Legal opinion dated August 26, 2015

On legal regulation distinctions of electronic monitoring of the use of corporate computers by the employees in the countries of the Benelux and Europe in general

Initial data.

The client disposes its software product "*Ekran System*", which can be used in particular for monitoring of the employees' activity on the corporate computers. The aim of monitoring - control over consumption of working time, handling of inside information, corporate policy compliance and other.

As potential consumers of this product can be employers from European countries (in particular the Benelux), the Client is interested in legality of the product use for the above purposes.

This legal opinion is prepared exclusively for the Client's consideration (as well as its affiliated persons) and purports to be a confidential result of the intellectual work of *SBT Systems Ukraine*'s specialists (hereinafter - the Expert) within the Expert-Client communications and cannot be used by other companies, except for the Client (unless otherwise is agreed in writing with the Expert).

Legal analysis.

Currently in the EU legislative system, there are no special regulations governing all aspects of the process of electronic monitoring of the usage of corporate computers by employees. In this regard, all the issues related to electronic monitoring and employee privacy are taken to decide based on the provisions of the European Convention on Human Rights, Labor law, EU Data Protection law and in particular Directive 95/46/EC regarding the processing of personal data wholly or partly by automatic means.

Working Party of the European Commission (Article 29 Working Party, hereinafter - Working Party) has developed recommendations to guarantee the respect for human rights while employee monitoring. In general, these recommendations have been duplicated in many ways at the level of EU member states. For example, in Belgium, there was signed the National Collective Agreement number 81 on the protection of employee privacy in relation to the electronic online communications monitoring. In Norway and Luxembourg, the national authorities for the personal data protection proposed similar recommendations.

The recommendations of the Working Party can be summarized to the following:

1. Electronic monitoring should be provided openly and based on a voluntary consent of the employee. The employer must provide the employee with clear and accessible information on the policies regarding the use of corporate computers.

The relevance of this recommendation is confirmed by the decision in the case of *Halford v. United Kingdom*, where it was established that an employee that used a corporate phone for personal reasons, **had a legitimate reason to expect privacy of her calls, as she was not warned** about the possible monitoring of telephone conversations by the employer.

At the same time, the decision in the *Florez* case (Spain) demonstrates that **in certain circumstances covert monitoring can be justified**. In this case the defendant, who eventually won an action, fired its

employee because of systematic visiting the Internet game website during working hours. Catalonian High Court found that monitoring of the employee's corporate PC without his knowledge did not constitute a breach of his right to privacy because of the existence of reasonable grounds to believe that an employee seriously breached his obligations.

2. Continuous automatic monitoring of specific employees (for example, by recording user sessions) **is inadmissible.** In this regard, it is necessary to provide selective monitoring, recording only the **minimum amount of information required** for the employer.

For example, the complete recorded session, during which the employee was communicating with friends in social networks, will be evaluated as an excessive interference into his private life. In turn, records of irrelevant sites visiting with accompanying metadata (like duration) are quite acceptable measures.

3. Employer should respect the right to secrecy of correspondence of employee and his interlocutor, who may be unaware that their dialogue is monitored by third parties.

Based on the above principle, the court in *Onof v. Nikon* case has found that viewing personal employee's e-mail is a violation of human rights, even if employer has directly prohibited using of a corporate computer for private purposes. Thus, monitoring of the correspondence can be justified in a very limited number of cases (if there is a system security threat or the specific employee is involved in the illegal activities affecting the interests of the employer).

4. Information obtained by the employer must be used solely for the corporate security purposes (for which it was collected), as well as carefully protected from unauthorized access. Audit trails should not be stored longer than 3 months.

Summary.

The electronic monitoring of the use of corporate computers by the employees in the European countries (in particular the Benelux) is eligible provided that the companies-employers meet a set of conditions:

- It is a must to approve an internal document with a comprehensive description of the company's policy regarding the use of the corporate computers by the employees, in particular the Internet and e-mail use. The document must contain the answers to the following questions:
  - Can the computers be used for private purposes? If yes, at what time and for how long?
  - What are the reasons and aims of electronic monitoring?
  - Who, how and when will conduct the monitoring?
  - How long will the monitoring data be kept?
  - How the employer can be made aware of the information about himself and lodge a protest against it?
  - How and when will the employees be notified about the policy violations?
  - What are the probable consequences of the policy violations?
- When working on the text of the company's policy it is recommended to discuss its draft with the representatives of the staff as the adoption of such document can materially affect the labor conditions. After approval of the policy it is necessary to bring it to the attention of all employees and obtain their agreement to its application towards them.
- In connection with the prohibition to a permanent automatic monitoring the employers should conduct a comprehensive non-personalized monitoring at the primary phases. Such monitoring must give some insight whether the company's policy is breached without detecting certain breachers. The monitoring of the activity of certain users can be conducted after notice the employees about the detected violations.
- It is worth to notify the employees about the necessity to place personal files and letters in a separate folder or topic with the corresponding name (for example "Private") for the avoidance of receiving the private information by the controlling persons in the course of monitoring.
- The employer must ensure the performance of the requirements of the data protection laws applicable in the corresponding country.

Currently technical features of the software product "*Ekran System*" make it possible for the users to comply with all the requirements mentioned above in order to ensure protection of human rights while conducting the monitoring.

Managing partner  **Dmitry Ovcharenko**

Tel: (044) 383-02-08 | 03040, Kyiv, Ukraine, Vasylkivska str., 14, Business Center «STEND» |
www.sbtsystems.com | Email: info@sbtsystems.com