Marlena Wach
dr, radca prawny
Kancelaria J. Bójko i Wspólnicy („JBW")
m.wach@kancelariajbw.com.pl

DOI: 10.35117/A_ENG_20_11_03

How to protect data in the face of remote operation?

Abstract: The current epidemiological situation has a stigma on entrepreneurs, posing challenges related to maintaining business continuity. In previous articles on the protection of personal data, we focused, among others on the reduction of biological exposure of employees or the protection of personal data as part of the collection of medical data of employees and customers / potential customers of enterprises by entrepreneurs. However, these aspects focus on situations where the presence of employees in workplaces is essential. So what is the data protection situation for entities in which it is possible to transfer all or some part of their activities to remote mode and what rules
should be followed?

Keywords: Remote operation mode; Epidemic; Undertaking

Introduction

A large percentage of enterprises have the capabilities and instruments to adjust the services they provide to the remote mode. However, the remote nature of work entails the need to follow several procedures to ensure the highest possible safety in the performance of employee tasks and smooth business operations by entrepreneurs. In the field of personal data protection during remote work, the Personal Data Protection Office in the communication of March 17, 2020, indicates, inter alia, the following activities to maintain the security of personal data while working outside the office in the field:

Devices:
- Compliance with the safety procedure in the field of work on devices and with the use of the software provided by the employer;
- No additional applications and software installed;
- Providing the necessary updates of operating systems, software, and anti-virus systems;
- Properly stored documentation and preventing access to it by third parties;
- logging out of the official platforms after finishing work;
- Maintaining special security measures, securing the equipment and platforms used with strong passwords;
- Taking special security measures used for remote operation of the device against loss or theft and immediately informing the employer in the event of such an event (including taking steps to remotely wipe the device's memory - if possible).

Electronic mailboxes:
- Compliance with the security procedure for the use of the official e-mail;
- Using primarily business e-mail accounts, if there is a need to use private e-mail, making sure that the content and attachments are properly encrypted;
- Making every effort to ensure that the correspondence always reaches the right addressee;
- Abstain from opening e-mails from unknown recipients, attachments, and links in such messages;
- Sending an encrypted message and decryption password by various methods;

Network and cloud access:
- Use of networks and cloud services only from trusted sources, and follow all organizational policies and procedures for logging in and sharing data;
- Proper archiving and data storage if it is not possible to work in the cloud or if there is no network access.

Remote work regulations
It is worth making an inventory of what can be transferred to remote mode, and what activities must be performed in person in the office or the field, in the plant, and whether the latter do not require reorganization and adaptation to the situation. When moving the office to remote mode, you should also consider whether everything really needs to be moved, what documents the employee must have access to, how to archive them (whether to destroy them and if so, how). This and other information should be included in the Regulations for remote work or another document implementing binding rules for remote work. These regulations may define online meetings with employees at fixed times in the morning and afternoon, and methods for recording working time and showing your activity. Maybe the employer can equip employees with lockable boxes so that they can submit documents to them after the end of work so that they do not accidentally get flooded or damaged in the so-called home office environment. In terms of the protection of personal data, the employer should analyze the data processing, whether, for example, in new circumstances, additional personal data are not processed or otherwise, whether data is made available to third countries. It is also worth training employees in the new regulations or procedures regulating remote work because in the new home office environment it is easy to inadvertently send, for example, confidential information to the wrong recipient, and depending on the content, it may constitute an incident in the field of data security.

The organization of remote work requires its regulation in a policy or regulations
The current situation, when the WHO has declared a pandemic, and the Polish government has introduced a state of epidemic threat and closed Polish borders, undoubtedly affects the organization of work in the enterprise. Citizens were obliged, by legal acts issued by the Government, to stay at home [1]. This forced entrepreneurs to look for remote work solutions to be able to continue their business. Failure to adapt to the current situation may lead to many negative consequences for entrepreneurs.

Preparing an entrepreneur for remote work
It requires an analysis of whether due to the services provided, goods delivered, and the overall scope of the entrepreneur's activity, it is possible to completely transfer work to remote mode, and if not, in what part. What processes and activities can take place remotely and which must still be operated from the office. It is good to make an inventory inside the organization involving people from the IT department, people managing teams, and taking into account the actions that must be taken concerning employees. The above map of processes and activities must be consulted with the Data Protection Officer (DPO) or the person supervising data protection and security issues in the entity. The DPO should be involved in these processes from the very beginning.

Hardware inventory
The department responsible for hardware, devices, tools, which is usually the IT department, should check how much, with what hardware and software it has, whether it should buy new hardware and equip it with the latest software. It requires verification whether there are data monitoring and security tools installed on the devices and whether technical support is

provided. The entrepreneur may consider whether he will allow the employee to use his own private equipment, the so-called Bring Your Own Device (BYOD) [2]. The issued tools should be technically checked. It is also worth checking if we need any tools, e.g. for recording working time and organizing remote work or online meetings, and currently, we do not have these tools. Then you should consider what tools we need and buy them by also installing this software on devices.

Remote work regulations or policy

The entrepreneur should also verify the applicable policies, instructions, regulations and introduce them as a supplement or as a new document, regulations, or remote work policy (or update the existing one). We must obtain certainty and accountability: records of the issued equipment, handover protocols, records of certificates and declarations.

Employee Responsibilities

Such regulations should define the employee's obligations not only in the scope of compliance with the employer's policies, procedures, and instructions, but also to remain at the employer's disposal during fixed working hours and to remain in constant contact with him by means of agreed means of communication.

It is worth agreeing on the method of communication and how the employee's activity will be shown, fixed hours of joint meetings, e.g. 10 am and 3 pm. The employee should be obliged to inform about the results and effects of his work and the proper use of the entrusted company equipment. Also for immediate reporting to the employer of obstacles to work from home, in particular equipment failures. The employer should also have the right to check whether the employee actually performs the work entrusted to him. It is also worth specifying the methods of transmitting and verifying orders, as we show activity that we are available

Technical area

It is good for the employer, after reviewing the tools and software, identifying new tools and solutions that need to be purchased, e.g. for online project management or work time register, also to establish a list of acceptable software and those that cannot be installed because they are not authorized. The regulations should include arrangements for the use of devices, e-mail boxes, networks, and clouds.

a) Devices: used software supplied and recommended by the employer (list of authorized software) and the prohibition of installing unauthorized software, performing necessary updates of operating systems, software, and anti-virus systems. Documentation, whether paper or electronic, should be secured and only authorized persons may have access to it. The employee should log out of the official platforms after finishing work and turn on the screen protection every time he has a break or is not near the computer, strong passwords should also be used, devices should be protected against loss or theft, and the obligation to immediately inform the employer in the event of such an event, including taking steps to remotely wipe the device's memory - if possible. Introducing a ban on sharing business equipment with family members, rules on reporting breakdowns, and the issue of allowing the use of external media.

b) E-mail boxes: using primarily business e-mail accounts, checking the correct recipients, attachments, encrypting the content, attachments, not opening e-mails from unknown recipients, attachments, and links in such messages, sending an encrypted message and decryption password by various methods. Providing training to sensitize employees to various methods of phishing.

c) Access to the network and cloud: use of networks and cloud services from verified sources, compliance with security rules in the field of logging in and sharing data, sharing materials in

the form of screen sharing only to authorized persons. Verifying the method of connecting to the network and choosing a safe connection, using a VPN.

Organizational area, documentation
Analysis of whether all devices and documents are needed to perform remote work, or whether some of them can remain in the office, entering records of the issued documentation. The employer should also regulate how paper documentation is provided to employees (when it cannot be converted into an electronic form), whether it is internal documentation of the company or customer documentation, how it is then archived, and whether it is to be destroyed by the employee or stored and handed over to the office when returning to work or by courier. The employer may equip employees with lockable boxes, containers, folders so that they can put paper documents in them after the end of work so that they will not be flooded or damaged by accident in the so-called home office environment. The use of tools for distribution, settlement of tasks, time and effects of work as well as verification of the work performed.

Permanent office hours
Is it necessary to establish a permanent duty in the office and to appoint an employee who deals with the circulation of paper documents and incident handling? When it is necessary to maintain a stationary office, the work procedures of the support team and on-call duty should be updated. Similarly, how electronic and archived documentation is stored, backup management, and whether and when they will be performed should also be regulated. You should also not forget to secure a stationary office, rooms, equipment, and keys. Staff should receive ready-made instructions, rules on how to secure documentation, workstation, workstation, keys, and access cards.

Permission to use employees private equipment
The employer may also consider allowing the use of employees' private equipment for business purposes (Bring Your Own Device (BYOD), especially in a situation where they do not have an adequate number of portable devices that the employee could use at home. The employer should introduce security software that should be installed. on this private device and introduce authorization, VPN use, passwords, and screen locks as well as similar security mentioned above. In addition, the separation of documents, business and private data, the prohibition of using the company mailbox for private purposes, opening certain applications during use of official tools. Need to install software updates. The employer is obliged to protect confidential information, personal data, and information of third parties, clients, but also to balance this with the protection of privacy and private information of the employee.

Responsibilities of the person responsible for the protection of personal data
The analysis requires whether the new tools or the existing ones, but used differently, do not collect or process additional personal data, e.g. private email or the employee's IP address or the location of the place of residence and whether data is sent outside the European Economic Area. Are there any additional threats or risks for the protection of personal data related to remote work?

In terms of personal data protection, the employer should carry out risk analysis in connection with the organization of remote work and prepare an impact assessment for the protection of personal data.

There is an increased risk of incidents and violations during remote work in the field of, inter alia, errors while sending emails to a large group of recipients (discovered emails); attach an incorrect file to an email; providing a screenshot of the computer screen; no

password for attachments is used; providing personal data in the form of an image of people; becoming a victim of data fraud; infecting the computer with malware; sharing information on social media.

There are also probably new processes that need to be entered into the Register of Processing Activities (RCP). The scope of issued authorizations for data processing and their updating as well as updating the procedure for reporting data security incidents in the event of transferring this process to remote mode requires an analysis. The data controller still has only 72 hours to submit a notification of a personal data breach to the regulatory authority (President of the Personal Data Protection Office).

Online training

Due to a significant change in the method of data processing and tools and the introduction of additional policies regulating remote work and authorized applications, tools, and updating security rules, training should also be conducted, e.g. in the form of e-learning. It is also worth training employees in the new procedure regulating remote work because in the new home office environment it is easy to inadvertently send e.g. confidential information to the wrong recipient and depending on the content, it may constitute a data security incident.

In a situation where, in many cases, remote work has been forced and some people use such solutions for the first time, or some processes have been transferred to a remote mode in which they were not implemented before, it is easy to make mistakes, especially in stressful situations, but there is also an increase in cybersecurity attacks, more frequent phishing attempts and impersonating another person or entity. Therefore, employees should be definitely sensitized to such situations, sharing confidential information during online training or on social media. Awareness of the increasing dangers, especially in times of crisis.

Source materials

[1] On February 28, 2020, the coronavirus infection was covered by the provisions of the Act of December 5, 2008, on preventing and combating infections and infectious diseases in humans. The COVID-19 Act applies from March 8, 2020. From March 14, 2020, until further notice, an epidemic threat was declared throughout the country in connection with coronavirus infections. Regulation of the Minister of Health of March 13, 2020, on the declaration of an epidemic threat in the territory of the Republic of Poland. Regulation of the Minister of Health of 14 March 2020 amending the regulation on the declaration of an epidemic threat in the territory of the Republic of Poland.

[2] Act on mutual obligations of the employer and the employee working on private equipment (teleworker). Regulations for performing work at the employee's place of residence with the use of electronic devices. Safety and health instructions at work performed with the use of electronic devices at the place of residence.