Limits on internal investigations

An employee in the sales department of a company that sells its own products reported to a management board member a suspicion that the employee's superior—the head of the sales department—was passing confidential information to a competitor. The employee discovered this when accidentally copied on an email the superior sent to the competitor. The company launched an internal investigation.

Dr Marta Derlacz-Wawrowska

Katarzyna Żukowska

The investigation was conducted to protect the company's information, determine the scale of the damage done, and prevent similar cases from occurring in the future. The employer's aim was to introduce technical and organisational safeguards and to take action against the employee who breached his obligations.

At times an employer may have a legal obligation to launch an inquiry. This is the case for example when occupational health and safety rules are breached or there are reports of bullying or harassment. This is because an employer is required by law to take measures to prevent dangers from arising in the workplace.

Effective, but within the law

When an internal inquiry is required, the employer has to decide what kind of measures should be taken and determine the legal limitations within which it can manoeuvre. The aim is to achieve the objectives of the inquiry effectively, but not risk allegations of violating the law. Any legal violations could render the employer liable, or cause the evidence collected to be contested or inadmissible. Although in the Polish legal system there is no rule that evidence obtained unlawfully is inadmissible in court, use of such evidence can be grounds for third-party claims (brought for example by former employees whose privacy has been infringed). It can also affect how the employer's actions are viewed in terms of the principle of community life, which in turn could lead to an unfavourable ruling in civil cases.

The investigation will certainly proceed more efficiently if the employer already has in place an appropriate policy for internal inquiries into wrongdoing, a privacy policy, and rules properly regulating surveillance issues. Rules also need to be introduced on the employer's disclosure of personal data to other entities, in particular other companies in the group. This is because the law does not provide for specific rules for conducting proceedings of this kind, even when the law requires the employer to launch an inquiry.

Problems may arise, for example, if the employer has not established rules required under the Labour Code on monitoring of work tools issued to employees, such as computers and telephones, and the applications installed on them, such as company email and messaging programmes. An employer is required to define the scope of such monitoring (whether it only collects metadata or accesses the content of messages, and if so in which situations) and inform employees in the appropriate manner. If the employer does not comply with this obligation, then when obtaining information about illicit contact between an employee and the competition, retrieving that data could give rise to a risk not only of breach of the employee's personal interests, in particular privacy, but also an allegation of unlawful processing of personal data. This could lead not only to imposition of an administrative fine under the General Data Protection Regulation, but also criminal liability under the Personal Data Protection Act of 10 May 2018, or possibly, if applicable, failure to comply with the GDPR notification obligation, which can also lead to an administrative penalty. This issue becomes even more complex if the employer also allows private use of work tools and applications. Essentially, introduction of monitoring in any form of employees or civil-law contractors could require a data protection impact assessment to be performed, as stated in Art. 35 GDPR. Failure to conduct a data protection impact assessment could also lead to an administrative penalty. These risks are always assessed case by case, but nevertheless any wrongdoing in these areas could be examined by the Personal Data Protection Office if it learns of it.

Today best practice, soon to become compulsory

Within the next few years, it could become compulsory for employers to implement rules for investigation of reports from employees of wrongdoing in the organisation. In April 2018, a proposal (COM (2018) 218) was published for a Directive on the protection of persons reporting on breaches of Union law. Under the proposal, from mid-2021 onwards, essentially all employers with a headcount of 50 or more would have to introduce procedures for reporting and investigating actions or failures to act that might constitute a breach in certain areas of law, such as public procurement, financial services, safety of products, foodstuffs or transport, environmental protection, protection of consumers, privacy and personal data, and security of networks and IT systems.

Under the proposal, the procedure would have to state the forms in which wrongdoing could be reported, ensuring that the identity of the reporting person is kept secret. It would also have to specify a person or unit to investigate the matter diligently within a reasonable time, as a basic rule not exceeding three months from the time the activity is reported, and inform the reporting person of the results of the action taken. Similar legislative proposals have been put forward in Poland. One of these is a government proposal for an Act on Transparency of Public Life. Work on this bill has practically come to a halt in recent months. Another, concerning entities in the public finance sector, is a citizens' proposal for a bill protecting whistleblowers. This has yet to be submitted to the Sejm.

Protection of the data of a person in breach?

When examining policies for conducting internal investigations, regulations in various areas of law have to be consulted. The issue of protection of the personal interests and personal data of the reporting person and persons subject to the inquiry has to be considered, and, under certain circumstances, criminal law provisions as well.

In terms of the confidentiality of investigations, there is an important notification obligation towards people whose data are processed in connection with the inquiry. This is

a requirement under Art. 13–14 GDPR. This obligation can be fulfilled by notifying the data subject among other things of the identity and contact details of the data controller, the categories of data processed, the source from which they are obtained, the purpose for which they are processed, and who they are disclosed to. Information must also be given about the data subject's rights in the context of the processing of their data. This essentially means that in the case in question, the suspect and the competitor's employee, and thus the competitor as well, had to be notified that the company was conducting an inquiry concerning them and that it might be taking legal action against them, depending on the findings.

Providing this information during the inquiry seems at best ill-advised, but failure on the part of the data controller to observe this notification obligation could lead to liability under the GDPR. Fortunately, in the case in question, the system in place at the company for investigating wrongdoing, based on the Article 29 Working Party guidelines in opinion 1/2006 and the European Data Protection Supervisor guidelines of July 2016 (applicable to EU institutions but not the private sector), not only described in detail the procedure for internal inquiries. It also provided information required under Art. 14 GDPR. Due to these employer rules, notification of the individuals concerned that the inquiry had been launched could be deferred or even omitted.

This raises the question of compliance with the GDPR. As a rule, the notification obligation has to be fulfilled within a reasonable time once the personal data are obtained, within no more than one month. Meanwhile, if personal data are intended to be disclosed to another recipient (for example another company in the group responsible for conducting inquiries within the group), the deadline is the moment the data are disclosed for the first time. However, if providing the information specified in Art. 14(1)–(2) GDPR is likely to prevent or seriously impair achievement of the objectives of the processing, the notification obligation does not apply, provided that the controller takes appropriate measures to protect the data subject's rights and freedoms and legitimate interests. In the case in question, the company decided to apply this exception in relation to the suspect and the competitor's employee.

Third-party participation

If other entities in addition to the employer are involved in the inquiry, for example another company within the group (as in this case) or external entities providing internal investigation and evidence-gathering services, rules have to be established regarding those entities' access to information, including personal data, collected and processed in connection with the assistance they provide to the employer. In the case in question, the company's management board requested the compliance team at the parent company, based in the EU, to conduct the inquiry. The subsidiary and the parent signed an agreement on engagement of another processor as required under Art. 28 GDPR. This is one of the solutions available. As a rule, the solutions chosen should depend on the circumstances and true role of the entities involved in the data processing.

Consequences for the reporting person

When conducting an investigation, the possibility that the allegations of unlawful contact with the competition would prove unfounded had to be considered. In the case in question, the employee had sufficient grounds to reasonably presume that inappropriate contact with the competition had occurred. The form in which the information was reported was also judicious, suggesting that the report was made in good faith and within the law.

Even if further investigation had revealed the allegations to be unfounded, this would not be grounds for the suspect or the employer to impose sanctions on the reporting person. The employer has to make sure that there is no retaliation in the future against the reporting person by the superior whose actions were reported. Although the law does not currently provide special protection for whistleblowers who act in good faith, apart from provisions applicable to certain sectors, this protection follows from labour law, for instance due to the obligation of equal treatment and non-discrimination against employees. This is also an established international standard. At the same time, the need for protection of whistleblowers is acknowledged in the case law (e.g. Supreme Court of Poland judgment of 6 March 2018, Case II PK 75/17).

However, protection is not afforded for reporting in bad faith, for instance when the reporting person is aware that the information provided is factually untrue, or the reporting takes a form that exceeds the limits of acceptable criticism. In such a case, claims can reasonably be brought against the reporting person for breach of the personal interests of the person concerned. The employer also has the option for example of terminating the employment contract of a person who reports misconduct in bad faith.

To summarise, it is worthwhile to introduce in-house procedures for investigation of wrongdoing, while properly observing the limits for investigation procedures specified above all in provisions on protection of personal interests and personal data, even if in general there is no current requirement to adopt such procedures.

Dr Marta Derlacz-Wawrowska, attorney-at-law, Employment practice

Katarzyna Żukowska, adwokat, *Employment practice*