LEGAL OPINION
REGARDING THE COMPLIANCE OF EMPLOYEE MONITORING ACTIVITIES WITH DATA PROTECTION LAWS

March 9, 2021

This Legal Opinion is prepared by Alcor regarding the compliance of employee monitoring activities via the “Ekran System” software with current Data Protection Laws (particularly, GDPR).

The analysis is carried out with the use of all reasonable skills, professional attitude and attention, based on the best legal practices applied on the market. Our experts have considered only information provided by Ekran System Inc., and did not independently verify it, proceeding from the assumption that such data is true, relevant, complete, and accurate.

This Legal Opinion does not include any express or implied warranties, except that it is prepared on the basis of the principle of "best endeavors", and is provided "as is" in accordance with existing generally accepted practices and standards that are consistent with the level of competence and diligence that are demonstrated by professional consultants who provide the same or similar services.

BACKGROUND

Ekran System Inc. disposes its software product "Ekran System" designed for insider threat management, which can be used for monitoring of the employees' activity on the computers. The aim of such monitoring is control over consumption of working time, handling of inside information, corporate policy compliance and other. Since potential consumers of this product can be employers from European countries, the analysis below explores the legality of the product use for the above purposes.

BASIC STATEMENT

In general, the use of employee monitoring software is not prohibited under current Data Protection Laws. As Data Protection Working Party stated in its Opinion 2/2017 on data processing at work (hereinafter referred to as "WP 249"), "*the use of such technologies can be helpful in detecting or preventing the loss of intellectual and material company property, improving the productivity of employees and protecting the personal data for which the data controller [employer] is responsible*". Therefore, it is not the nature of monitoring programme but its manner of use which is crucial for ensuring compliance with data protection requirements. As outlined in previously mentioned WP 249, monitoring software deployment should strike the balance between the legitimate interest of the employer to protect its business and the reasonable expectation of privacy of its employees.

EU Data Protection Working Party in its several recommendations have provided a set of specific rules, that are based on European Court of Human Rights (hereinafter – "ECHR") practice and which may ensure the compliance with Data Protection Laws while surveilling personnel activity.

1. TRANSPARENCY

Data Protection Working Party in its Working Document on the surveillance of electronic communications in the workplace (hereinafter referred to as "WP 55") stated that *"the provision of proper information by the employer to the worker may reduce the workers legitimate expectation of privacy."* Therefore, employees should be clearly and fully informed of the processing of their personal data, including the existence of any monitoring. This requirement is also reflected in GDPR as principle of transparency (Art. 5.1 (a) of GDPR). At a minimum, employees should be aware about details of monitoring, namely who? what? how? when? for what reasons and purposes? surveilles their activities.

In practice, employers (usually, IT staff) develop policies and rules concerning monitoring, which are clear and readily accessible to employees concerned. In WP 249 it was noted that "*employers must implement and communicate acceptable use policies alongside privacy policies, outlining the permissible use of the organisation's network and equipment, and strictly detailing the processing taking place*". Provided policies may include, among other things, the description of:

- the extent to which communication facilities owned by the company may be used for personal/private communications by the employees (e.g. limitation on time and duration of use) with examples of what constitutes appropriate/inappropriate use of the technology;
- the monitoring systems applied with regard to workers' behavior to prevent and detect misuse of employer's facilities and software or other violations;
- the enforcement procedures outlining how and when workers will be notified of breaches of internal policies and be given the opportunity to respond to any claims against them;
- the possibilities for employees to prevent their data being captured by monitoring technologies (if applicable, like in case with monitoring based on employee's consent, which may be opted out), etc.

Ideally, employees should confirm by signing their awareness and consent with provided policies. Moreover, it is good practice when employers inform and/or consult worker representatives before introducing worker-related policies – in such case such policies will be accorded a higher level of reliability from the standpoint of supervisory authorities. In WP 249 it was also said that as such policies are recommended to be evaluated at least annually.

In its turn, absence of provided policies may have a negative impact. In case of Bărbulescu v. Romania the ECHR came to conclusion that domestic courts failed to determine whether Bărbulescu had received prior notice from his employer of the possibility that his communications on Yahoo Messenger might be monitored (para. 140), although this circumstance had played a crucial role in determining whether rights of employees were violated.

Ekran System software allows not only to inform the employees about the fact that their activities are monitored, but also to obtain their consent and thus make sure that monitoring is in line with the applicable legislation and general corporate policies dealing with internal data processing activities, appropriate use of corporate devices and confidential information, etc.

2. PURPOSE LIMITATION

Under Art. 5.1 (b) of GDPR, processing of personal data should be carried out only for specified, explicit and legitimate purposes and not in a manner that is incompatible with those purposes. Where employer has to monitor employees' activities for valid reasons, it may rely on employer's legitimate interest. Working Party in WP 55 noticed, that "*while workers have a right to a certain degree of privacy in the workplace, this right must be balanced against the right of the employer to control the functioning of his business and defend himself against workers' action likely to harm employers' legitimate interests […] The need of the employer to protect his business from significant threats, such as to prevent transmission of confidential information to a competitor, can be such a legitimate interest.*" In its turn, Working Party in WP 249 stipulated that the employer's necessity to protect the personal data of customers as well as his assets against unauthorized access or data leakage might also be regarded as its legitimate interest.

Another option here is to obtain employees' consent to monitor their activities and process respective data. This justification may be used in situations, when employer wishes to monitor personnel activity for purposes which exceed those lying within employer's "legitimate interest".

If the worker has a genuine free choice and is subsequently able to withdraw the consent without detriment, it is possible to rely on such consent while justifying monitoring of employees. It is worth to notice that consent should be specific and active, thus given by clear affirmative action (usually – "opt in" consent) (Art. 7, Rec. 32 of GDPR).

In this regard, Ekran System product allows to obtain user's "opt in" consent before commencement of monitoring to ensure compliance with applicable laws.

Furthermore, in certain cases employment law may impose legal obligations that necessitate the processing of personal data. In this case employer may explore the possibility of relying on this ground according to Art. 6.1(c) of GDPR.

3. PROPORTIONALITY

Working Party in WP 55 said that "*personal data including those involved in monitoring must be adequate, relevant and not excessive with regard to achieving the purpose specified."* For example, "*the monitoring of e-mails should, if possible, be limited to traffic data on the participants and time of a communication rather than the contents of communications if this would suffice to allay the employers concerns*". However, this principle does not wholly exclude the possibility to monitor content of e-mails (as in previously mentioned example) or of another means of communication. To do so, employer has to justify necessity of provided monitoring activities and demonstrate inability to achieve its legitimate purposes without application of such serious measures. WP 55 contains an example: "*[…] a check on the time spent, or a check on the sites most frequently visited by a department may suffice to reassure an employer that their facilities are not being misused. If these general checks reveal possible misuse of the Internet, then the employer may consider the possibility of additional monitoring of the area at risk.*" Moreover, even video surveillance is not prohibited and may be regarded as fully proportionate to employer's purposes. This is conclusion of the ECHR, reflected in decision in case López Ribalda and Others v. Spain, where the surveillance system installation to monitor workers' behavior was approved.

It is worth noting that mechanism of collective bargaining may be very useful instrument in deciding what actions are proportionate to risks faced by employer – if policies and rules concerning monitoring activities constitute a consensus between the employer and its workers, it is easier to prove that the balance of interests of both sides is struck.

Furthermore, the employer may perform Data Protection Impact Assessment (Art. 35 of GDPR) if processing (taking into account its nature, scope, context and purposes) is likely to result in a high risk to the rights and freedoms of employees (e.g. in situation with automated processing including profiling, as stated in WP 249).

Ekran System product, in its turn, allows customers to configure all the settings depending on how intensive security monitoring should be. Therefore, it may be used in accordance with proportionality requirements described herein.

3. ALERT DETECTION

The Working Party highlighted that "*it is advisable from a practical point of view that the employer immediately informs the worker of any misuse of the electronic communications detected, unless important reasons justify the continuation of the surveillance. […] Prompt information can be easily delivered by software such as warning windows, which pop up and alert the worker that the system has detected an unauthorised use of the network. Quite a lot of misunderstandings can also be solved in this way*" (WP 55). Such option is provided by Ekran System product and may be further customized by employer to achieve full compliance with Data Protection Laws. Alert warnings of various forms may be demonstrated both to security personnel and those employees, whose activity is defined as potentially dangerous.

4. ACCURACY AND STORAGE LIMITATION

Simply put, every personal data collected should be accurate and up-to-date, as well as retained only for as long as necessary to achieve the purposes for which the data was collected. These requirements are reflected in Art. 5.1 (d,e) of GDPR. As Working Party remarked in WP 55, *"any data legitimately stored by an employer (after consideration of all the other principles in this chapter) […] must be accurate and kept up to date and not kept for longer than necessary. Employers should specify a retention period for e-mails in their central servers based on the business needs. It is hard to see that a retention period longer of three months would be normally justified."* In addition, Working Party in WP 249 stated that "*risk comes from the "over-collection" of data in such [monitoring] systems*". Considering that Ekran System Inc. does not store personal data collected by customers during monitoring of its employees, Ekran System products do not violate the abovementioned data protection principles.

5. SECURITY

According to Art. 5.1 (f) of GDPR, personal data should be processed in a manner that ensures its appropriate security, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage. Working Party in WP 55 stipulated that *"this principle obliges the employer to implement appropriate technical and organisational measures to ensure that any personal data held by him is secure and safe from outside intrusion. It also encompasses the right of the employer to protect his system against viruses and may involve the automated scanning of e-mails and network traffic data"*.

Moreover, only limited circle of persons, whose necessity in provided information is clearly and reasonably justified, should have access to information obtained through monitoring. Those staff members should be given appropriate training on data protection and security in order to ensure that they "*are sufficiently aware of data protection obligations*" (WP 249). Working Party in WP 55 also emphasized necessity to ensure that *"the system administrator and anyone else who has access to personal data about workers in the course of monitoring, is placed under a strict duty of professional secrecy with regard to confidential information, to which they have access".* It is worth to mention that none of Ekran System Inc. personnel has access to personal data collected by its

customers using Ekran System product. Therefore, neither Ekran System Inc. nor its employee monitoring software anyhow violates data protection requirements specified herein. Vise versa, Ekran System may be used as an instrument for ensuring compliance with various up-to-date recognized security standards, such as ISO/IEC 27001, NIST 800-53, etc.

6. DATA MINIMIZATION

According to Art. 5.1 (c) of GDPR, personal data collected should be adequate, relevant and limited to the intended purpose only. Therefore, employers are required to justify the amount of data collected. Considering that Ekran System product allows to customize the volume of data collected, customers may choose appropriate settings to collect exclusively those portions of information concerning personnel behavior, which are necessary in every particular case, taking into account customer's own needs and interests.

7. ACCOUNTABILITY

This principle, provided in Art. 5.2 of GDPR, requires organizations to be accountable for the information under their control. This implies that all measures to gather and process the data must be thoroughly documented and comply with the law. Ekran System product, in its turn, allows to record all monitoring activities and provides detailed reports on them, which ensures compliance with current Data Protection Laws.

8. CAUTION TO COMING CONCLUSIONS

It is good practice to give an employee, who is suspected in violation identified by means of monitoring, a possibility to explain its behavior and contest detected breaches. Obviously, the extent of such worker's right depends on the particular circumstances of each separate case. For instance, Working Party in W55 stated that in situation with visiting of dangerous webpages account should be taken to "*the ease with which websites can be visited unwittingly through unintended responses of search engines, unclear hypertext links, misleading banner advertising and miskeying*."

FINAL CONSIDERATIONS

To put it all together, considering the recommendations of European Union Data Protection authorities and practice of the ECHR, Ekran System product itself does not violate the rules regarding protection of personal information. Moreover, it provides various instruments to configure settings of programme so as its performance would correspond needs of its customers and simultaneously comply with current standards of personal data protection. Therefore, the employers should develop their internal policies with a view to the applicable legislation and choose the corresponding set of options provided by Ekran System that are aligned with local rules and their internal policies.