Company property, but maybe private?

Katarzyna Żukowska Agnieszka Lisiecka

While exercising supervision over staff, may an employer access content stored on company computers or smartphones or transmitted using such devices? Or does the employer's accessing such content violate the confidentiality of the employee's correspondence, as well as data protection regulations?

In furtherance of its duty to organise the work of employees, the employer provides employees with working tools. Now, for many employees, basic working tools include computers and other multifunctional devices used for transmitting and storing data, such as smartphones.

In most cases these devices are the property of the employer. The employer entrusts them to its employees as working tools they need to properly perform their official duties pursuant to their employment contract. Some employers also award employees additional employment benefits in the form of permission to use such devices for personal purposes.

When using such devices for business purposes or private purposes, a wide range of content is transmitted via the device, containing for example information covered by the employer's business secrecy, but also personal data of correspondents and personal data concerning other individuals. If the employer permits employees to use such devices for private purposes, the content transmitted via the device or stored in its memory may also contain sensitive data (e.g. concerning the health condition of the employee or family members).

Because content stored in such devices or transmitted via the devices generally contains information concerning the employer's business, including trade secrets, it should be assumed that as a reasonable business entity, the employer will apply all necessary measures to protect its property (including information) against threat, damage or loss. Consequently, such data may be stored in the employer's IT system, including the employer's servers or backup copies. Moreover, in connection with processing of personal data in the employer's IT system, the employer as a data controller has a legal obligation to secure the data by applying technical and organisational measures ensuring protection adequate to the threats and to the categories of protected data. More specifically, the employer must secure the data against access or receipt by unauthorised persons, processing in violation of law, as well as alteration, loss, damage or destruction.

This raises the question whether in exercising supervision over employees, which is one of the fundamental characteristics of an employment relationship, the employer may access content stored or transmitted via devices provided to employees, or monitor the employee's use of such devices; or, conversely, does the employer's viewing of such content violate the privacy of the employee's correspondence or data protection regulations? This is a particularly vital issue as devices provided to employees are essential tools for performance of their work for the employer, and the devices themselves typically belong to the employer. Furthermore the information stored or transmitted via the device relates to the employee's work obligations pursuant to his or her employment by the employer. Thus limiting the employer's right to access such content means restricting the exercise of supervision over the employee's work.

ECtHR on monitoring

The European Court of Human Rights issued a landmark ruling on this issue in *Copland v UK* (judgment of 3 April 2007) concerning monitoring of Lynette Copland's telephone, email and Internet connections at the workplace by her supervisor. The Internet monitoring involved an analysis of the sites she visited, the date, time and duration. The ECtHR found that telephone calls from work, emails and Internet usage are covered by the notions of private life and the confidentiality of correspondence. The court also found that the employee had never been informed that her conversations, emails and Internet usage could be monitored, and thus she had a reasonable expectation of privacy. The court consequently held that there was interference with rights guaranteed by the European Convention on Human Rights and Fundamental Freedoms, including the right to respect for private life and correspondence. The court also pointed out that staff must be aware that their activities could be monitored, and this requires creation of an appropriate procedure and familiarisation with the procedure by staff.

Supreme Administrative Court on monitoring

The essence of the ruling in the *Copland* case also holds under Polish law. In the judgment of 13 February 2014 (Case I OSK 2436/12), the Supreme Administrative Court held that failure to inform an employee of the existence of a functionality of the IT system that gathers information between the intranet at the workplace and the Internet means that the employee is not aware that he or she is subject to monitoring, and thus the monitoring is not transparent and violates the employee's right to privacy. It was irrelevant that the employer did not use this functionality to monitor the correctness of performance of the employee's work duties, but only to secure its own IT system and the data processed in the system. The court cited Art. 23(1)(5) of the Personal Data Protection Act, under which processing of personal data is permissible only if processing is necessary for the legitimate interests pursued by the data controller or the party to whom the data are disclosed, and the processing does not violate rights and freedoms of the data subject.

The Supreme Administrative Court found that installation of this functionality did meet the requirement of a legitimate purpose on the part of the employer (as the data controller), but nonetheless

processing of the employee's data obtained in this manner violated the employee's rights and freedoms. Under the circumstances of the case, the software gathering information about connections between the employer's intranet and the public network also constituted workplace monitoring of the employee, because it enabled the employer to check a list of websites visited, the time of the connections, addresses of websites and files to which the connection was made. Assuming that monitoring of the IT system is necessary to achieve the legitimate purposes of the employer as the data controller, this provision could not be grounds for legal processing of the employee's personal data—the processing violated the employee's right to privacy because the employee was not aware that his computer usage could be monitored. The court stressed that the monitoring must meet the requirements of lawfulness, legitimate purpose, proportionality, transparency, and compliance with data protection regulations. The transparency requirement means that employees must know that they are subject to monitoring and be aware of the rules for how the monitoring will be conducted.

Council of Europe on monitoring

A similar position was presented by the Council of Europe in Recommendation CM/Rec(2015)5 on the processing of personal data in the context of employment, issued on 1 April 2015. The recommendations are not binding, but may be followed as a statement of best practice, particularly as they correspond to rules for processing of personal data under Polish law and are consistent with the rulings of the ECtHR and Poland's Supreme Administrative Court.

The recommendations stress respect for human dignity and privacy. Processing of personal data must comply with principles of lawfulness, legitimate purpose, transparency and proportionality.

The recommendations permit monitoring of employee activity (when the foregoing principles are complied with), but require prior notice to employees concerning the monitoring, including the technologies and IT systems installed for this purpose. Employees should be informed of the categories of personal data processed, the recipients of the data, the right to access the data (including the possibility of correcting or removing the data), and the purpose of the given operation, as well as the period of storage or retention of a backup copy.

The employee's private electronic communications must not be monitored even if conducted at work.

The Council of Europe also recommends introducing procedures for accessing correspondence of an absent employee when there is a professional necessity, in the least intrusive way possible, and only after having informed the employees concerned. And after an employee departs, his or her work email account should be deactivated. If employers need to recover the contents of an employee's email account for the efficient running of the organisation, they should do so before the employee's departure and, when feasible, in his or her presence.

In the event of processing of personal data relating to Internet or intranet pages accessed by the employee, preference should be given to the adoption of preventive measures, so that in the first place less intrusive solutions are applied (e.g. filters preventing particular operations). Any monitoring of personal data should also be done in steps, with preference for non-individual random checks on data that are anonymous or in some way aggregated.

It clearly follows that the employer's right to control devices belonging to the employer but provided to employees as working tools may be significantly restricted in light of the content recorded on the devices—all because of legal protections of the employee's personal rights and personal data.

Katarzyna Żukowska, Employment Law Practice and Personal Data Protection Practice

Agnieszka Lisiecka, adwokat, *partner, head of the Employment Law Practice*