. Therefore, video surveillance is permitted only with the consent of the works council.

Must the employer provide the employee with all gathered evidence?

There is no general obligation to provide all evidence gathered to the employee. However, the rights of employees vary depending on the circumstances. Employees who are subject to investigations by state authorities and court proceedings for potential compliance violations may be entitled to access certain documents and information.

The employer should inform an employee of any allegations, so that he or she can fully respond and give the employer relevant information.
When is an employer required to conduct an internal investigation?

There is no generally applicable requirement on employers to conduct internal investigations. There is, however, a specific legal obligation on employers to conduct an investigation in the case of a complaint about bullying, sexual harassment or violence at work.

What are typical subjects for an employment investigation in your country?

Investigations carried out by an employer typically include:

- financial impropriety (e.g. fraud);
- theft;
- disciplinary matters;
- allegations of harassment (including violence, sexual harassment, bullying or discrimination);
- whistle-blowing by an employee regarding, for example, corporate wrong-doing.

How much time does the employer have to conduct the investigation once it learns of wrongful conduct?

There is no set period of time within which to investigate, but an employer is expected to act reasonably quickly. How long an investigation takes will depend on the complexity of the issues, their nature, the number of people to be interviewed and their availability.

The progress of the investigation should be well-documented, and if so, it should be possible to verify whether it was carried out within a reasonable timeframe.

What data privacy duties and obligations should an employer be aware of when conducting an investigation?

Information collected in relation to investigations might qualify as the processing of personal data. If so, data protection principles apply. Particularly relevant are the duty to process fairly and to use the data for specified purposes.

Is an employer required to involve collective employee representatives (e.g. a works council or trade union) in an investigation?

There is no requirement on employers to involve employee representatives in an investigation, unless this has been agreed at company level (e.g. in a collective bargaining agreement or the organisation’s work regulations). Employees can ask union representatives to assist them when they are being interviewed.

It is also good practice to inform or consult employee representatives when developing company policies.

What are best practices when using social media in an investigation?

Accessing social media used by an employee in a private context is considered
intrusive. Before doing so, an employer should consider its own policy on the use of social media.
All employers should devise a policy on the use of social media in so far as it affects work. They should make sure that employees know what is allowed and what is not and should set out the employer’s expectations clearly and explicitly. If limited private use of social media is permitted in the workplace, employers need to be clear what the limits of this are.

› Is an employer who is investigating able to (a) read an employee’s emails on the employer’s devices and servers or (b) film an employee who is under suspicion covertly.

**Emails**

Employers should have a policy on the use of email and the Internet by their employees. The policy should cover (a) the do’s and don’ts of using email and the Internet and (b) the conditions under which the employer can monitor the use of email and the Internet and intercept emails. The employer should always inform its employees that emails may be intercepted for specific reasons. The employee representatives should be informed and consulted about the policy.

**Camera surveillance**

Case law is divided about whether an employer can arrange for the covert filming of an employee. Some courts will only accept camera surveillance if the employer has respected its legal obligations regarding camera monitoring and data protection (meaning, for example, that the employer must inform and consult the employee representatives before installing cameras). If the employer does not respect these obligations, those courts will admit the covert filming in evidence. Other courts are more tolerant with regard to covert filming and will accept filming used to establish serious misconduct.

› Does the employer have to provide all gathered evidence to the employee? Why or why not?

There is no general obligation to provide all gathered evidence to an employee.
When is an employer required to conduct an internal investigation?

There is no Brazilian employment law that requires the employer to conduct an internal investigation. However, it is common for employers to conduct internal investigations into facts that may result in termination of employees for cause. This is because terminations for cause are usually challenged in court and employers must be able to properly document the fault that resulted in the termination. In the event of termination of an employee who is an union representative and, as such, is entitled to tenureship, it is highly recommended that an internal investigation be conducted in order to support the judicial inquiry which must be filed before the employee can be terminated for cause.

What are the typical subjects for employment investigations?

The circumstances that may lead to termination for cause are the following:

- acts of dishonesty;
- lack of self-restraint or misconduct;
- performance of regular business without the employer’s consent or where there is a conflict of interest between such activities and those of the employer;
- criminal convictions;
- capability issues with the employee’s performance at work;
- regular intoxication during work;
- disclosure of trade secrets;
- insubordination;
- abandoning employment;
- damaging the reputation of any person during working hours or physical violence, except where there is a legitimate reason;
- damaging the employer’s reputation or that of senior management;
- physical violence, except where there is a legitimate reason;
- continuous gambling.

It is common to initiate investigations when there is evidence or if the employer suspects that employees are engaged in activities that may be damaging to the employer and can result in terminations for cause.

How quickly must the employer conduct an investigation once it is aware of the conduct?

There is no fixed period of time within which an employer must conduct an investigation but it is expected to act reasonably quickly for potential termination for cause. How long an investigation takes will depend on matters such as complexity, the nature of the allegations, the number of people to be interviewed and the availability of interviewees. Once a fact is proved, the employer must proceed with the termination. A failure to act promptly is deemed as a waiver of the right to terminate for cause.

What data privacy rules must the employer be aware of when conducting an investigation?

There is no specific law governing data protection in Brazil.
Under the Brazilian Federal Constitution, privacy, private life, dignity and reputation of individuals must not be violated. The Constitution includes a right to compensation for moral harm resulting from violations.

Under civil law, individuals can apply for injunctions before any relevant court, to prevent or stop any violation of privacy. Therefore, unauthorised collection or use of personal data may attract injunctions and potential liability for damages.

Generally, employers must not perform random drug testing on employees, as this may be considered discriminatory. Only in limited situations may it be acceptable to perform drug or alcohol tests, for example, where the lives of others may be put in danger as a result of the employee’s actions. The same requirements apply to making enquiries about an employee’s criminal history.

The employer should obtain prior consent from employees before collecting private information or accessing information about employees’ use of social media during work or use of the organisation’s equipment. Organisations should make sure there are clear policies about waiving the right to privacy for work emails and private emails and social media when accessed using a work computer during working hours. These policies should be widely distributed and employees should unequivocally acknowledge and adhere to those policies.

Further, the employer should keep information collected in an investigation as secure as possible. It should only allow access by people who need access. Those who have access must be made aware of the need to treat the information confidentially and to not disclose it to others.

Must employers involve collective employee representatives?

There is no requirement to involve collective employee representatives in an investigation.

What is best practice when using social media in an investigation?

Employers should have a social media policy that governs misuse of confidential information, defamation and harassment of other employees. Further, the employer should have a policy under which employees waive the right to privacy in relation to the use of work email. Those who have access to information collected during an investigation must treat the information confidentially and must not disclose information to others.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

Generally, employers may monitor employee emails. As long as the employer has a computer or email usage policy that advises employees that there is no expectation of privacy of the organisation’s email server, the employer may review the employee’s emails.

Surveillance cameras

Brazilian law does not prohibit monitoring and supervision of employees. However, according to the labour courts, there are some restrictions that must be observed.

For example, monitoring with surveillance cameras should be used only where it is the least intrusive means to achieve the specified purpose. It may be used to prove certain actions or conduct, but it must be specific, rather than general monitoring.

The Superior Labour Court has ruled that monitoring by surveillance cameras or any other monitoring in places like dining halls, cafeterias and bathrooms is forbidden. The Court has held this violates constitutional provisions on privacy, private life, dignity and reputation.

Therefore, for an employer to monitor its employees, precautions must be taken, such as:

- the employee must be aware of the audiovisual monitoring and its purpose before installation;
- limiting the monitoring to actions that could cause damage to the organisation’s property or reputation, lead to liability on the part of the employer or be considered unlawful;
- taking all reasonable measures to ensure confidentiality, protection and proper use of the data, as the organisation could be responsible for any misuse.

Employee Tracking Devices

Many employers monitor employees through computer networks, computer programs designed to track productivity and other relatively new technological means, such as global positioning systems (‘GPS’) on employer-owned vehicles.

The employer should inform employees about the procedures in place to protect privacy, such as the ability to disable GPS devices during off-duty hours. Employers should also implement policies that outline which devices will be equipped with GPS technology, when the employees will be monitored, what information will be collected and how the information will be used.

Must the employer provide the employee with all gathered evidence?

There is no general obligation to provide all evidence gathered to the employee.
When is an employer required to conduct an internal investigation?

There are no legal requirements as to when employers must conduct internal investigations. However, if an employer becomes aware of gross misconduct by an employee and is considering summary dismissal, it will often conduct the internal investigations necessary to ensure that summary dismissal is justified. If dismissal is not justified, the employer must pay the employee his or her usual salary within the prescribed notice period and may also have to pay additional compensation to the employee, depending on the circumstances.

What are the typical subjects for employment investigations?

An employer will commence an investigation in the following situations:

- allegations of gross misconduct (e.g. theft);
- allegations of discriminatory behaviour (e.g. sexual harassment or harmful treatment of colleagues);
- whistleblowing.

How quickly must the employer conduct an investigation once it is aware of the conduct?

If the employer intends to carry out a summary dismissal as a result of the conduct, it must take quick action. Any unreasonable delay may be seen as inaction. However, the employer may carry out any necessary investigations before dismissing the employee without this being considered to be inaction.

What data privacy rules must the employer be aware of when conducting an investigation?

The law on processing employee data applies to the employer’s investigations. The following provisions, in particular, must be considered:

- the employer must only collect necessary information;
- information must not be held longer than necessary to achieve the purpose of holding it;
- the employee must be informed of the purpose for which personal data are being processed at an appropriate stage (i.e. most likely after the evidence has been gathered);
- the employer must hold the personal data securely (e.g. password protected) and ensure that only a limited group of people have access to the information.

Under Danish data protection law, the employer must have a legitimate purpose for collecting and processing personal data. The Danish Data Protection Agency has stated that suspicions of employee misconduct; the running of the employer’s business; health and safety reasons; and control measures (i.e. the monitoring of employees’ activities such as email or internet activity to ensure compliance with internal policies) may all be legitimate purposes for collecting and processing personal data. Therefore, generally, the investigation of an employee’s conduct will be considered a legitimate reason to collect and process personal data.
Must employers involve collective employee representatives?

The employer is not generally required to involve employee representatives in an investigation. However, the applicable collective agreement may say that, in certain situations, the employee representatives should be informed. An employee who is to be approached about misconduct that may lead to a summary dismissal is entitled to be accompanied by, for example, a union representative.

What is best practice when using social media in an investigation?

Normally, the employer does not have access to employee social media activity if this is private. If an employee's social media activities are public, however, the employer may have access without the employee's permission. Data protection law applies to investigations into social media. An employer may only look at an employee's profile, for example, if the employer has a legitimate purpose, for example, it suspects gross misconduct or it is conducting a control measure (i.e. the monitoring of employee activities such as email or internet activity to ensure compliance with internal policies). Before collecting and processing employee personal data as part of general monitoring or surveillance, the employer should usually inform the employee in advance. By contrast, this may not apply if there is a specific suspicion, as opposed to general surveillance.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

Employers are entitled to monitor employees’ Internet and email usage and to monitor employees using surveillance cameras as long as these monitoring activities comply with Danish law and any data protection provisions set out in applicable collective agreements. Breach of the secrecy of correspondence is a criminal offence under Danish law. Therefore, the employer must not read employees’ private letters or emails in the course of its monitoring activities. The Danish Data Protection Agency has issued an opinion on the scope of monitoring employees by electronic means. According to this opinion, monitoring activities must have a legitimate purpose and must be necessary to achieve that purpose. Legitimate monitoring purposes include facilitating the operation of the employer’s business, increasing security, investigating alleged gross misconduct or ensuring compliance with relevant guidelines and employee policies. As a general rule, the employer should inform employees of the collection and processing of employee data in advance, but if the employer is investigating a specific suspicion, it may be justified in informing the employee only after the evidence has been gathered, if the purpose would otherwise be defeated.

Camera surveillance

Generally, the employer may monitor employees using surveillance cameras. The employer must comply with Danish data protection law when processing personal data obtained by this method. This means, as a starting point, that an employer may not perform covert surveillance. Further, the employer must inform employees about any surveillance by displaying signs in an obvious place indicating to everyone entering the premises that they will be filmed. Covert filming of an employee is rare in Denmark.

Must the employer provide the employee with all gathered evidence?

There is no general requirement for the employer to provide employees with all evidence gathered. However, an employee is entitled to be informed about personal data processed by electronic means. In practice therefore, the employer must provide the employee with information about evidence gathered if the data falls within the scope of data protection law. Further, an employee may file a request for access to his or her own personal data if the processing falls within the scope of data protection law. More generally, the employer should provide the employee with information gathered in order to give him or her an opportunity to comment. It is for the employer to prove that the sanction imposed on the employee is justified. If the employee has not been given an opportunity to comment on the allegations, this may have an impact on whether a dismissal, for example, is justified.
When is an employer required to conduct an internal investigation?

There is no generally applicable direct requirement to conduct an internal investigation. There are, however, circumstances in which a failure to investigate might have adverse financial consequences so there is, in effect, an indirect requirement. Further, if an employee has committed a crime, the employer may be subject to a fine if the crime was committed in the interests of, or for the benefit of, the employer. However, a fine can be avoided if the actions were reasonable, that is, if reasonable diligence can be shown, for example, by documentation, internal controls or necessary investigations. There are also circumstances in which principles of good governance may involve an internal investigation by the employer to establish facts.

What data privacy rules must the employer be aware of when conducting an investigation?

Information collected during the course of an investigation is likely to include personal data.

Data protection principles

The data protection principles apply to investigations because of the personal data involved. The rights of the data subject, the general principles for processing personal data and the data quality principles are particularly relevant.

Necessity requirement

According to the general necessity requirement of Finnish data protection law, all personal data that are processed must be necessary for the stated purpose of the processing.

The necessity requirement is especially strict in relation to employee data and the employer may only process personal data directly necessary for the employment relationship where the processing:

- relates to managing the rights and obligations of the parties to the relationship;
- is connected with the benefits provided by the employer to the employee.

What are the typical subjects for employment investigations?

Investigations carried out by employers generally include enquiries into suspected or actual misconduct, misdemeanours, or whistleblowing by an employee regarding, for example, a corporate wrongdoing.

How quickly must the employer conduct an investigation once it is aware of the conduct?

There is no set period of time within which the employer must conduct an investigation, but criminal sanctions may later be alleviated if the employer has conducted a proper investigation, taking the time necessary to do so.
employee; or
> arises from the nature of the work.

Further, processing some categories of data, such as sensitive personal data, requires that the data subject has given his or her unambiguous consent to the processing (i.e. actively and knowingly). However, there are no exceptions to the necessity requirement, even with the employee’s or client’s consent. If the necessity of information is questioned, the onus is on the data controller to demonstrate that processing the information is required. The employer should ensure that information used is compatible with the purposes for which it was obtained.

Collecting personal data on employees

The employer must collect any personal data about employees primarily from those employees. To collect personal data from elsewhere, for example, from other employees in the organisation or through a hotline, the employer must generally obtain the prior consent of the employee.

If an employee does not give consent or it is impossible to obtain consent, an employer may collect personal data without the employee’s consent if two criteria are met:

> the information must be directly necessary; and
> the employer must have an acceptable reason for the collection related to establishing whether the employee is trustworthy.

The employer must inform the employee of the collection.

Data security

Any information collected should be held securely and should be accessible only by those who require access.

Must employers involve collective employee representatives?

There is no direct requirement to involve employee representatives in an investigation. However, if the investigation results in the setting up or alteration of technical surveillance (e.g. camera surveillance, access control, technical monitoring or changes to surveillance data systems) or other significant changes to how personal data is processed within the organisation, the involvement of an employee representative may be required.

What is best practice when using social media in an investigation?

Generally, an employer should collect personal data primarily from the employee. Other sources of information, such as the use of social media, are subject to strict and significant restrictions. Therefore, an organisation must assess whether it is able to use social media in an investigation before doing so.

When making this decision, it is especially important to ensure that the employer informs employees of the use of social media in investigations. Additionally, the employer should ensure that the information gathered from social media sources is necessary and accurate.

Must the employer provide the employee with all gathered evidence?

The employer must primarily collect personal data about the employee directly from the employee. If information about an employee has been collected from a source other than the employee, the employer must notify the employee before it is used to make decisions about the employee. This principle applies both to situations where the employee has given consent to the collection of information and when no such consent is given.

The employer has a right of access to all his or her personal data in a personal data file. Access can be denied only if one of the exceptions set out in law applies. As a result, the employee has the right to receive a written copy of all personal data on request. Note that this right to access cannot be denied based on a witness request that the information should be kept confidential.

Emails

Finnish data protection law sets out exceptionally strict provisions that must be taken into account in all situations were an employer retrieves, reads or monitors employee emails. As a result, an employer may only open emails in very limited situations. In general, before opening an employee’s email, the employer must take specific steps in advance to try to prevent the need to do so.

Additionally, the employer must confirm that the prerequisites for the individual situation are fulfilled, for example, the consent of employee could not be obtained and the matter cannot be delayed. The employer must also observe strict steps regarding the retrieval and opening of each specific message, for example, it must write and sign a report about this each time it is done.

Further, the monitoring of emails, for example, for email flow and the monitoring of an employee’s access to certain Internet sites, is subject to exceptionally strict provisions and may require prior notification to the Finnish Data Protection Ombudsman.

Camera surveillance

There are no express provisions prohibiting covert filming. However, filming an employee is subject to strict information provisions that, in practice, prevent covert filming. These provisions set out when, for what purposes and how camera surveillance may be implemented at a workplace and how the information may be used. Further, the provisions include rules on informing employees of the surveillance. Employers are required to display prominent notification of camera surveillance and the methods of implementation in areas where cameras are located.

> Must the employer provide the employee with all gathered evidence?
When is an employer required to conduct an internal investigation?

There is no generally applicable requirement to conduct an internal investigation. However, if an employee claims he or she is being subjected to harassment or ‘psychosocial risks’ (e.g. as a result of high workloads or tight deadlines), the employer must investigate the allegations. If the employer fails to do so, it may risk an employee bringing a claim for damages either based on constructive dismissal or failure to safeguard his or her health and safety in the workplace.

Further, there are circumstances in which a failure to investigate might have adverse financial consequences so there is, in effect, an indirect requirement. For example, if an employer suspects an employee of misconduct but dismisses without investigating, it may be liable to pay compensation for unfair dismissal. There are also circumstances in which principles of good governance involve an employer in establishing facts.

What are the typical subjects for employment investigations?

Investigations carried out by an employer typically involve:

- disciplinary allegations;
- a grievance raised by an employee about treatment by a manager or between two employees;
- allegations of discrimination or detrimental treatment on the grounds of a protected characteristic (e.g. gender, race, disability, religion or sexuality);
- allegations of harassment;
- allegations of psychosocial risks (i.e. employee being exposed to a risk to his or her health and safety);
- whistleblowing by an employee regarding, for example, corporate wrongdoing.

How quickly must the employer conduct an investigation once it is aware of the conduct?

There is no set period of time within which an employer must conduct an investigation but it is expected to act reasonably quickly. For a disciplinary investigation, the employer must act (i.e. invite the employee to a disciplinary interview) within two months of becoming aware of the conduct. How long an investigation takes will depend on matters such as complexity, the nature of the allegations, the number of people to be interviewed and the availability of the interviewees.

What data privacy rules must the employer be aware of when conducting an investigation?

Information collected in the course of investigations is likely to include significant personal data. The data protection principles apply. Particularly relevant are the duty to process fairly and to use the information only for specified purposes. An employer should ensure that processing is consistent with the legal processing conditions including those for sensitive data where relevant. In most contexts, the relevant condition will be that the processing is
necessary for the legitimate interests of the data controller.
The nature of the information processed and the use of personal data must not be disproportionate to the seriousness of the matter being investigated.
The duty to process information fairly generally involves listening to what the employee says before making a decision.
Any information collected should be held securely and accessible only to those who need access to it.

Must employers involve collective employee representatives?

There is no requirement to involve employee representatives in an investigation. It is, however, good practice to inform or consult and, in some cases, involve representatives in the investigation.

Note that the employer should investigate with health at work committee members where there is a claim of harassment or ‘psychosocial’ risk (e.g. as a result of high workloads or tight deadlines) or when there is a serious and imminent danger at work.

What is best practice when using social media in an investigation?

Accessing social media used by an employee in a private context is intrusive. Before doing so, an employer should:

- have specific reasons for accessing social media;
- consider if it is necessary to do so (i.e. whether there is a proper reason or whether it is simply travelling for information);
- consider what the employee has been told about the use of social media and what his or her expectations are likely to be;
- consider applicable rules on the use of social media;
- consider whether access to social media is public or private as this is a key consideration under law (e.g. Twitter is considered public, Facebook can also be considered public, depending on who has access).

If an employee has publicly criticised the organisation on social media, an investigation will be easier to justify. The employer should ensure that processing is consistent with legal processing conditions including those for sensitive data, where relevant.

In most contexts, the relevant condition will be that the processing is necessary in the legitimate interests of the data controller or a third party. If so, the employer should identify its legitimate interest and consider whether the interest is outweighed by prejudice to the rights of the data subject.

Only in serious cases would it be justified for the employer to view a social media site used for personal purposes. For example, it might be justified if a group of employees use social media to make racist or sexist remarks about colleagues.

Groundwork to enable use of social media

Employers should have a policy on the use of social media as it affects work, it should ensure employees know the policy and should set out expectations clearly in terms of what behaviour is acceptable. If limited private use of social media is permitted at work, employers should be clear about what is meant and to what extent the use is private. Bullying colleagues, making detrimental remarks about customers or colleagues or raising work-related grievances publicly would normally be prohibited.

Before introducing a policy, the employer must consult staff representatives (i.e. works council members and health at work committee members) and inform employees (i.e. preferably through an agreement with employee representatives). Consultation will avoid the risk of staff feeling unable to express themselves and will ensure that staff and managers feel protected from online bullying.

Social media sites are sometimes used to air complaints because employees find it difficult to speak to a manager. Employers should ensure that there is proper dialogue. One approach is to organise one-to-one meetings with managers.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

To read an employee’s emails, an employer must ensure that its actions are authorised by the law on interception of communications and that reading the emails complies with data protection law and with the internal rules of the organisation.

Interception for business purposes is authorised when emails are exchanged on work computers. The only exception is when the employees specify that the email is confidential. In this case the employer should invite the employee to be present before opening the email.

If interception is authorised, the employer should consider the data protection implications. The employer should ensure that a processing condition is satisfied before accessing emails. The employer should ensure that accessing the email complies with the data protection principle relating to fairness. In general terms, as long as the employer is investigating in connection with a serious allegation regarding the business, reading the email should be permitted.

Camera surveillance

Covert filming is particularly intrusive and not only in relation to the person under investigation. Before initiating filming, an employer should consider whether its purpose can be achieved without filming or without continuous filming and in a less intrusive way. The employees must be informed about the possibility of being filmed.

Further, an employer should ensure that filming is consistent with the data protection principles and that a processing condition is satisfied. If the public are to be filmed, the employer may need to declare the presence of the cameras to the local authority.

The condition for processing will normally be that the covert filming is necessary for the legitimate interests of the employer and that, in the particular case, the interest is not outweighed by prejudice to the rights of the data subject.

Because covert filming is so intrusive, except when investigating particularly serious allegations, the data subject’s rights may well outweigh the employer’s interests in filming.

Must the employer provide the employee with all gathered evidence?

There is no general obligation to provide all evidence to the employee. However, the employer must act fairly. It must provide the employee with any information that is relevant to the matter being investigated. There is no need to provide information collected that is not relevant.

Employees sometimes say they will provide evidence but only if the employer will keep it confidential. In general employers should not agree to this.

If a witness requests confidentiality, an employer may try to agree an approach, for example, by saying it will try to keep it confidential but may need to release it for use in court proceedings.
When is an employer required to conduct an internal investigation?

There is no explicit regulation of internal investigations in Germany, although there is a legal obligation on stock companies to set up a monitoring system for misconduct, breaches of the law and criminal activity. However, there are circumstances in which a failure to investigate might have adverse financial consequences so there is, in effect, an indirect requirement. For example, if an employer suspects an employee of misconduct but dismisses the employee without properly investigating, it may be liable to make a voluntary severance payment in order to end any litigation. This is usually approximately half the gross monthly salary per year of employment, but it can be much more, depending on the facts and the employee’s demands. If a settlement agreement cannot be reached and the dismissal is considered unfair by the court, the employee is entitled to reinstatement. Further, there are circumstances in which the principles of good governance involve an employer in establishing the facts so as to decide on what further steps to take.

What are the typical subjects for employment investigations?

Investigations are generally carried out for reasons involving:

- a violation of the law or a criminal offence (e.g. theft or corruption);
- fraud against the employer (e.g. misreporting travel costs or working time);
- allegations of discrimination, for example, sexual harassment or detrimental treatment on the grounds of a protected characteristic (e.g. gender, race, disability, religion or sexuality);
- online misconduct;
- insults in the workplace;
- whistleblowing by an employee regarding, for example, corporate wrongdoing.

How quickly must the employer conduct an investigation once it is aware of the conduct?

There is no set period of time within which an employer must conduct an investigation in Germany. However, an employer is expected to act reasonably quickly. Under German law, a summary termination without notice (for cause) may only be carried out within two weeks of the employer becoming aware of the facts. Usually, this timeframe does not end until the investigation is complete, but the employer should conduct the investigation as quickly as possible to avoid legal risks, and especially to avoid the unlawful dismissal of an employee. In practice, internal investigations often lead to termination for cause. Typical reasons are:

- criminal offences, if they burden the employment-relationship and destroy trust;
- unauthorised absence for a long period;
- unauthorised annual leave;
- falsely claiming sick leave.
What data privacy rules must the employer be aware of when conducting an investigation?

As information collected in the course of investigations is likely to include significant employee personal data, the investigation must comply with German data protection law. As it is normally considered that consent is not given freely in the employment context - especially in relation to an investigation against an employee - the employer must ensure that it complies with data protection law.

The law says an employee’s personal data may be collected, processed or used for employment-related purposes where this is necessary for hiring decisions or for carrying out or terminating the employment contract. Employees’ personal data may be collected, processed or used to investigate criminal offences only if there is a documented reason to believe the data subject has committed a crime while employed; the collection, processing and use of the data is necessary to investigate the crime; and the employee does not have a legitimate interest that overrides the purpose of collection, processing or use. The type and extent of the processing must be not disproportionate to the purpose.

Therefore, in most contexts, the most relevant condition will be that the data processing must be necessary in the legitimate interests of the employer (e.g. suspicion of criminal activity). The nature of the information processed and the use of personal data must not be disproportionate to the seriousness of the matter being investigated. There is also a duty to process fairly, which involves listening to what the employee says before making a decision (e.g. to dismiss).

Investigations involving telecommunications such as email and the Internet give rise to specific legal difficulties in Germany. If the employer allows personal use of the organisation’s email account or Internet access, there is a strong legal view that any resulting investigation must be conducted in accordance with stricter requirements of telecommunications law – which are stricter. In our experience, the vast majority of German employers do allow private use of email and the Internet, despite the legal issues this may create for investigations.

Note that any information collected should be held securely and made accessible only on a ‘need to know’ basis.

Must employers involve collective employee representatives?

If there is an internal data protection officer within the organisation, he or she should be informed before any investigation to give guidance on data protection. (This will apply if more than nine employees have access to automatically collected personal employee data or if more than 20 employees have access to personal employee data collected in other ways.)

The data protection officer should be told about the reason, purpose, investigation procedure, affected employees, data recipients and any data transfer to third countries.

If there is a works council it should also be notified. The circumstances of each case will determine when and to what extent it should be informed. Recent German case law suggests that before contacting the works council, the employee under investigation should be told of the allegations and given the chance to react (e.g. by confessing), so as to avoid the need to disclose the matter to the works council. Trade unions do not need to be involved in internal investigations.

What is best practice when using social media in an investigation?

There is no law on the use of social media in Germany and a review of German data protection law has been shelved until the EU Regulation is finalised. Therefore, the investigation of social media must be consistent with the general principles of German data protection law. This means that only in exceptional cases is it justified for an employer to view or access a social media site used by an employee for personal purposes.

If the employee has not given prior consent, there is no single answer as to whether the employer can investigate social media activities. If the employer does not allow use of the Internet at work for reasonable personal use (i.e. only about 10% of German employers) the employer can investigate Internet or social media activities if it acts in accordance with data protection law. This means that the investigation must be necessary in the legitimate interests of the employer (e.g. suspicion of criminal activity). The employer should identify the legitimate interests and consider whether those interests are outweighed by prejudice to the rights of the employee. The investigation of social media use by an employee in a private context is very intrusive and a serious encroachment on the employee’s personal rights. Therefore, the employer should be specific about its reasons for accessing social media and consider if it is really necessary to do so. The employer should consider whether there is a proper reason or whether it is simply trawling for information. Further, the employer should consider what the employee has been told about the use of social media (e.g. the content of policies on social media use) and what the employee’s expectations are likely to be.

By contrast, if the employer allows employees to use workplace Internet access for personal use, there is a strong legal view that it must meet the stricter regulations relating to telecommunications. These make it unlawful to investigate ‘live’ social media activities or access active social media accounts. However, after the data transmission, the investigation of stored social media data may be lawful where necessary in legitimate interests of the employer.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

The question of whether the employer can investigate telecommunications, such as reading employees’ emails has no simple answer. If the employer does not allow employees to use the organisation’s email account for personal use – and this is rare - the employer may read the employee’s emails under data protection law if this is necessary in its legitimate interests. If the employer allows personal use of the organisation’s email account – which is usually the case - most legal commentators believe the employer can be seen as a telecommunications provider, which means it is required to meet strict telecommunications regulations. By these, it is only lawful to investigate emails that have already been opened, stored or printed in paper form. It is largely unlawful to read unopened emails, the live transmission of email data or to investigate an employee’s private email account.

Camera surveillance

Covert filming is particularly intrusive and is a serious encroachment on the employee’s personal rights. It is therefore only lawful in exceptional cases. Normally, covert filming must be necessary in the legitimate interests of the employer and its interests must not be outweighed by the rights of the employee. Therefore, before starting to film, an employer should consider whether its purpose can be achieved without filming, and in a less intrusive way. Covert filming should only be considered as a last resort.

Finally, covert filming - including audio transmission - may constitute a criminal offence by the employer under German criminal law, if it is not justified by a clear suspicion of a serious crime by the employee.

17
Must the employer provide the employee with all gathered evidence?

There is no general obligation to provide any evidence to the employee. Therefore, the employer may provide the employee with only an extract of an investigation report, rather than the entire report. The employer only needs to give the employee sufficient information to enable him or her to prepare for a case at a disciplinary hearing or termination. Generally, it is not necessary to provide the employee with a written investigation report. However, the employer must act fairly. For example, if the employer considers a termination or substantial change to working conditions for an employee based on an investigation, the employee has a right to be given sufficient detail to be able to fully understand the case against him or her and to comment on the outcome. This need not necessarily be in writing but the written form might be helpful for evidential purposes. Further, in the course of litigation, it is the employer’s duty to prove the allegations that have led to termination. This typically requires disclosure of the result of the investigation and an explanation to the court about how the investigation was conducted.

Employees sometimes say they will provide evidence, but only if the employer will keep it confidential. In general, employers should not agree to this because if information has been provided in confidence this may mean the employer cannot use it, as it would be both unfair to rely on it and unlawful.

If a witness requests confidentiality, an employer should try to agree an approach, for example, by saying it will try to keep it confidential but cannot promise confidentiality. Alternatively, just the person’s name could be kept confidential or certain matter redacted.
When is an employer required to conduct an internal investigation?

There is no general requirement to conduct internal investigations. However, if, for example, the employer believes that an employee has breached an employment obligation, before terminating the employment or taking disciplinary action, the employer should investigate the circumstances. If, as a result of the investigation, it is proved that the employee has breached an employment obligation, this may result in the termination of the employment or in disciplinary action.

What are the typical subjects for employment investigations?

Investigations carried out by an employer typically involve:

- disciplinary allegations;
- allegations of discrimination (e.g. sexual harassment or detrimental treatment on grounds of a protected characteristic);
- whistleblowing by an employee regarding, for example, corporate wrongdoing.

How quickly must the employer conduct an investigation once it is aware of the conduct?

There is no specific timeframe within which an employer must conduct an investigation under employment law, but the employer should do so relatively quickly. If it is alleged that the employee has seriously breached a significant obligation arising from the employment, this may result in the termination of employment with immediate effect. The employer has 15 days to serve the termination, from the point it becomes aware of all the circumstances. Therefore, the investigation must be completed to meet the deadline.

What data privacy rules must the employer be aware of when conducting an investigation?

The employer may carry out investigations in connection with the behaviour of the employee, but the methods used during such investigations must not interfere with the employee’s dignity.

The data protection principles apply. These provide that personal data must:

- be processed fairly, lawfully, accurately and in compliance with law;
- be obtained only for specified and lawful purposes and not processed in a way that is incompatible with those purposes;
- be adequate, relevant and not excessive.

Particularly relevant are the duties to process personal data fairly and use it for specified purposes. The nature of the information processed and the use of personal data must not be disproportionate to the seriousness of the matter being investigated.

Must employers involve collective employee representatives?

There is no obligation in labour law to involve employee representatives in internal investigations. However, if there are rules about this in an applicable
collective bargaining agreement or its internal policies, the employer may be obliged to involve employee representatives in an investigation.

What is best practice when using social media in an investigation?

Under the Data Protection Authority’s guidelines, the employer may only freely monitor Internet usage of employees if private use has been prohibited and the employees are aware of this. The employer may, for example, prohibit access to certain websites at work. The employer should create policies about this, addressing the following issues:

- the employer should set out clearly and explicitly its expectations about the kind of behaviour that is acceptable or unacceptable, and ensure employees are aware of this;
- if limited private use of social media is permitted at work, employers need to be clear what this means and to what extent the use is private;
- the employer should make it clear that bullying colleagues, making detrimental remarks about customers or colleagues or raising work-related grievances publicly is prohibited.

Even if use of the Internet is not limited and there is no policy in place, both during working hours and outside of work, employees must not behave in a way that directly jeopardises the economic interests of the employer (e.g. by making damaging statements through social media sources).

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Employers are entitled to monitor employees’ activities in the workplace. However, the monitoring must be directly connected to the employment and the employer must inform employees about the monitoring and the methods used. Therefore, the employer should include the rules about monitoring and the methods used in a separate, detailed policy. The monitoring rules must comply with the principle of balancing the interests of the employer and employee. They must also allow for accountability.

Email

In terms of monitoring email, only automatic controls on the type of attachments sent with emails and virus scans are permitted. The content of emails must not be controlled or read by the employer even if sent from an employee’s work address. This is because to do so would infringe the personal rights of the recipient.

However, if data security or the security of the IT system is at risk, the IT system administrator may review the content of emails. He or she must not automatically forward the content to the employer, but if the email address is only intended for business purposes, the employer may check the name of the sender, the addressee and the subject of the email. If the employee cannot provide further information on the content of the email, ultimately the entire content of the email may be disclosed to the employer.

Further, the employer may list addresses from which employees must not accept emails and may limit the size of attachments.

Camera surveillance

Covert filming is not permitted, but the employer is entitled to use electronic surveillance cameras for monitoring if it can demonstrate compliance with data protection law. To do this, the employer must inform employees about the camera surveillance, but their consent is not required.

Note that general information about the surveillance is not sufficient. The employees must be given a detailed description of the legal basis and purpose of surveillance; the area covered by it; the people operating the surveillance system; the location where recordings will be kept and how long for; any data security measures to be taken; the people allowed access to the data collected; the rights of the employees in connection with the surveillance and how to exercise them.

The only absolute restriction on the use of surveillance cameras is that it must not be harmful to human dignity. The prime objective of the use of the cameras must be to protect the life, safety and freedom of employees and the employer’s business secrets.

Must the employer provide the employee with all gathered evidence?

It is not mandatory to provide the employee with any evidence. However, any termination of employment or disciplinary action taken must include reasons. The employee may apply to the court to challenge the reasons. The employer must be able to prove that the reasons were accurate and proportionate.
When is an employer required to conduct an internal investigation?

In India, an employer is generally required to conduct an internal investigation into an employee if there is alleged misconduct or significant insubordination. An employer must carry out a fair investigation, following the principles of natural justice into misconduct before taking any action against the employee.

What are the typical subjects for employment investigations?

The following could be treated as misconduct, but this would need to be confirmed through an investigation:

- significant insubordination;
- intentional insubordination, disobedience or neglect of work;
- theft, fraud or dishonesty towards the employer’s business or property;
- intentional damage or loss of the employer’s goods or property;
- taking or giving bribes or any ‘illegal gratification’; and
- convictions for a criminal offence.

How quickly must the employer conduct an investigation once it is aware of the conduct?

Under employment law that applies to organisations and/or industries at state level and generally only covers blue-collar employees, there is a time limit of up to three months to complete an investigation. However, the time limit may be extended for a further three months.

In cases where the law does not apply, the investigation should be completed within a reasonable period. For white-collar employees there is nothing to stop the employer completing an investigation in a shorter period. However, it should not be done in haste. With respect to sexual harassment at work the law requires the investigation to be completed by a special internal complaints committee, within 90 days.

What data privacy rules must the employer be aware of when conducting an investigation?

Except in relation to sexual harassment, there are no specific data privacy duties that must be complied with by the employer while conducting an investigation. However, if during the course of the investigation, the employer collects sensitive personal data (e.g. passwords, financial information, health status, sexual orientation, medical records and biometrics records), certain requirements under technology law must be met. These are that before collecting any sensitive personal data the employer must obtain the data subject’s consent to the purpose of use. The information must therefore be collected for a lawful purpose connected to a function or activity of the employer. The employer should also obtain the permission of the employee if it wishes to transfer the data to any third party. Finally, the employer must ensure that the information is kept securely and protected from unauthorised access, damage, use, modification, disclosure or impairment.

In an investigation relating to sexual harassment, all the parties to the investigation must maintain confidentiality in relation to the identity and address of the aggrieved person, respondent and witnesses, any information
relating to conciliation and inquiry proceedings, the recommendations of the internal and local committees and the action taken by the employer or district officer.

Must employers involve collective employee representatives?

There is no legal obligation to involve employee representatives in an investigation. However, where employment law allows, the employee may be accompanied by a colleague or representative of a trade union. If the law does not provide for this, the employee may be accompanied by a representative if prior permission has been given by management. For complaints of sexual harassment, if prior permission is given by the internal complaints committee, the employee may be accompanied by a colleague.

What is best practice when using social media in an investigation?

Accessing social media used by an employee in a private context is intrusive. Therefore, before doing so, an employer should:

- check that the reason for accessing the social media of the employee is specific and unambiguous;
- ensure access is only granted where absolutely necessary and is supported by a reasonable explanation;
- consider what the employee has been told about use of social media and what his or her expectations are likely to be.

Employers should have detailed policies concerning employees and their conduct at the workplace or outside. Policies on the use of social media should be limited to what is relevant for work. Employees should be aware of the behaviour that is considered acceptable in the use of social media. If limited private use of social media is permitted at the workplace, employers must explain in their policy to what extent the use will be considered private.

Bullying colleagues, making detrimental remarks about customers or colleagues or raising work-related grievances publicly would normally be prohibited by employers.

Before introducing a new policy it is good practice to notify employees and employee representatives and agree on any new terms that may amount to a change in employment conditions.

Social media sites are sometimes used to air complaints because employees find it hard to speak to a manager. Employers should ensure that employees can voice complaints in the workplace and be given a timely response. One approach is to organise one-to-one meetings with managers.

Must the employer provide the employee with all gathered evidence?

In order to give a fair opportunity to an employee under investigation:

- the management or the employer must supply the list of witnesses to the employee during the investigation;
- copies of the documents relied on must be supplied to the employee, so that he or she has an opportunity to make submissions on the truth of the documents;
- the employee must be allowed to cross-examine the witnesses; and
- the employee must be permitted to inspect the documents relating to the allegations against the employee.

If the employer does not satisfy these requirements, an employee can challenge the action, decision or outcome of the investigation.

Camera surveillance

Before filming an employee, the employer must consider whether it is necessary to collect film evidence against the employee or whether this can be avoided. Most organisations inform employees before they start work that they will be filmed on a daily basis and that the footage could later be used against them during an investigation into allegations of misconduct or sexual harassment. If there is no standard policy to which an employee has consented in writing, the employer should obtain prior written consent from employees before beginning filming.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

There is no law on the subject of email monitoring in India. Therefore, an employer may access official emails of an employee, but to avoid claims of violation of privacy, should give the employee prior notice of the employer’s right to access the emails and should have obtained the employee’s acknowledgement of this right.
When is an employer required to conduct an internal investigation?

There is no generally applicable requirement to conduct an internal investigation. However, employers must act reasonably and follow internal policies, practices or procedures which may provide that an internal investigation will be conducted in certain circumstances. In many situations, for example where an employee raises a grievance or makes an allegation of bullying and harassment against another employee, the employer will not be able to act fairly and reasonably without conducting a thorough and fair investigation.

What are the typical subjects for employment investigations?

Typical subjects for investigations include:

- disciplinary issues;
- grievances raised by employees;
- allegations of discrimination (e.g. on the grounds of gender, civil status, family status, race, disability, age, sexual orientation, religious belief or membership of the Traveller community).

How quickly must the employer conduct an investigation once it is aware of the conduct?

There is no fixed timeframe within which an employer must conclude an investigation, however, it should seek to conduct the investigation efficiently and without undue delay. The length of the investigation will depend on various factors including the number and nature of the allegations, the number of witnesses and the availability of those witnesses.

What data privacy rules must the employer be aware of when conducting an investigation?

At the beginning of an investigation, an employer should identify any personal data it holds about individuals affected by the investigation, such as employees, customers or clients. Under data protection law in Ireland, personal data means data relating to a living individual who is or can be identified either from the data on its own or with other information that is in, or is likely to come into the possession of the data controller. Sensitive personal data are specific categories of data about an individual’s racial origin, political or religious beliefs, trade union membership, health, sexual life, criminal convictions or the alleged commission of an offence. Sensitive personal data must not be processed by a data controller except where certain criteria are met, so an employer must check if an investigation satisfies one or more of those criteria before it can lawfully collect and use that information.

A data controller controls the content and use of personal data. An employer is a data controller under law which makes various European data protection laws part of Irish law. An employer must also respect employees’ privacy rights under the Constitution of Ireland, the European Convention on Human Rights and the Charter of Fundamental Rights of the European Union.

In processing personal data in an investigation, an employer must ensure that:
the investigation is limited to a legitimate purpose and personal data is processed for that specific purpose;

- there are appropriate procedures in place which are proportionate to the purpose of the investigation and which safeguard the rights and interests of the data subjects;

- individuals whose personal data is processed are, to the extent reasonably practicable, notified of the purposes of the investigation;

- personal data confidential to the investigation, is kept secure and used only for the purpose of that investigation;

- personal data gathered for the investigation is not be retained once there is no longer a legitimate reason for retention; and

- personal data is not transferred unlawfully within the organisation or to a third party outside of the organisation.

Must employers involve collective employee representatives?

There is no generally applicable requirement to involve employee representatives in an investigation. Employers, however, should comply with internal policies and practices, which may allow for the involvement of collective employee representatives.

What is best practice when using social media in an investigation?

An organisation may monitor employee use of social media at work provided it does so transparently and not systematically or excessively. An employer should be aware that collecting, recording, using or disclosing information about an employee taken from a social media platform constitutes processing personal data under data protection law.

To avoid a breach of data protection or privacy laws, an employer should have a clear written policy about permitted use of social media websites by employees using the organisation’s IT systems or when managing or interacting with social media websites. The policy should, at a minimum:

- state who will have access to social media on behalf of the employer;

- set out what falls within acceptable use and have a definition of unacceptable use;

- clearly state the specific purpose for any monitoring of social media use; and

- state that if monitoring reveals a breach of acceptable use then that information may be used in disciplinary proceedings.

Employment contracts and disciplinary policies should also clearly set out an employer’s expectations in relation to the employee’s use of social media at work.

Employees should also receive regular training on the use of social media and this training should highlight the monitoring practices of the employer. It is also important to consider whether an employee’s social media use is in an employment or private context as this will be relevant to whether use of the personal data is permitted in an investigation. The use of recording mechanisms to obtain personal data without an employee’s knowledge is generally unlawful. An employer should create and clearly prescribe its policies in this area from the outset, inform employees of its approach and take care that any monitoring of social media use is proportionate and reasonable.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Must the employer provide the employee with all gathered evidence?

An employer must act reasonably and fairly and, as such, should provide the employee with a copy of all relevant evidence gathered that the employer wishes to rely on in the context of the investigation. Data protection laws give an individual a right of access to his or her personal data if he or she requests it and that right applies to employee data.
When is an employer required to conduct an internal investigation?

There is no requirement under law to conduct an internal investigation. Internal procedures on investigation might be useful, however, in specific areas such as health and safety or data protection. Privacy and employment law set limits on investigations and accessing data.

What are the typical subjects for employment investigations?

The employer must verify the facts in disciplinary procedures before issuing a warning letter (i.e. this is compulsory before a disciplinary dismissal). Therefore, a duty to verify, rather than investigate, arises. Employers must protect and act in cases of threats to the health of employees. These measures are necessary for alleged risks or misconduct. Investigations are usually carried out in relation to unlawful or damaging behaviour that occurs outside the scope of the employee’s duties. Note that the monitoring of performance under the contract follows different rules. In Italy there is no whistleblowing law. However a draft law is in Parliament waiting to be discussed. The only relevant regulation in this area is general and limited to the public sector.

How quickly must the employer conduct an investigation once it is aware of the conduct?

There is no specific timeframe within which an employer must conduct an investigation. Disciplinary warning letters, however, must always be timely and be served shortly after the facts are established, to protect the employee’s right to defend the allegations. The time it takes to establish the facts will vary (e.g. investigating fraud may take months but investigating a fight should not). Once the facts are known, they must be put to the employee in writing in the form of a disciplinary warning letter and this has the effect of starting the disciplinary procedure. At the end of this, the employer might impose sanctions, ranging in severity up to dismissal for cause. It must be noted that the investigation and the disciplinary procedure are separate and the latter can be based on the outcome of the investigation.

What data privacy rules must the employer be aware of when conducting an investigation?

There is a general duty to provide employees with information on the scope and purpose of the processing and about the data processed. The processing must be limited to the specific purpose and carried out with notice and consent. A reform enacted in September 2015 provides a duty to inform employees about possible monitoring and its consequences, and expressly mentions the requirements of privacy law. The reform gives a new emphasis to procedure and information rights. Investigations into misconduct must also be performed under privacy and data protection legislation, though these investigations may be done by third parties. There are few exceptions to the general rules and these must be managed carefully. All the general duties, including proportionality, fairness and protection of data, apply to investigations.
Must employers involve collective employee representatives?

There is no general duty to involve trade union or employee representatives in an investigation. However, note that if an employer wishes to install and manage long-distance monitoring devices for security, protection or organisational reasons (such as cameras and other monitoring tools), a compulsory procedure must be followed involving trade union representatives.

What is best practice when using social media in an investigation?

All employers should have an internal policy relating to social media that sets out the possible disciplinary action for misconduct. It is preferable for the policy to be signed by each employee or attached to the employment contract. Accessing a private social media profile is intrusive but if the information is passed to the employer by third parties (e.g. clients) or if access to the profile is not restricted, it can be used. There are various trends in case law with regards to social media use, but the main point that can be drawn from it is that information on non work-related subjects should be deemed irrelevant and in most cases cannot be used in the context of the employment relationship.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

Until September 2015, there was a general prohibition on ‘long distance’ monitoring of employees’ activities. This included email use and investigation work, if it related to the performance of employment duties. Case law provided exceptions to this when dealing with ‘defensive checks’, (i.e. checks carried out to protect the company’s assets or industrial secrets). This general prohibition has changed. New law divides long distance monitoring tools in two categories: those installed for safety, security or organisational reasons and those that amount to ‘work tools’ given to the employee to be used for work. To use the first category of tools, permission needs to be obtained under a collective agreement. For the second, the requirement is communication to the employee about the possible monitoring of the activity using the tools. If the above conditions are met, the use of data from the tools is considered fair. However, it remains to be seen what practical impact the new law will have on company practice and court decisions.

Camera surveillance

Camera surveillance falls within the first category of monitoring tools and therefore requires collective agreement before the cameras can be installed in the workplace.

Must the employer provide the employee with all gathered evidence?

There is no general obligation to disclose information to employees. Often access rights under privacy law can be invoked to obtain information, although data processed to defend proceedings before the courts are exempt from disclosure. The full results are only usually revealed before the courts during proceedings. Once the employment relationship is over, checks can be carried out to confirm
When is an employer required to conduct an internal investigation?

Employers are required to carry out an internal investigation if there is an allegation of sexual harassment or bullying and harassment in the workplace. Further, in the financial sector, if an employee blows the whistle on practices at the employer, the employer must carry out an internal investigation. In some other cases too, it may be good practice to conduct an investigation. For example, it is advisable to establish there is evidence of misconduct before taking disciplinary action (e.g. for theft).

What are the typical subjects for employment investigations?

Investigations carried out by an employer typically involve:

- allegations of sexual harassment;
- allegations of bullying, harassment and direct or indirect discrimination on the grounds of protected characteristics (i.e. religion, convictions, disability, age, sexual orientation, assumed or actual membership of a race or ethnicity and gender);
- whistleblowing by an employee regarding, for example, bribery or corporate wrongdoing;
- disciplinary allegations (e.g. allegations of theft, mismanagement and malpractice).

How quickly must the employer conduct an investigation once it is aware of the conduct?

There is no set period of time within which an employer must conduct an investigation but it is expected to act reasonably quickly. How long an investigation takes will depend on matters such as complexity, the nature of the allegations and the number of people involved and to be interviewed.

What data privacy rules must the employer be aware of when conducting an investigation?

Internal investigations must comply with the data protection principles, which require fair processing of data, specified and legitimate purposes and compliance with the requirement of proportionality. An internal investigation must be carried out while observing the data subject's fundamental rights, including privacy. Therefore, the rights of any affected employee, including the employee who is subject to the investigation must be protected by respecting privacy, confidentiality and the right to access and correct the data being processed and to challenge the allegations. The processing of personal data linked to an internal investigation must be fair and lawful. Therefore, an employer conducting an internal investigation must not use unlawful or unfair methods such as covert surveillance or eavesdropping.

Further, the employer must have a legitimate purpose. In the context of bullying or violence at the workplace, for example, the employer can easily demonstrate a legitimate purpose for conducting an internal investigation in particular, in terms of its obligation to protect employees’ health and safety. The employer must ensure continued compliance with the principle of proportionality. This principle requires that personal information is processed
only where necessary for the purposes of the internal investigation, that is, to determine whether the allegations are substantiated. The least intrusive means of processing must be used.

Must employers involve collective employee representatives?

For sexual harassment, staff delegates must be involved in the investigation if the employee alleging the sexual harassment requests. The employer may exercise the right to be accompanied by a staff delegate during interviews with the employer.

The some industry agreements expressly require the direct involvement of staff representatives in writing relevant procedures and prevention policies and for conducting subsequent internal investigations.

The employer should involve collective employee representatives at each step of the internal investigation to avoid a dispute about the reliability of the methods used for the investigation.

For example, certain industry agreements encourage the involvement of staff representatives to prevent and manage bullying or violence at work, by ensuring participation in drafting relevant procedures.

What is best practice when using social media in an investigation?

There are no specified rules on how the employer may use social media in an internal investigation.

However, the employer must comply with legal and general privacy and data protection requirements. These requirements prohibit unfair or unlawful acts resulting in privacy or data protection breaches. Further, the use of social media while conducting internal investigations must be proportionate to the objective of discovering the truth of the allegations.

The employer must ensure it adheres to the following:

- it uses the least intrusive source of information;
- accesses information through social media fairly and lawfully (e.g. by not using covert monitoring and only using information made publicly available on social media);
- the collection of data through social media must only be aimed at specific employees where strictly needed for the purpose of evidencing the allegations that triggered the internal investigation;
- there must be no use of personal information that exceeds the scope of the internal investigation.

The employer must consult with employee representatives to create clear procedures on how to carry out internal investigations by detailing the circumstances under which investigations may involve the use of social media.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

According to data protection law and the national Data Protection Authority, under no circumstances may the employer read an employee’s emails that are expressly labelled as private or that are obviously private. This is the position even where those emails are sent or received or stored on work devices and servers.

In principle, the employee’s professional emails may be subject to control by the employer. However the national Data Protection Authority has taken a very restrictive interpretation of the law. Individual controls of emails can only take place as a further step, where the employer has identified or has a sound suspicion of misuse of the work email system.

On this interpretation, an employer may read an employee’s work emails on work devices and servers provided that the employer is able to evidence sound suspicion of wrongdoing or misconduct.

However, note that this practice may fall within the definition of surveillance of the use of the email by the employer, which requires prior authorisation from the Data Protection Authority. The employee must be informed that the employer may monitor the use of email and, in some cases may carry out checks at an individual level.

Camera surveillance

Covert filming may be considered a breach of privacy and data protection laws, and this expose the employer to criminal liability.

Data protection law allows monitoring in the workplace through video surveillance, but only under very restrictive conditions. This type of surveillance must have prior authorisation from the national Data Protection Authority and must never be used to permanently control the individual’s actions or movement. Further, in the case of a dispute, film captured covertly is likely to be regarded as inadmissible and as constituting unlawful evidence.

Must the employer provide the employee with all gathered evidence?

There is no requirement to provide the employee with the evidence gathered. The only obligation on the employer is to give the employee rights of access to and correction of his or her personal data.

This requirement is the same as the right of access and correction granted to any individual whose personal data are processed. In addition to these rights, common sense may dictate that the employer should provide the employee with relevant evidence in order to enable him or her to respond and provide an explanation.

Access to gathered evidence must be balanced with the right to privacy of other individuals involved in the internal investigation.
When is an employer required to conduct an internal investigation?

Although conducting internal investigations is not required by law, once an employer receives a complaint about harassment, discrimination, or retaliation, it must take prompt action to investigate, correct and prevent the behaviour. Under Mexican federal employment law, the employer must not take part in or allow discrimination or harassment in the workplace. Further, actions by the employer that may undermine the employee’s dignity may result in termination of the employment relationship, with liability on the employer. Internal investigations become important as they may provide evidence if a claim is brought.

The employer may conduct investigations related to employee misconduct, for example, theft, violence and use of controlled substances at work. If misconduct is found to have taken place, the employer may terminate the employment relationship without liability. If the employee makes a claim against the employer, the burden of proof will be on the employer.

What are the typical subjects for employment investigations?

Investigations that employers most commonly carry out involve:

- allegations of harassment or discrimination on the grounds of a protected characteristic (e.g. sex, pregnancy, race, colour, ancestry, citizenship, religion, national origin, age, marital or medical status, sexual orientation, disability, or any other characteristic protected by law);
- allegations of sexual harassment by a colleague, manager, vendor or client;
- allegations of retaliation against an employee (e.g. when the employee is refused a salary increase or different work schedule).

How quickly must the employer conduct an investigation once it is aware of the conduct?

Although there are no set rules for conducting investigations, employers should conduct investigations promptly. For disciplinary measures to be applied, there is a time limit of one month for employers to terminate the employment relationship without liability, which begins the day after the employer becomes aware of the cause.

Features of a fair, impartial, and thorough investigation include:

- beginning the investigation promptly;
- having a policy for how investigations will be handled;
- hearing both sides and providing the employee with a fair opportunity to respond;
- providing the alleged wrongdoer with a reasonable opportunity to defend the allegations;
- making any findings on objective evidence.

What data privacy rules must the employer be aware of when conducting an investigation?

Information collected in the course of investigations is likely to include significant personal data and sensitive personal data. Sensitive personal data are data related to the most private aspects of the data.
subject’s life or where misuse might lead to discrimination or involve a serious risk. In particular, sensitive data may include characteristics such as racial or ethnic origin, present and future health status, genetic information, religious, philosophical and moral beliefs, union membership, political views and sexual preferences.

The data protection principles of lawfulness, consent, information, quality, purpose, necessity, proportionality and accountability apply.

An employer should:

- check its privacy notice provides information to data subjects on processing and its purposes and informs employees of the possibility of internal investigations;
- ensure that processing is consistent with the statutory processing conditions including those for sensitive data, where relevant.

By law, when processing sensitive personal data, the data controller must obtain express written consent from the data subject.

The nature of the information used and use of personal data must not be disproportionate to the seriousness of the matter being investigated.

The employer should ensure that information is processed only for purposes compatible with the purposes for which it was obtained.

Any information collected should be held securely and accessible only to those who need access. The data controller must establish and maintain physical, technical and administrative security measures designed to protect personal data from damage, loss, alteration, destruction or unauthorised use, access or processing. Data controllers must not adopt security measures that are less robust than those used to manage the organisation’s information. When establishing security measures, the employer should consider the risk involved, the potential consequences for the data subjects, the sensitivity of the data and technological developments.

Must employers involve collective employee representatives?

There is no legal requirement to involve collective employee representatives in internal investigations.

What is best practice when using social media in an investigation?

Before using social media in an investigation, an employer should:

- check its privacy notice provides information to data subjects on the use of social media. Employers may access publicly available social media if they inform the employee of the purpose and use and are specific about the reason for accessing social media.
- consider what the employee has been told about use of social media and what his or her expectations are likely to be.

The employer should ensure that processing is consistent with the legal processing conditions (i.e. including the processing conditions for sensitive data, where relevant).

Employers should establish and maintain a policy on the use of social media as it affects work. Employers should ensure employees know clearly and explicitly the expectations of what kind of behaviour is acceptable. If limited private use of social media is permitted in the workplace, employers should be clear to what extent use is private. The expectation of privacy should be clear.

Must the employer provide the employee with all gathered evidence?

The employer need not and should not provide all gathered evidence to the employee.

Internal investigations may provide defence evidence for the employer in court proceedings. However, from a data privacy standpoint, the data subject has a right to access personal data being processed by a data controller. Therefore, the employer may have to provide any evidence considered to be personal data.

Email

Employers should have a policy on the use of work emails. Employers should ensure that employees know the policy and the expectations of what kind of behaviour is acceptable. As long as the employer has told employees that emails may be accessed and that accessing is necessary for the investigation, reading emails should be permitted.

If limited private use of work email is permitted in the workplace, employers must be clear what the limits are and the extent to which privacy can be expected.

Camera surveillance

Covert filming is particularly intrusive and may not only involve the person under investigation. Therefore, before initiating filming, an employer should consider if there are other means to achieve its purpose in a less intrusive way.

An employer should ensure that any filming is consistent with the data protection principles and that one of the processing conditions is satisfied.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

An employer should check its privacy notice and policies provide information to data subjects on the monitoring of work emails and the possibility of filming when under suspicion.
When is an employer required to conduct an internal investigation?

There is no generally applicable requirement to conduct an internal investigation. There are, however, circumstances in which a failure to investigate might have adverse legal and financial consequences so there is, in effect, an indirect requirement. For example, if an employer suspects an employee of misconduct but dismisses without investigating, it may be liable to pay compensation for unfair dismissal and the employee may be reinstated. Similarly, where a grievance is raised and an employer ought to investigate but unreasonably fails to do so, any award made may be subject to an uplift. Further, the employer’s responsibility for maintaining a satisfactory working environment could result in a duty to conduct an internal investigation, even if no grievance is raised. There are also circumstances in which principles of good governance require an employer to establish the facts.

What are the typical subjects for employment investigations?

Investigations carried out by an employer typically include:

- disciplinary allegations;
- a grievance raised by an employee about treatment by a manager or between two employees;
- allegations of discrimination, for example, sexual harassment or detrimental treatment on the grounds of a protected characteristic (e.g. gender, race, disability, religion or sexuality);
- whistleblowing by an employee regarding, for example, corporate wrongdoing;
- establishment, exercise or defence of a legal claim.

How quickly must the employer conduct an investigation once it is aware of the conduct?

There is no set period of time within which an employer must conduct an investigation but it is expected to act reasonably quickly. How long an investigation takes will depend on matters such as complexity, the nature of the allegations, the number of people to be interviewed and the availability of interviewees.

What data privacy rules must the employer be aware of when conducting an investigation?

An internal investigation will normally involve ‘control measures’. These are the steps the employer takes to ensure compliance with law and contract by its employees. Norwegian employment law applies to all control measures used by the organisation and the measures will only be lawful if they are objectively justified in the circumstances and do not involve undue pressure on employees. The employer must discuss the requirements, design, implementation and any major changes to control measures with employees’ representatives. In the case of an internal investigation, the measures used will depend on its purpose, but could involve, for example, health or drug controls or control over work performed.

Information collected in the course of investigations is likely to include significant personal data. Norwegian data protection law normally applies. Particularly relevant are the duty to process for specified and legitimate purposes and the
obligation to inform the employees during the process.

An employer should:

- check its internal policies (i.e. privacy notice or other policies), provide information to data subjects on control measures, processing and its purposes;
- ensure that both the control measures and processing of personal data are consistent with law, including the processing conditions for sensitive data, where relevant, as this may require a licence from the Norwegian Data Inspectorate.

The employer should ensure that information processed is compatible with the purposes for which it was obtained.

Any information collected should be held securely and accessible only to those who need access.

In most contexts, control measures and the processing of personal data will be necessary to protect the legitimate interests of the employer, for example, where the processing is necessary to enable the employer to fulfill employment obligations or rights or for the establishment, exercise or defence of a legal claim.

Must employers involve collective employee representatives?

The employer must discuss the design, implementation and any major changes to any control measures it wishes to take to ensure employee compliance with the law and the employee’s contract, as soon as possible with the employees’ elected representatives.

However, there is no obligation to involve the representatives each time the same measures are used in the future.

Therefore, the employer should implement any necessary control measures before an investigation occurs. This may include, for example, policies to monitor emails. The employer should document the process and assess the measures.

What is best practice when using social media in an investigation?

It is normally intrusive to access social media used by an employee in a private context and this is usually not justifiable. However, if an employer is investigating the use of social media (e.g. where an employee criticises the organisation or a client) and has created rules about this, it may be easier for the employer to justify.

Before accessing social media, an employer should:

- consider whether such access is in accordance with law;
- be specific about its reason for access;
- consider if it is necessary to do so (i.e. whether there is a proper reason or whether it is simply trawling for information);
- consider what the employee has been told about the use of social media and what his or her expectations are likely to be;
- consider whether there are particular rules on the use of social media.

Employers should put in place policies and endeavour to agree them with staff. Employers should have a policy on the use of social media as it affects work, should ensure employees know the policy and should set out expectations clearly in terms of what behaviour is acceptable.

If limited private use of social media is permitted at work, employers should be clear about the extent to which the use is private.

Bullying colleagues, making detrimental remarks about clients or colleagues or raising work-related grievances publicly would normally be prohibited.

Before introducing a policy it is good practice to consult staff and staff representatives and endeavour to reach an agreement. The employer must to consult employee representatives in relation to any control measures it wishes to introduce.

Social media sites are sometimes used to air complaints because employees find it hard to speak to a manager. Employers should ensure that there is proper dialogue. One approach is to organise one-to-one meetings with managers.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

To read an employee’s emails, an employer must ensure that its actions comply with employment and data protection law. An employer may only explore, open or read email in an employee’s email box:

- where necessary for daily operations or another justified interest of the business;
- for justified suspicions that the employee’s use of email constitutes a serious breach of employment duties or may constitute grounds for termination or dismissal.

The employee must be notified wherever possible and given an opportunity to comment before the employer examines the emails. The employee must, wherever possible, have the opportunity to be present during the examination and has the right to the support of an elected delegate or other representative. If the employer does not give prior warning, the employee must be given subsequent written notification.

Camera surveillance

Covert filming is particularly intrusive and not only in relation to the person under investigation. Case law has held that covert filming will normally be unlawful and will normally be refused as evidence if submitted in court.

Must the employer provide the employee with all gathered evidence?

Generally, the employer must inform employees about all personal data it holds on each individual. However, this obligation is limited to information about the processing of personal data and does not include the right for employees to inspect documents.

There is no general obligation to provide all evidence to the employee. However, the employer must act fairly. It must provide the employee with any information that is relevant to the matter being investigated. Failure to do so could make it more likely that a court would rule in favour of an employee, for example, if a dismissal case is brought to the courts.

Employees sometimes say they will provide evidence, but only if the employer will keep it confidential. In general, employers should not agree to this, as this will not exempt them from having to provide evidence in court, possibly including the information they have agreed is confidential. The information may also need to be provided to the police or other official inspection authorities, depending on the circumstances.
When is an employer required to conduct an internal investigation?

Under Polish law there is no direct requirement to conduct an internal investigation but an obligation may result from internal policy. In some cases, a failure to conduct an internal investigation may have negative consequences for the employer. The employer must prevent workplace bullying or harassment. It is generally accepted that this obligation involves investigating whether the alleged harassment took place. Therefore, employers often adopt internal procedures which set the standards for those investigations.

Polish law permits the employer to terminate employment without notice for fault by the employee in some circumstances. The employer’s decision must be made within one month of the date it became aware of the circumstances that constitute grounds for termination. According to case law, the one month deadline begins to run from the date when the employer was able to determine whether there is merit to the allegations. The employer should conduct an internal investigation to clarify the misconduct and to gather evidence to prove it in court, in case the employee later makes a claim against the employer.

Termination of permanent employment must be justified. When providing justification in the notice, the employer must be specific. Further, if the matter goes to court, the reasons for termination must be evidenced in court by the employer. This means effectively that there is an indirect requirement to conduct an internal investigation in order to collect evidence to support any later claim to the court against the termination.

What are the typical subjects for employment investigations?

Internal investigations are typically conducted in the following situations:

- allegations of workplace harassment or discrimination;
- allegations of theft, fraud or other misconduct;
- to establish reasons to justify notice of termination of permanent employment.

How quickly must the employer conduct an investigation once it is aware of the conduct?

Generally, there is no set period of time within which an employer must conduct an investigation, although there is an exception to this for termination without notice, where a timeframe of one month applies. Generally, an employer is expected to act reasonably quickly. In extreme cases, a lengthy investigation by the employer without a credible reason may be treated as wrongful conduct allowing the employee to terminate employment without notice. Employees may also claim a lengthy internal investigation is evidence of workplace harassment.

What data privacy rules must the employer be aware of when conducting an investigation?

Polish employment law strictly regulates what kind of employee personal data may be collected by the employer. This generally includes the employee’s:

- name and surname;
This means the employer's ability to collect or process personal data in the course of the internal investigation is significantly limited. Employers should not collect sensitive data during investigations. Unlawful collection or processing of personal data may constitute a criminal offence incurring fines, community service or imprisonment.

In practice, it is likely that, during the investigation, the employer may obtain information that includes personal data beyond that permitted by law, including sensitive data. Therefore, the employer should take precautions to mitigate the risk of collecting excessive personal data. Thus, the data should be processed only for the purpose for which they were obtained and the purpose should be proportionate to the nature of information gathered. Personal data of the employee should also only be processed by an authorised person, as processing by an unauthorised person may constitute a criminal offence. Personal data should be also properly secured against unauthorised access.

Must employers involve collective employee representatives?

There is no requirement to involve employee representatives in an investigation unless an obligation exists in internal regulations. If an investigation concerns alleged mobbing, harassment or discrimination, the internal regulations may allow the employee (either the accused employee or the victim) to bring someone along for support and in practice employees do that. Usually, it will be the employee’s lawyer.

What is best practice when using social media in an investigation?

Accessing social media might be considered intrusive and, in many cases also unlawful, as it jeopardises the employee's right to private life. In order to avoid or minimise the risks associated with monitoring social media, clear rules should be set in the internal regulations and/or in the employment agreement.

The employer’s social media policy may limit or prohibit the use of social media during working time and the use of electronic equipment provided by the employer. The employer should inform employees that it may monitor its equipment at any time. The policy should prohibit the making of work-related comments on social media. It should include a general prohibition against bullying colleagues, making damaging remarks about clients or colleagues or raising work-related grievances publicly.

Any use of social media should be properly justified by the employer. This avenue of investigation should be used only if there is a justification. For example, the employer may carry out an investigation only if there is a justified suspicion that the employee has used social media to make derogatory or untrue comments about the employer’s business.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

Work-related emails may be accessed and reviewed. However, the employer should inform employees about any monitoring it may do of these emails, along with the scope and timing of this. However, the employer should always refrain from reading emails that are clearly private.

Camera surveillance

Polish law does not provide clear rules on video surveillance in the workplace. Before commencing video surveillance employers should inform employees that they might be filmed and should introduce clear rules governing the purpose (e.g. the monitoring of performance or the protection of property or trade secrets) and the basic principles of the surveillance. Employers should ensure that employees are aware of the rules by obtaining written confirmation.

The employer may monitor the activities of employees on its premises or the use of transport provided (e.g. company cars, trucks and buses). Video surveillance should, however, be organised in such a way that respects the privacy of the employees. For example, it would be unlawful to install video cameras in toilets. Any information obtained from video surveillance should be collected and processed in accordance with data protection law and used only for the purposes indicated in the internal rules. For example, data should not be used for marketing purposes or publicised in social media. Covert filming of employees in the workplace and filming outside the organisation’s premises during free time is unlawful.

Must the employer provide the employee with all gathered evidence?

There is no general obligation to provide all evidence obtained during an investigation to the employee. The employee is usually only informed of the outcome of the investigation. The employee may receive, for example, a report of the investigation, indicating who the witnesses were, without disclosing the content of the interviews. For investigations related to dismissals, the employee simply receives a notice of termination indicating the reason for the dismissal. The employer is not obliged to provide evidence to the employee to support the reason, but it must be prepared to disclose all available evidence in court.
When is an employer required to conduct an internal investigation?

The employer must conduct investigations into health and safety incidents and industrial diseases in relation to employees and any other individuals engaging in the business of the employer. There are circumstances in which a failure to investigate might have adverse negative consequences so there is, in effect, also an indirect requirement to investigate. For example, if an employer suspects an employee of misconduct but disciplines him or her without investigating, this may be considered by the court or regulatory authority as unfair and unlawful. In this case, the employer will be forced to reverse any disciplinary action (e.g. annul a warning or reinstate an employee).

What are the typical subjects for employment investigations?

Investigations carried out by an employer in Russia typically include:

- health and safety incidents and cases of professional sickness;
- disciplinary procedures for misconduct, for example, disclosure of confidential information or conflicts of interest;
- actions of senior management that adversely affect the organisation and stakeholders;
- establishing an employee’s liability (i.e. where harm is caused to employer by an employee’s actions or inaction).

How quickly must the employer conduct an investigation once it is aware of the conduct?

The standard timeframes for investigation of health and safety incidents and cases of professional sickness are three to 15 days depending on the circumstances. In some cases the investigation may take longer. There are no statutory timeframes for other investigations. However, if an employer intends to use evidence from an investigation to discipline an employee or prove liability, the timeframes for imposing disciplinary sanctions or claiming financial compensation should be taken into account.

Disciplinary action may be imposed on an employee no later than one month after the employer becomes aware of the misconduct, excluding time for any employee illness, annual leave or time required for liaising with trade unions.

Disciplinary action cannot be imposed once six months has passed from the date of the misconduct. For misconduct detected as a result, for example, of a review or audit of the business, disciplinary action cannot be imposed after two years has passed. These timeframes do not include the time required for criminal procedures. Special timeframes exist for claiming financial compensation from employee.

What data privacy rules must the employer be aware of when conducting an investigation?

Information collected in the course of investigations is likely to include significant personal data. The data protection principles apply to this.
Particularly relevant are the duties to process information fairly and for specified purposes. Processing must not be excessive. In summary:

- The employer must obtain appropriate consent to processing (in most cases this is written and must contain certain information, including information about the data subject and controller);
- The rules on cross-border transfers must be observed;
- Relevant agreements with data processors must be concluded;
- Security measures must be taken;
- Processing must be performed in accordance with an internal data processing policy.

Some restrictions must be taken into account:

- The employer must not obtain and process personal data about an employee’s political, religious and other views, private life, membership of public associations or union activity except where required by law.
- The employer must not make a decision affecting an employee based on personal data obtained as a result of automated processing (e.g. by email) without documentary evidence.
- The employer must not use technical means for covert surveillance. Purchasing technical equipment for covert surveillance is prohibited and subject to criminal liability.
- The results of the internal investigation may not be admissible as evidence in the criminal courts unless this is necessary to comply with criminal procedure.
- Evidence obtained in the course of an internal investigation will not be accepted by Russian courts without appropriate validation. The procedure may be divided into stages. First, the employer must issue an internal order on how the internal investigation will be carried out and it must set up an Investigation Committee. Second, the employer should obtain written consent from the employees subject to investigation to collect and process their personal data. Finally, the employer must request explanations from employees in the course of the internal investigation. As a result of the internal investigation the Investigation Committee must issue a written report outlining the main findings of the investigation. Written evidence must be provided in Russian but may be provided both in Russian and another language.

Must employers involve collective employee representatives?

There are certain requirements for the involvement of collective employee representatives for investigations into health and safety incidents and professional sickness (e.g. a representative of a trade union or other employee representation body must be included in an Investigation Committee). Otherwise, there is no requirement to involve collective employee representatives in an investigation. However, involvement may be required if, for example, the employer decides to dismiss an employee as a result of the investigation.

What is best practice when using social media in an investigation?

General principles, rules and restrictions on processing personal data apply to the use of social media. In order to use information obtained from social media as evidence of an employee’s misconduct the employer should obtain the employee’s clear consent for processing the information for investigation or broader purposes. Without this consent the information may only be processed for purposes for which the social media exists (e.g. communication with friends and professional discussions). Processing for other purposes (including for the investigation) may be considered excessive and unlawful.

If an individual does not agree that he or she made a particular statement on social media, this can be very difficult to prove without engaging official investigation authorities. The employer must not take a decision affecting the interests of an employee based on personal data obtained solely as a result of automated processing (e.g. from social media).

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

Employees’ work emails, conversations and information on behaviour obtained in the course of investigation may contain information about an employee’s private life. Third parties who correspond with employees are protected by the Russian Constitution and other laws. Under the Constitution the right to privacy, private correspondence and conversations may be restricted only by a court. Monitoring work emails, conversations and behaviour is possible provided that data protection principles, rules and restrictions are fulfilled and provided that private use of the employer’s resources (e.g. emails, telephones and premises) is prohibited under the employer’s internal policies.

Camera surveillance

Camera surveillance of employees’ activities is generally prohibited by Russian law. In order to implement camera surveillance employees must be informed of the fact that it will be done. The internal rules of the employer must cover how the recording will be conducted and the employer must obtain the employees’ consent to the recording, otherwise this may be in breach of the employees’ constitutional rights.

Must the employer provide the employee with all gathered evidence?

There is no general obligation to provide all evidence gathered during an investigation to the employee. However an employee may receive evidence by requesting the employer provide the employee’s personal data. This is because Russian employment law compels employers to provide employees with copies of any record or document containing personal data of the employee upon request.

Further, the employer must provide, upon request of the employee, copies of any document related to that employee’s work.

If documents contain personal data about another individual, they must be withheld or redacted from the extracts provided to the data subject. Upon official request of a data subject, the data controller (e.g. the employer) must provide the following:

- confirmation of the fact of data processing;
- the legal grounds for data processing;
- the purposes and manner of processing;
name and address of the data controller, all data processors and all those with access to personal data or who may have access under an agreement with the data controller;
categories of processed personal data and the source;
the terms of processing, including retention periods;
the rights of data subjects;
information on cross-border transfers (i.e. including proposed transfers);
other information if provided by law.
When is an employer required to conduct an internal investigation?

Generally, employers are not obliged to conduct internal investigations, unless there are work-related accidents or if an employee has reported bullying by another employee. For reports of bullying, a failure to conduct an investigation may give rise to liability, including criminal sanctions. However, a good governance policy should be implemented for when employees bring formal complaints. A commission should be created to handle this, with participation from the works council.

What are the typical subjects for employment investigations?

The most common cases where an investigation in the workplace may take place are:

- disciplinary allegations;
- a grievance raised by an employee about treatment by a manager or between two employees;
- allegations of discrimination, for example, sexual harassment or unfavourable treatment on the grounds of a protected characteristic (e.g. gender, race disability, religion or sexuality);
- whistleblowing by an employee regarding, for example, corporate wrong-doing.

How quickly must the employer conduct an investigation once it is aware of the conduct?

Investigations should be conducted in a timely manner by the employer. However there is no law that requires it to complete the investigation within a specific period of time. Lack of action, purporting to conduct an investigation when in fact no investigation is taking place, or inaction, may be deemed inappropriate conduct by the employer. These may result in fines ranging from EUR 6,251 to 187,515.

What data privacy rules must the employer be aware of when conducting an investigation?

According to the Spanish Constitutional Court, the employer should consider proportionality, legitimacy, necessity and suitability when conducting an investigation. If the employer abides by these principles correctly, its interest in investigating will not trigger a breach of the employee’s fundamental rights to privacy and secrecy of communications.

When accessing information, the employer should use the least intrusive means. Therefore, the nature of the information being processed and the use of personal data must not be disproportionate to the matter being investigated.

The employer should ensure that information used is compatible with the purposes for which it was obtained and it should not use the information for other purposes.

In obtaining personal data, employees must be expressly informed of
the aim of the collection of that information. Processing will require the unequivocal consent of the person affected.

Must employers involve collective employee representatives?

There is no requirement to involve employee representatives in an investigation. It is, however, good practice to inform or consult with employee representatives when developing policies. Some collective bargaining agreements contain provisions on the involvement of employee representatives and this can mean they are entitled to play an active role in ascertaining the facts and protecting employee privacy. Note that before an employer sets up monitoring systems, such as cameras, employee representatives must be informed and given the opportunity to issue a report.

What is best practice when using social media in an investigation?

There are no specific provisions in Spanish law about how social media may be used in an employment context. In theory, employers may access any publicly available information and process the information, if it is relevant for professional purposes. This could include information about selection, recruitment or disciplinary measures, for example. The courts tend to consider this kind of information public.

However, in the interest of fairness, employers should put in place policies about social media use and endeavour to agree these with employees and employee representatives. Consultation with staff about this should help ensure staff and managers feel protected from online bullying.

If limited private use of social media is permitted at work, employers should be clear about what is meant and to what extent the use is private. Bullying colleagues, making detrimental remarks about clients or colleagues or raising work-related grievances publicly would normally be prohibited. Social media sites are sometimes used to air complaints because employees find it hard to speak to a manager. Employers should ensure that staff have the opportunity to have a proper dialogue. One approach is to organise one-to-one meetings with managers and to appoint a social media controller within the organisation to whom employees may air any grievances.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Transparency is essential when implementing surveillance over employees. Employment contracts may include specific clauses where the employee expressly accepts that the employer may have access to work emails or monitor web pages visited by employees. However, note that this may not be sufficient as the employees’ consent is required when intruding on his or her privacy.

Emails

To read an employee’s emails, an employer must ensure it has the express consent of the employee. Tacit or unspoken consent will be insufficient as the courts apply a narrow interpretation of the meaning of consent. Therefore, organisations usually put in place an email policy informing employees in advance that interception and constant monitoring will take place.

Further an employer should make sure that any accessing of emails complies with the data protection principle of fairness. Generally, if the employer has told employees that emails may be accessed and it is investigating a serious allegation, reading an email should be permitted.

Camera surveillance

Covert filming is particularly intrusive, not only in relation to a person under investigation. Before initiating filming, an employer should consider whether its purpose can be achieved without filming, or without continuous filming.

Further, an employer should ensure that filming is consistent with the data protection principles and that a processing condition is satisfied. The condition for processing will normally be that the covert filming is necessary in the legitimate interests of the employer and that, in the particular case, these interests are not outweighed by the rights of the data subject.

For example, if the filming discloses any aspect of the employee’s private or family life that falls outside the scope of the investigation, his or her privacy rights would be unlawfully breached.

In addition to a legitimate interest, there must be prior communication with the employee and the employee’s representatives that a record sounds or images will be created and that this may be used as evidence for disciplinary purposes.

Must the employer provide the employee with all gathered evidence?

There is no general obligation to provide all evidence gathering as part of an investigation to the employee. The employee will be aware of the information as the works council will have participated in obtaining it and will let the employee know what specific proof has been collected. Note that the employer may withhold evidence obtain as part of a disciplinary investigation against the employee and disclose it later in court proceedings.
When is an employer required to conduct an internal investigation?

There are no mandatory rules about when it is necessary to conduct an internal investigation in Turkey. However, employers are entitled to carry out investigations, under the right to manage employees, in order to find out if there has been a breach of workplace procedures or a disruption of harmony in the workplace. If an employer carries out an investigation it should do so in good faith, in accordance with Turkish employment law.

An employer may wish to investigate matters such as disorder, corruption, theft, mobbing or disharmony amongst employees. Investigations should be conducted confidentially.

What are the typical subjects for employment investigations?

Investigations are usually conducted for reasons such as alleged theft, injury, corruption, disorder or discord amongst employees.

How quickly must the employer conduct an investigation once it is aware of the conduct?

There are no rules regarding the period within which an employer must conduct an investigation in Turkey. However, if the employer finds just cause for termination of the employment contract as a result of an investigation, the employer must terminate the employment contract within six business days. Investigations in situations other than those leading to termination with just cause should be conducted within a reasonable period. The length of the investigation must be sufficient to demonstrate that the employer has carried out the investigation properly.

What data privacy rules must the employer be aware of when conducting an investigation?

There are no provisions about data privacy in Turkish labour law. There is draft law on data protection, but it has not yet been enacted. Therefore, personal data should be handled according to general legal provisions. This means that information contained in the personnel file of the employee must be used lawfully and in good faith by the employer.

The employer must also retain identification information and certain other documents and records about the employee. The employer must use this information lawfully and in good faith and must not disclose the information if the employee has an interest in its non-disclosure.

Must employers involve collective employee representatives?

In Turkey there are no works councils. There is no legal obligation to involve employee representatives in an investigation. If there is a collective agreement, this must be reviewed to determine whether there is a relevant provision.

If there is an investigation about workplace health and safety, employee representatives must be consulted under health and safety law about employees’ occupational health and safety.
What is best practice when using social media in an investigation?

There are no rules regarding the use of social media in investigations in Turkish law. However, there is a draft law on data protection that may alter the position.

In the event of an investigation using social media accounts (e.g. Facebook and Twitter) against the employee, the legal position is unclear. However, in a potential dispute, the investigation will be reviewed to ensure the protection of the personal rights of the employee and avoid violation of the employee's dignity or offensive action against the employee.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

As a rule, the employer must not read employees’ emails on the employer’s devices and servers. However, if it is provided for in the employment agreement or the employer's policies, the employer may look at the employee’s computer or laptop.

Camera surveillance

Generally, employers must not covertly film employees who are under suspicion during an investigation. Nothing related to the employee must be filmed covertly. If the employer wishes to film the employee’s actions, it must display a sign in a visible place and state that there is a camera operating. Otherwise, filming by the employer will constitute a breach of the employee’s right to privacy.

Must the employer provide the employee with all gathered evidence?

There are no rules on whether evidence must be provided to the employee. However certain evidence may need to be shared with the employee to enable the employee to defend himself.
When is an employer required to conduct an internal investigation?

Generally, employers exercise control over employees in respect of performance, diligence and safety. By law, the employer must be involved in accident or medical investigations related to occupational hazards, such as professional illnesses. If there is a suspected breach of duties or rules on safety, the employer may conduct an investigation. In terms of misconduct, there are no statutory rules, but in practice, internal investigations about misconduct will be governed by the employer’s internal policies. Note that during an investigation, the employer will not normally have the option to suspend the employee, unless the employee was intoxicated, refused to be examined by a doctor or refused to be instructed about safety rules.

What are typical subjects for an investigation in your country?

The most common investigations include allegations of theft, poor performance, wrongful conduct and work-safety accidents. Investigations into poor performance are carried out entirely in-house, in contrast to work-safety investigations which require the participation of state authorities. Misconduct investigations are referred to the relevant law enforcement authority, which may be the police, the Public Prosecutor’s Office, the State Emergency Service, other industrial safety bodies, or health institutions.

How much time does the employer have to conduct the investigation once it learns of wrongful conduct?

There are no standard time limits within which an employer must conduct an investigation. For example, an investigation into misconduct would normally take place before the deadline for applying disciplinary sanctions. This deadline is one month from the date when the employer becomes aware of the misconduct, but no later than six months from the day the misconduct occurred. Therefore, a timely investigation allows the employer to take disciplinary action against the employee. A work-safety accident should be investigated within four days by a commission created by the employer. Where a special investigation by state bodies is required, as a general rule, this must be completed within ten days. However, this timeframe may be extended.

What are the data privacy protections that the employer needs to be aware of when conducting an investigation?

Personal data processing should be conducted in accordance with the legal purpose of the processing. Generally, data privacy rules do not prevent the employer from carrying out an investigation, but the rules exist to protect personal data from unlawful use or access by third parties. Specific rules apply to processing sensitive data. Normally, sensitive data may be processed if, for example, this is required to protect legal rights, for performance of the employer’s legal duties or for medical treatment. The timeframe for storing personal data should reflect the purpose of the processing.
Employee tracking devices

Many employers monitor employees through computer networks, computer programs designed to track productivity and other relatively new technological means, such as global positioning systems (‘GPS’) on employer-owned vehicles. Employers contemplating implementing such techniques should consider:

- the impact on employee morale;
- whether the implementation is subject to collective bargaining;
- the purpose of gathering the information;
- how the information will be used;
- how it will be stored;
- what procedures are in place to ensure employee privacy;
- how employees will be notified that they are being monitored; and
- whether employees will be given the opportunity to view or access the data obtained.

Employers should be transparent with employees about the use of such techniques and ensure that employees are aware of procedures in place to protect privacy, such as the ability to disable GPS devices during off-duty hours, or the extent of or circumstances in which tracking may occur outside of working hours. Employers should also implement policies that outline which devices will be equipped with GPS technology, when the employees will be monitored, what information will be collected and how the information will be used.

Must the employer provide the employee with all gathered evidence?

Generally, there is no obligation to provide the evidence to employees. However, some state laws allow employees to request copies of the information contained within personnel files. To the extent that any information gathered during the investigation is contained within the employee’s personnel file, the employer may have to disclose it to the employee.
When is an employer required to conduct an internal investigation?

There is no generally applicable requirement to conduct an internal investigation. There are, however, circumstances in which a failure to investigate might have adverse financial consequences so there is, in effect, an indirect requirement. For example, if an employer suspects an employee of misconduct but dismisses without investigating, it may be liable to pay compensation for unfair dismissal with an uplift of up to 25% for an unreasonable failure to investigate. Similarly where a grievance is raised and an employer ought to investigate but unreasonably fails to do so, any award made may be subject to an uplift. There are also circumstances in which principles of good governance involve an employer in establishing facts.

What are the typical subjects for employment investigations?

Investigations carried out by an employer typically include:

- disciplinary allegations;
- a grievance raised by an employee about treatment by a manager or between two employees;
- allegations of discrimination, for example, sexual harassment or detrimental treatment on the grounds of a protected characteristic (e.g. gender, race, disability, religion or sexuality);
- whistleblowing by an employee regarding, for example, corporate wrong-doing.

How quickly must the employer conduct an investigation once it is aware of the conduct?

There is no set period of time within which an employer must conduct an investigation but it is expected to act reasonably quickly. How long an investigation takes will depend on matters such as complexity, the nature of the allegations, the number of people to be interviewed and the availability of the interviewees.

What data privacy rules must the employer be aware of when conducting an investigation?

Information collected in investigations is likely to include significant personal data. The data protection principles apply. Particularly relevant are the duty to process data fairly and to use the information for specified purposes. An employer should:

- check its privacy notice or other policy provides information to data subjects on processing and its purposes;
- ensure that processing is consistent with the legal processing conditions, including the processing conditions for sensitive data, where relevant.

In most contexts, the relevant condition will be that the processing is necessary for the legitimate interests of the data controller or a third party, except where unwarranted on the basis of prejudice to the legitimate interests of the data subject.
The nature of the information used and use of personal data itself must not be disproportionate to the seriousness of the matter being investigated. The duty to process fairly generally involves listening to what the relevant employee says before making a decision. Any information collected should be held securely and accessible only to those who need access.

Must employers involve collective employee representatives?

There is no requirement to involve collective employee representatives in an investigation. It is, however, good practice to inform or consult representatives in developing policies.

What is best practice when using social media in an investigation?

Deciding whether to access social media in connection with an investigation

Accessing social media used by an employee in a private context is intrusive. Before doing so, an employer should:

- have specific reasons for accessing social media;
- consider if it is necessary to do so (i.e. whether there is a proper reason or whether it is just trawling for information);
- consider what the employee has been told about use of social media and what his or her expectations are likely to be;

If an employee has publicly criticised the organisation on social media, investigating will be easier to justify.

Checking that a processing condition is satisfied

The employer should ensure that processing is consistent with legal processing conditions including the processing conditions for sensitive data where relevant.

In most contexts, the relevant condition will be that the processing is necessary for the legitimate interests of the data controller or a third party. If so, the employer should identify its legitimate interest and consider whether the interest is outweighed by prejudice to the rights of the data subject.

Only in serious cases would it be justified for the employer to view a social media site used for personal purposes. For example, it might be justified if a group of employees use social media to make racist or sexist remarks about colleagues.

Groundwork to enable use of social media

Employers should have a policy on the use of social media as it affects work, should ensure employees know the policy and set out expectations clearly as to what behaviour is acceptable and what is unacceptable. A policy would normally cover behaviour outside work which may have an impact on an employer’s business and should identify the standards expected.

If limited private use of social media is permitted at work, employers should be clear about what is meant and to what extent the use will be treated as private.

Bullying colleagues, making detrimental remarks about customers or colleagues or raising work-related grievances publicly would normally be prohibited.

Before introducing a policy it is good practice to consult employees and employee representatives. Consultation may help achieve ‘buy in’ from staff.

Effective management

Social media sites are sometimes used to air complaints because employees find it hard to speak to a manager. Employers should ensure that there is proper dialogue. One approach is to organise one-to-one meetings with managers.

When investigating, can the employer read employees’ email and covertly film employees under suspicion?

Emails

To read an employee’s emails, an employer must ensure its actions are authorised by regulations on interception of communications and that reading the emails complies with data protection law.

Interception for business purposes will generally be authorised but the employer must have made all reasonable efforts to inform every user of the system (i.e. employees) that interception may take place. Typically, a policy will state that if serious misconduct is suspected, emails may be intercepted.

If interception is authorised, the employer should consider the data protection implications. The employer should ensure that a processing condition is satisfied before deciding to access emails. Further, an employer should ensure that accessing the email complies with the data protection principle relating to fairness.

In general terms, as long as the employer has told employees that emails may be accessed and is investigating in connection with a serious allegation, reading the email should be permitted.

Camera surveillance

Covert filming is particularly intrusive and not only in relation to the person under investigation. Before initiating covert filming, an employer should consider whether its purpose can be achieved without filming, or without continuous filming, and in a less intrusive way.

Further, an employer should ensure that filming is consistent with the data protection principles and that a processing condition is satisfied. The condition for processing will normally be that the covert filming is necessary for the legitimate interests of the employer and that, in the particular case, the interest is not outweighed by prejudice to the rights of the data subject.

Because covert filming is so intrusive, except when investigating particularly serious allegations, the data subject’s rights may well outweigh the employer’s interests in filming.

Must the employer provide the employee with all gathered evidence?

There is no general obligation to provide all evidence gathered to the employee. However, the employer must act fairly. It must provide the employee with any information that is relevant to the matter being investigated. There is no need to provide information collected that is not relevant.

Employees sometimes say they will provide evidence but only if the employer keeps it confidential. In general employers, should not agree to this. If information has been given in confidence it may not be possible to use that information as it would be both unfair to rely on it and unlawful.

If a witness requests confidentiality, an employer should try to agree an approach, for example, by saying it will try to keep it confidential but cannot promise confidentiality or by keeping just the person’s name confidential or redacting information.
When is an employer required to conduct an internal investigation?

When an employer receives a complaint of harassment, discrimination or retaliation, it must take swift action to investigate and, if warranted, rectify the behaviour. Under law, employers have a duty to take all reasonable steps to prevent the unlawful conduct. Employers that fail to conduct an investigation may be subject to further liability for any failure to investigate complaints. A failure to investigate an allegation of unlawful conduct is a separate cause of action against an employer.

Although not mandatory, there are additional circumstances in which an employer may conduct an investigation relating to misconduct (e.g. theft, violence or the use of controlled substances at work).

What are the typical subjects for employment investigations?

Investigations that employers must carry out involve:

- allegations of harassment or discrimination on the grounds of a protected characteristic (e.g. sex, pregnancy, race, color, ancestry, citizenship, religion, national origin, age, marital status, medical status, sexual orientation, disability);
- allegations of sexual harassment by a colleague, manager, vendor or customer;
- allegations of retaliation against an employee for engaging in a protected activity, for example, opposing an unlawful employment practice or requesting reasonable accommodation.

How quickly must the employer conduct an investigation once it is aware of the conduct?

Employers are required to conduct a prompt investigation. Although there is no set period of time, the federal administrative agency, the Equal Employment Opportunity Commission, suggests that an investigation should begin within 48 hours of receiving a complaint.

Under federal law, a proper investigation may provide a complete defence to liability. However, under some state laws, the investigation will only reduce damages. The adequacy of an investigation is an important element for most employment law proceedings where a jury decides whether to assess punitive damages against an organisation and its agents.

Some important characteristics of a fair, impartial, and thorough investigation are the following:

- beginning the investigation promptly;
- having a policy on how investigations will be handled;
- hearing both sides and providing the employee with a reasonable opportunity to present his or her comments;
- providing the alleged wrongdoer with an opportunity to defend the allegations;
- making findings on objective evidence.

What data privacy rules must the employer be aware of when conducting an investigation?
Employers should not unnecessarily intrude into an employee’s privacy when conducting an investigation. There should be a clear audit trail to protect the organisation from a claim of invasion of privacy.

**United States Constitution**

The United States Constitution protects the ‘right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures’. Because the Constitution protects private citizens against governmental intrusions, most searches by private employers do not create federal constitutional concerns. When an employer is acting with the government, however, an unreasonable search may give rise to a claim.

**State constitutions**

Each state has its own constitution that may provide individuals employed by private employers with a right to privacy. Generally, a balancing test is applied to determine whether the invasion of privacy is justified by a competing interest.

**Health information**

Federal law restricts employers from using or disclosing employee protected health information (‘PHI’). To be considered PHI, the information must:

- relate to the physical or mental health of an individual or to the provision of or payment for healthcare; and
- identify or have the potential to identify the individual.

**Criminal background checks**

Several states prohibit employers from requiring applicants and employees to disclose any arrests, detentions, or spent convictions. There are exceptions to this rule for certain industries such as customs, law enforcement, and certain positions in healthcare. It is important for employers to review the applicable state law before making such an inquiry.

- **Must employers involve collective employee representatives?**

If the employees are covered by a collective bargaining agreement, the employees have a right to have a union representative present during an interview with the employer if the employee reasonably believes the interview may result in disciplinary action.

- **What is best practice when using social media in an investigation?**

**Required disclosures**

Employers may access publicly available social media information but are generally prohibited from requiring employees to divulge private information unless directly relevant to the investigation of misconduct or a violation of law. The laws on social media vary from state to state. Employers should have a social media policy that covers employee misuse of the employer’s confidential information, defamation, and harassment of other employees. An employer may discipline an employee for violating its social media policy. However, the employer should take care to ensure that disciplinary action does not violate federal labour law and should take extreme care before taking any disciplinary action in these circumstances.

**Permitted use of social media**

Employers must not discipline employees for voicing opinions concerning the terms and conditions of employment. Federal law generally permits employee communications to the public if the employee:

- indicates the comments are related to an ongoing labour dispute or if the comments involve a controversy concerning the terms and conditions of employment; and
- are not so disloyal, reckless or malicious in nature that they waive legal protection.

- **When investigating, can the employer read employees’ email and covertly film employees under suspicion?**

**Emails**

As long as the employer has a computer or email use policy that advises employees they do not have an expectation of privacy related to the work email server, the employer may review the employee’s work emails. The law on an employee’s personal emails accessed on the employer’s computer system is an unsettled area.

**Camera surveillance**

The laws concerning filming or recording an employee vary from state to state. Generally, employers may film employees in common areas without obtaining consent. However, employers must not make audio or video recordings of an employee in a restroom, locker room, or a room designated for changing clothes.

The following guidelines are relevant to camera surveillance:

- the cameras should be visible;
- employers should give employees written notice of camera surveillance;
- employers should avoid or narrowly restrict the use of cameras in restrooms or other areas that might raise privacy concerns, limit camera angles and control access to recordings;
- if the cameras record voices as well as pictures, the employer must comply with state and federal law applicable to the interception of oral communications.

With respect to off-duty conduct, an employer generally is permitted to covertly observe an employee in a public area to determine whether the employee is honest about employment-related issues (e.g. a leave of absence or workplace injury) as long as the investigator is not unreasonably intrusive.
Employee tracking devices

Many employers monitor employees through computer networks, computer programs designed to track productivity and other relatively new technological means, such as global positioning systems (‘GPS’) on employer-owned vehicles. Employers contemplating implementing such techniques should consider:

- the impact on employee morale;
- whether the implementation is subject to collective bargaining;
- the purpose of gathering the information;
- how the information will be used;
- how it will be stored;
- what procedures are in place to ensure employee privacy;
- how employees will be notified that they are being monitored; and
- whether employees will be given the opportunity to view or access the data obtained.

Employers should be transparent with employees about the use of such techniques and ensure that employees are aware of procedures in place to protect privacy, such as the ability to disable GPS devices during off-duty hours, or the extent or circumstances in which tracking may occur outside of working hours. Employers should also implement policies that outline which devices will be equipped with GPS technology, when the employees will be monitored, what information will be collected and how the information will be used.

Must the employer provide the employee with all gathered evidence?

Generally, there is no obligation to provide the evidence to employees. However, some state laws allow employees to request copies of the information contained within personnel files. To the extent that any information gathered during the investigation is contained within the employee’s personnel file, the employer may have to disclose it to the employee.
AUSTRIA
Kunz Schima Wallentin
Porzellangasse 4
1090 Vienna
Austria
T +43 1 313 74 0
F +43 1 313 74 80
www.ksw.at

BELGIUM
Claeys & Engels
280 Boulevard du Souverain
1160 Brussels
Belgium
T +32 2 761 46 00
F +32 2 761 47 00
www.claeysengels.be

BRAZIL
Veirano Advogados
Av. Presidente Wilson, 231-23rd Floor
Rio de Janeiro 20030-021
Brazil
T +55 21 3824 4747
F +55 21 2262 4147
www.veirano.com.br

DENMARK
Norrbom Vinding
Amerikakaj Dampfaergevej 26
2100 Copenhagen
Denmark
T +45 35 25 39 40
F +45 35 25 39 50
www.norrbomvinding.com

FINLAND
Dittmar & Indrenius
Pohjoisesplanadi 25 A
00100 Helsinki
Finland
T +358 9 681 700
F +358 9 652 406
www.dittmar.fi

FRANCE
Capstan
83 rue La Boétie
75008 Paris
France
T +33 1 44 95 48 00
F +33 1 45 63 99 62
www.capstan.fr

GERMANY
Kliemt & Vollstädt
Speditionstrasse 21
4021 Düsseldorf
Germany
T +49 211 88288 0
F +49 211 88288 200
www.kliemt.de

HUNGARY
CLV Partners
Tartsay Vilmos u. 3.
1126 Budapest
Hungary
T +36 1 488 7008
F +36 1 488 7009
www.clvpartners.com

IRELAND
LK Shields Solicitors
40 Upper Mount Street
Dublin 2
Ireland
T +353 1 661 0866
F +353 1 661 0883
www.lkshields.ie

ITALY
Toffoletto De Luca Tamajo e Soci
Via Rovello, 12
20121 Milan
Italy
T +39 02 721 44 1
F +39 02 721 44 500
www.toffolettodeluca.it

LUXEMBOURG
CASTEGNARO
67 rue Ermesinde
1469 Luxembourg
T +352 26 86 82 1
F +352 26 86 82 82
www.castegnaro.lu

MEXICO
Basham, Ringe y Correa S.C.
Paseo de los Tamarindos No. 400-A, 9th Floor
Bosques de las Lomas
05120 Mexico D.F.
Mexico
T +52 55 5261 0400
F +52 55 5261 0496
www.basham.com.mx

MOROCCO
Aubert & Belkaoui
58 Avenue des Nations
10600 Casablanca
Morocco
T +212 2272 2372
F +212 2272 2377
www.aubertbelkaoui.com

NORWAY
Hjort
Akersgaten 51
P.O. Box 471 Sentrum
0105 Oslo
Norway
T +47 22 47 18 00
F +47 22 47 18 18
www.hjort.no

POLAND
Raczkowski Paruch
ul. Bonifraterska 17
00-203 Warsaw
Poland
T +48 22 380 42 50
F +48 22 380 42 51
www.raczkowski.eu

SPAIN
Sagardoy Abogados
C/Tutor 27
28008 Madrid
Spain
T +34 91 542 90 40
F +34 91 542 26 57
www.sagardoy.com

TURKEY
Bener Law Office
Itri Street, Number:32,
Balmumcu 34349, Istanbul,
Turkey
T +90 212 270 70 50
F +90 212 270 68 65
www.bener.com

UNITED KINGDOM
Lewis Silkin LLP
5 Chancery Lane, Clifford's Inn
London EC4A 1BL
United Kingdom
T +44 20 7074 8000
F +44 20 7864 1200
www.lewissilkin.com

UNITED STATES
FordHarrison
271 17th Street NW, Suite 1900
Atlanta, Georgia 30363
USA
T +1 404 888 3800
F +1 404 888 3863
www.fordharrison.com