LEGAL BRIEFING – Corporate

by Kostas Fatsis – Partner and

Sofia Feizidou - Associate

The surveillance and recording of employees' data from compliance with data protection laws perspective.

22 May 2023

k.fatsis@aklawfirm.gr

s.feizidou@aklawfirm.gr

In the field of employment relationships, the legal basis for the processing of employees' data is usually the need to perform the contract (Article 6(1)(b) of the GDPR) or the fulfilment of the employer's statutory obligations (e.g., in relation to social security, Article 6(1)(c) of the GDPR). 1(c) GDPR). In addition, in respect of processing that takes place as a consequence of technical and organizational security measures taken by the employer, the latter may be able to rely on Article 1(f) of the GDPR, according to which processing is lawful if it is "*necessary for the purposes of the legitimate interests pursued by the controller or a third party, unless those interests are overridden by the interests or fundamental rights and freedoms of the data subject which require the protection of personal data*".

Such a legitimate interest for the employer may indeed be the optimal organisation of its business, the need to ensure its proper functioning by establishing mechanisms for the control of employees, as well as the need to protect the security of the business assets and networks from material threats, such as the risk of confidential information being disclosed to competitors or of malicious acts by an employee. In this context, it has been held that an employer is entitled to process staff data through the monitoring of their activities at work.

On the other hand, employees have a legitimate expectation of privacy in the workplace, which is not overridden by the fact that they are using the employer's equipment, devices or other business infrastructure. Thus, prior notice to an employee of the prohibition to use of employer-owned computers for non-work-related purposes does not in itself legitimize the processing of his or her personal data through surveillance or monitoring of his or her activity, but rather requires more specific notice. Such requirement is satisfied if the employer brings to the attention of the staff a clear and comprehensible policy on the acceptable use of computers, communications' networks and equipment available to the staff, as well as the policy and procedures for monitoring, accessing and controlling compliance with it. Even in that case, however, prior notification to the employee of the employer's possibility of monitoring his/her communications does not mean that the employee's individual right to privacy is not infringed. In the light of the above, it is necessary in each case to strike a fair balance between the legitimate interests pursued by the employer, on the one hand, and respect for the reasonable and legitimate expectations of employees with regard to the protection of their data in the workplace, on the

other. The legitimate and reasonable expectations of employees in this respect are based on the principles of lawful, fair, transparent and proportionate processing of their data.

For example, in cases of specific and targeted audits, where there are reasonable grounds to suspect that an unlawful act has been committed, it has been held that if the employer's internal policies prohibit the use of electronic means of communication or the corporate network, servers, etc., for private purposes and the employee has been informed both of the relevant prohibition and of the possibility for the employer, in the context of an internal investigation, to gain access to the relevant systems and thus to the personal data held, the employee's expectation of non-interference can be disregarded in accordance with the principle of proportionality. In contrast, systematic monitoring of every electronic activity of employees seems a disproportionate measure and infringes the right to privacy of communications. Instead, the employer should first consider using milder and less intrusive means of protecting the confidentiality of customer data and network security.

In the same spirit, it has been pointed out that, to the extent that monitoring of the employees' internet activity is deemed absolutely necessary, the device should be configured in such a way as to prevent permanent recording, such as by blocking suspicious incoming or outgoing activity and redirecting the user to an online information portal where it can request a review of the automated decision. In some cases, the proportionality requirement implies that no monitoring of any kind can take place. This may be the case where prohibited use of communications services can be prevented by blocking certain websites. If, however, a degree of general monitoring is still considered, to some extent, necessary, the device may also be configured so as not to store log data unless the device generates an incident alert, thus minimizing the information collected. More generally, the rule is that the processing of employees' data to achieve the employer's legitimate interests in the proper organisation and protection of its business must constitute a proportionate response to the risks it faces on a case-by-case basis.

102, Vas. Sofias Avenue
Athens 115 28

+30 210 33 92 600
info@aklawfirm.gr

www.aklawfirm.gr