https://doi.org/10.25143/socr.17.2020.2.011-018

Ensuring Protection of Personal Data in Time of Remote Work during the Covid-19 Pandemic

Mg. iur. ***Agnese Reine***
ORCID: 0000-0002-8222-8281
Rīga Stradiņš University, Faculty of Law, Latvia
agnese.reine@rsu.lv

Abstract

The biggest changes and challenges in the employment relationship in the last six months, especially regarding the provision of personal data processing, are related to the spread of the Covid-19 virus and measures to limit its spread. Globally, the situation developed faster; at the national level, however, starting from the moment when the Cabinet of Ministers Order No 103 of 12 March 2020 On Declaring a State of Emergency was issued in Latvia [1].

At the national level, the necessary restrictive measures to limit the spread of the virus and reduce the risk of disease were analysed. Although the spread of this virus and the legal consequences of the restrictions can be linked to medical issues, the state of emergency also had a major impact on employment relations. When the state of emergency was declared, employers had to evaluate the nature of their business and the possibilities of its realisation when employees perform work remotely. During this assessment, employers were initially divided into two categories – employers whose business specifics do not allow employees to work remotely and those employers who are able to ensure business continuity for employees performing work partially or completely remotely. The purpose of this article is to analyse legality of personal data processing by performing work remotely, respectively studying both employer's responsibilities for processing employees' personal data to ensure control over employee's performance and employees responsibilities for personal data processing.

Keywords: data processing, labor law, work remotley, Covid-19.

Introduction

The Covid-19 virus forced every employer to evaluate the performance of their company, determining whether it was possible to ensure the company's performance by employees working remotely. Companies that made changes to their daily routines and whose employees started working remotely needed to analyse not only the technical aspects, but also the aspects of being able to ensure business continuity while ensuring employee data protection and employee safety. In addition, it is very important for the employer to be able to control the employee's work, which means change in remote working conditions of types of work control and the possiblity to perform supervision using technological solutions. Nevertheless, there was the necessity to balance with the protection of personal data of the employee.

The aim of this article is to analyse the national and international legislation, to evaluate the provision of personal data protection during the spread of Covid-19 by employees performing work remotely, within the framework of which studying both the processing of the employees' personal data and the processing of such data performed by the employee on behalf of the employer.

Methods and Materials

In the article, the author uses methods of interpretation of legal norms – grammatical method, analysing the legal regulation of personal data protection and labor law from a grammatical and linguistic point of view, systemic interpretation method to establish the relationship between employment law and personal data protection legislation, as well as teleological interpretation method to clarify the meaning of legal relations and personal data protection regulatory enactments.

Processing of Personal Data of an Employee as Data Subject

Employers, who were able to reorient their daily work in an emergency situation and enable employees to perform their duties remotely, needed to develop an action plan and address not only technical support for employees, such as access to laptops for all employees and other technological equipment, it was also necessary to carry out an assessment and develop a plan specifically for the performance of work duties. If in the usual situation of an employee coming to work and performing work duties it seems easier for the employer to control the performance of work, then in remote work employers are increasingly trying to take advantage of technology and control the employee's performance, for example, using available data from employee work computer, systems, authorisation data and other available information. Therefore, now that a large part of employees perform their work duties remotely, it is increasingly important to define what

personal data held by the employer they are entitled to use to control the performance of the employee's work, as well as to distinguish the employee's personal data from company-owned information or data that cannot be classified as personal data.

According to Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), hereinafter referred to as the Data Protection Regulation, personal data means any information relating to an identified or identifiable natural person, an identifiable natural person being one who can be identified, directly or indirectly, in particular by reference to an identifier such as the person's name, identification number, location data, online identifier or one or more factors specific to that natural person's physical, physiological, genetic, mental, economic, cultural or social identity [2]. Given the definition in the Data Protection Regulation, it can be concluded that the requirements of the Regulation apply to a very wide range of information that can be classified as personal data, which in turn makes it difficult for employers to analyse which information on employee's work computer is classified as personal data. and how much such data, which the employer obtains from the technologies used by the employee, the employer is entitled to use in making an assessment of the control of the work performed by the employee or capacity measurements.

When providing an employee with technological equipment for the performance of work duties, such as a laptop or telephone, the employer first becomes convinced that any type and content of information or data found in these devices issued by the employer is the property of the employer who handles such data. There are no restrictions for the employer; however, when analysing the processing of such data from a legal point of view, such statements would be considered incorrect. In order to classify the ownership of data and the right to process the data, the Author wants to highlight not only the scope of the legal framework, but also the case law on this issue. Important findings are expressed in the judgment of the European Court of Human Rights in *Libert v. France* [3], where the court assessed the situation when an employer had analysed the contents of an employee's computer hard drive during an involuntary absence and terminated his employment on the basis of personal data. In the judgment, the court states that all data found on the employee's computer (the contents of the hard disk) cannot automatically be considered professional data related only to the performance of the employee's work duties. Irrespective of whether the employee stores or performs any activities with their data using technological means provided (issued) by the employer, primary protection of individual rights must be ensured – the right to privacy, housing and correspondence, which are established by international law and also in Article 96 of the Constitution of the Republic of Latvia [4]. The court states that the employer is not entitled to view / analyse files (data) from the employee's computer (hard drive) without the employee's presence, if the employee has marked such data as private, as well as to read the employee's private correspondence available on the employee's

computer. The employer would be entitled to view and analyse such information only with the employee's permission and in the employee's presence or only in cases where it is legally justified.

The judgment of the European Court of Human Rights in the case of *Barbulescu v. Romania* [5] analysed the situation where an employee used a work computer for personal correspondence, as a result of which the employer had access to the employee's correspondence and their work contract was terminated based on private data. The European Court of Human Rights concluded that the national court had failed to strike a balance between the interests of both parties, the privacy and correspondence of the employee and the employer's right to take the necessary measures to ensure the smooth and uninterrupted operation of the company. The Court also notes that the national court was unable to identify and define the specific reasons justifying this type of supervision of the employee's work, as well as whether the employer was able to control the employee's work but with less interference in the employee's privacy and correspondence. Consequently, the European Court of Human Rights states that the employee's right to privacy and correspondence was not guaranteed. Analysing the two mentioned court judgments, the Author draws attention to the emphasis on proportionality. The employer has the right to carry out supervision in order to ensure the operation of the company and to control the performance of the work, but the means by which such supervision is carried out must be such as to minimise the possibility of violating the employee's right to privacy and correspondence.

When evaluating the possible types of control over the employee's work performance, it is not possible to analyse only, for example, the information available on the work computer and its classification. Nowadays, the employer can use a variety of technological solutions that provide the opportunity to control the employee's performance, such as information recorded on entrance cards, video surveillance systems and others. Often, daily work requires technical means of communication – mobile and landline phones, which can also provide the information needed to monitor work. If landline phones provide a smaller range of functions, and therefore less monitoring capabilities, in the age of modern technological development of mobile phones it can provide a very wide range of information about the phone user's privacy. If the employer has information from the employee's mobile phone and the employer wants to use such data to monitor the employee's performance, it is necessary to analyse a very large amount of data that may be available to the employer, such as location data, information on calls made / received, correspondence contact information and others. If the employer has access to the employee's mobile phone, it is necessary to analyse in detail the data collected from the respective phone as well as assess the necessity of the obtained data and the legality of processing. In this case, as in any data processing, the principle of data minimisation must be observed. The employer may only process data for which there is a legal basis for processing and only to the extent necessary for the purposes of the processing. In order for the employer to be able to legally process, for example, employee location data, such

processing and, consequently, control of the employee must be based on the employer's need to control the day-to-day running of the employee. In addition, the availability of such data on the employee during periods when the employee is not performing his or her duties outside the agreed working hours should be assessed.

From the situations analysed by the Author, as well as case law, it can be concluded that the employer is entitled to control the employee's work performance using information at his disposal, provided that access and analysis of such information is necessary to ensure the legitimate interests of the company and the processing needed. According to the Data Protection Regulation, the data controller must clearly and unambiguously inform the data subject (person) about the manner, amount and purposes for which personal data are processed, as well as indicate other aspects of the Data Protection Regulation concerning erasure, processing location, etc. Analysing the provisions of the Data Protection Regulation in conjunction with the findings of the European Court of Human Rights in the case of *Barbulescu v. Romania* [5], the employer may monitor the employee's performance, but inform the employee or data subject in detail and unambiguously, principle of the protection of the privacy and correspondence of the staff member.

Ensuring Compliance of Data Processing when an Employee Performs Work Duties

Another circumstance, taking into account the state of emergency in the country, is the processing of data by an employee in the performance of his or her duties. Employers whose business specifics allow for such an opportunity provided employees with the opportunity to perform work duties remotely. In order to ensure the fulfillment of such remote work duties, employers had to assess the extent to which employees process personal data on behalf of the company and whether the processing of such personal data by remote work is permissible. The company has an obligation to ensure that the processing of personal data complies with the requirements of the Data Protection Regulation, while remote work increases the risk of possible data processing breaches. Employers needed to carry out a risk assessment, analysing the scope of data processing, data categories and evaluating in connection with the duties to be performed by employees. The degree of risk in relation to the processing of personal data also depends on the specifics of the company's activities and the extent to which personal data are processed in the company's activities. The declaration of a state of emergency created a forced situation for all employers, to ensure, as far as possible, the performance of remote work duties, but minimising all risks as much as possible. Regarding data processing, different types of risks can be distinguished, such as risks caused by technology – when an employee works remotely, risk of data processing violations in terms of technology security and increases of personnel risk, which the Author also aims to study in more depth in this article.

Personnel risks, or potential risks that employees may pose when working remotely, are related not only to employees' responsibility for accessing equipment used to perform their duties, such as a laptop computer, but also to the environment in which the employee performs his or her duties. In order for the employer to ensure the maximum compliance of data processing with the requirements of the legal framework, the employer needs to pay special attention to the instruction and training of employees. Although the emergency did not allow employers to prepare for such remote work, it was necessary to react immediately, but it must not in any way affect the protection of personal data. The employee must be informed about the security requirements to be observed when processing personal data, within the framework of work duties.

Employees may pose a risk of leaving devices used for unattended work in the presence of third parties or in places where third parties may be able to see / obtain personal data, both in person and on video surveillance systems. In this emergency situation, where several family members may be working in the same household, the employee may not be aware of the possible harm, without ensuring the unavailability of data, may lead to a data breach by disclosing information within the household.

The State Data Inspection has also provided its recommendations on how to ensure protection of personal data when employees work remotely, focusing mainly on the need to keep laptops, mobile phones and other devices inaccessible to others, make sure that the computer, laptop or device utilised is used in a safe place, such as a place where the device is always in the employee's field of vision and can minimise the number of people who can view the device screen, especially when working with sensitive personal data, restrict third party access to the device, use an effective access control system (e. g. multifactor authentication and secure passwords), if possible encryption which would also reduce the risk of information leakage if the device is stolen or misplaced, assess the need to send personal data, in particular sensitive data by e-mail, etc. [6]

Nowadays, with the rapid development of technology, not only is it possible to perform employees' work remotely, but it is partly becoming a daily necessity. The employer has an obligation to ensure the protection of personal data, both with regard to employees, ensuring the privacy of employees, and with regard to personal data which are held by the company and which are processed by the company as a data controller.

Conclusions

1. It is more important to define which personal data held by the employer, which they are entitled to use to control the performance of the employee's work, as well as to distinguish the employee's personal data from company-owned information or data, cannot be classified as personal data.
2. All data found on the employee's computer (hard disk contents) cannot be automatically considered as professional data related only to the employee's work duties.

3. The means used by the employer to supervise the work of the employee must be proportionate, so that the control of the performance of work can achieve only the specific goal of the employer – to verify the performance of the work performed by the employee by performing the work remotely.
4. When performing work performance control, inform the employee, or data subject, in detail and unambiguously, about the performance of such processing and observe the principle of data minimisation in order to ensure the inviolability of the employee's privacy and correspondence.
5. When working remotely, the employee must be informed of the security requirements to be met when processing personal data, in the context of the job responsibilities, which means that the employer has the obligation to specify the relevant requirements.

Personas datu aizsardzības nodrošināšana, darbiniekam veicot darbu attālināti Covid-19 vīrusa izplatības laikā

Kopsavilkums

Pēdējā pusgadā lielākās izmaiņas un izaicinājumi darba tiesiskajās attiecībās tieši attiecībā uz personas datu apstrādes nodrošināšanu ir saistīti ar Covid-19 vīrusa izplatību un tā izplatības ierobežošanas pasākumiem. Globāli situācija attīstījās jau agrāk, bet nacionālajā līmenī – sākot ar brīdi, kad Latvijā tika izdots Ministru kabineta 2020. gada 12. marta rīkojums Nr. 103 "Par ārkārtējās situācijas izsludināšanu". Valstiskā līmenī tika analizēti nepieciešamie ierobežojošie pasākumi, lai ierobežotu vīrusa izplatību un samazinātu saslimstības riskus. Lai arī pirmšķietami šī vīrusa izplatība un ierobežojumu tiesiskās sekas ir saistāmas ar medicīniska rakstura jautājumiem, valstī izsludinātā ārkārtējā situācija radīja lielu ietekmi arī uz darba tiesiskajām attiecībām. Līdzko tika izsludināta ārkārtējā situācija, darba devējiem bija jāizvērtē sava biznesa būtība un tā realizēšanas iespējas, ja darbinieki veic darbu attālināti. Veicot šādu izvērtējumu, sākotnēji darba devēji iedalījās divās kategorijās – bija darba devēji, kuru biznesa specifika nesniedz iespēju darbiniekiem veikt darbu attālināti, un darba devēji, kuri spēj nodrošināt biznesa nepārtrauktību, darbiniekiem veicot darbu daļēji vai pilnībā attālināti. Šī raksta mērķis ir analizēt personas datu apstrādes tiesiskuma nodrošināšanu gadījumā, ja darbinieks veic darbu attālināti, attiecīgi analizējot gan darba devēja pienākumus, apstrādājot darbinieku personas datus, lai nodrošinātu darbinieka veiktā darba izpildes kontroli, gan darbinieka pienākumus attiecībā uz darba pienākumu ietvaros veikto personas datu apstrādi.

Atslēgvārdi: datu apstrāde, darba tiesības, attālinātais darbs, Covid-19.

References

1. On Declaring a State of Emergency: Order No 103 of the Cabinet of Ministers of 12 March 2020. Entered into force on 12.03.2020. *Latvijas Vēstnesis*, 51A, 12.03.2020.
2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).
3. Judgment of the European Court of Human Rights of 22 February 2018 in the case "Libert *v.* France", application No 588/13.
4. The Constitution of the Republic of Latvia. 15.02.1922. law. Entered into force on 07.11.1922. *Latvijas Vēstnesis*, 43, 01.07.1993.
5. Judgment of the European Court of Human Rights of 5 September 2017 in the case "Barbulescu *v.* Romania ", application No. 61496/08.
6. Data State Inspectorate. Security measures when working remotely. Available from: https://www.dvi.gov.lv/lv/covid-19/