SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2024
ORGANIZATION AND MANAGEMENT SERIES NO. 193

ELEMENTS OF CRISIS MANAGEMENT DURING THE COVID-19 PANDEMIC IN POLAND

Małgorzata MICHALCEWICZ-KANIOWSKA[1], Monika ODLANICKA-POCZOBUTT[2], Aleksandra SZYSZKA-SCHUPPIK[3], Anna KOMARNICKA[4], Anna MURAWSKA[5*]

[1] Bydgoszcz University of Science and Technology, Department of Economics and Marketing, Faculty of Management; malgorzata.michalcewicz-kaniowska@pbs.edu.pl, ORCID: 0000-0003-2154-5838
[2] Silesian University of Technology, Faculty of Organization and Management; monika.odlanicka-poczobutt@polsl.pl, ORCID: 0000-0001-7834-1188
[3] Silesian University of Technology, Faculty of Organization and Management; aleksandra.szyszka-schuppik@polsl.pl, ORCID: 0000-0002-6535-4059
[4] Bydgoszcz University of Science and Technology, Faculty of Management, Department of Innovative Organization Management; anna.komarnicka@pbs.edu.pl, ORCID: 0000-0003-1705-1376
[5] Bydgoszcz University of Science and Technology, Department of Economics and Marketing, Faculty of Management; anna.murawska@pbs.edu.pl, ORCID: 0000-0002-3944-7657
* Correspondence author

Purpose: Contemporary threats are characterized by unpredictability, vehemence and interpermeation, and affect almost all areas of society functioning. The emergence of the Covid-19 pandemic, caused by the SARS-CoV-2a virus, resulted in crisis threats associated with possible loss of life, health or material possessions, destabilization of economic development, or loss of conditions for free existence. The lack of clear guidelines on how to deal with such a situation has revealed the inadequacies of the crisis management systems, which are - by design - aimed at efficient prevention of such situations as well as safety assurance and development of conditions for further advancement, i.e., containment of threat escalation, to the extent possible. The historical review of various events, analysis of the examined organizations' practices as well as overview of the legislation have led the Authors to address the issue of personal data protection throughout the ongoing pandemic. The article is thereby aimed at cataloging the risks and development of guidelines for operation during the COVID-19 pandemic, with respect to personal data protection.
Design/methodology/approach: For the purpose of the article, multiple case studies were conducted in various organizations, where one of the article co-authors acted as a professional Data Protection Officer. The research was carried out in 20 entities of different business profiles.
Findings: The main problems identified involved: body temperature measurement consents, virus test result or immunization data sharing, introduction of COVID-19 questionnaires and visiting regulations, employers' epidemiological proceedings conduct, and remote work models.
Practical implications: The study resulted in the formulation of recommendations, regarding the steps to be taken by organizations in order to establish a catalog of risks via the following: identification of the actual risks, conduction of a risk assessment, development of a catalog of appropriate undertakings and procedures, preparation and maintenance of forces and resources,

as well as definition of the principles for interaction of the actors involved. Further, a recommendation for implementation of a schedule of operation, based on the crisis management guidelines, has been formulated. Consequently, the basis for effective organizational operation involves ongoing verification of the procedures against the Chief Sanitary Inspector's and the Ministry of Health's guidelines, as well as observation and ongoing update of the trends in the crisis management changes.
Originality/value: By identifying a catalogue of risks and formulating guidelines for action during a COVID-19 pandemic in relation to data protection, this article can contribute to the discussion on appropriate practices and strategies in this area. Simultaneously, it provides a valuable perspective on the adaptation of organizations to the dynamic changes in crisis management in the context of the COVID-19 pandemic.
Keywords: personal data protection, crisis management, Data Protection Officer, Covid-19, pandemic.
Category of the paper: Case study.

1. Introduction

The continuous progress in various fields improves the overall living conditions, but it can also result in certain undesirable situations, such as industrial failures, construction disasters, traffic accidents, public order disturbances or even terrorist acts. In addition to natural hazards, such situations can constitute a potential source of crises, which adversely affect the level of personal, property or environmental security, as well as cause significant limitations in the operation of relevant public administration bodies, as a result of inadequate forces and resources (Kancelaria Sejmu, 2007, pp. 1-20). Such effects were also brought about by the Covid-19 pandemic, which emerged unexpectedly in 2020, affecting the entire globe. Infectious disease epidemics continue to plague societies (Baker et al., 2020) and are the leading cause of death worldwide, accounting for from a quarter to a third of all mortality. The numerous outbreaks of infectious diseases in the 21st century, including the Creutzfeldt-Jakob disease, hand-foot-and-mouth disease, severe acute respiratory syndrome (SARS), avian influenza (H5N1), or swine flu (H1N1), inter alia, have become the subject of numerous scientific studies (Keogh-Brown et al., 2010; Keogh-Brown, Smith, 2008) and have, understandably, heightened the fears of a more serious pandemic.

The emergence of the Covid-19 pandemic, caused by the SARS-CoV-2 virus which affected almost every country in the world, transpired as an unexpected crisis. The rapid increase in positive diagnoses, followed by an increase in secondary outbreaks in many countries around the world, led the World Health Organization (WHO) to declare a state of global pandemic on March 11, 2020 (Ferraro et al., 2020; Poláková, Klímová, 2021; Coronavirus disease (COVID-19): Mass gatherings, 2023). The unprecedented global travel bans, as well as implementation of 'stay-at-home' restrictions and assembly bans, affected nearly 90% of the world's population (Czech et al., 2020).

The contemporary threats are characterized by unpredictability, vehemence, multidimensionality, volatility and interpermeation, and affect almost all areas of society functioning. They can, in consequence, result in the loss of life, health or material possessions, destabilization of economic development, or loss of conditions for free existence and development (Falecki, 2016). They can be also difficult to determine in scope, intensity and duration of occurrence, as well as result in unpredictable repercussions. The task of countering these threats and limiting the potential losses requires the use of the interdisciplinary forces and resources possessed by state, which, inter alia, constitutes the reason for the emergence and dynamic development of crisis management.

Many publications have also been devoted to the impact of the coronavirus on human health and psyche or entrepreneurship (Litvinova, 2022), while less attention has been devoted to the inadequacies of administrative operations and the lack of proper crisis management guidelines.

Undoubtedly, the reason for the adverse impact on those affected by the pandemic was the restrictions imposed over subsequent months, including the restrictions on movement, the disruptions to employment, education and health care, as well as the continued isolation and distancing (Oswald et al., 2021).

Studies are now emerging, indicating that the effect of the pandemic may entail exacerbation of post-traumatic stress disorder (PTSD) symptoms, experienced by persons who have not been diagnosed with mental illnesses. The results of these studies, however, are not consistent with the hypothesis that research participants who have been diagnosed with depression are more susceptible to pandemic-related stress (Golińska et al., 2021). The research on the effects of the pandemic will continue to be conducted over the next few years, and perhaps then we will obtain answers to the questions regarding the impact of the pandemic on people.

The magnitude and nature of crises, as well as the number of the actors involved in ensuring the safety of citizens and the functioning of state structures, yields the need to organize, coordinate and cooperate within those structures (Majchrzak, 2018). Crisis management is aimed at preventing such emergency situations and assurance of national security, through pre-planned actions, by creating conditions for further development, i.e., containment of the threat escalation, to the extent possible.

Crisis management in Poland is based on the activities of public administration bodies, consisting in emergency situation prevention, preparation to take control through planned actions, response in the event of crises, and restoration of infrastructure or its original character (Kancelaria Sejmu, 2007, pp. 1-20). Important elements determining effective crisis response include the scale of the crisis and the course of its development as well as its characteristics (Wróblewski, 2007).

The emergence of the Covid-19 pandemic has enabled verification of whether the crisis management system in place is proper. The crisis management in force during the pandemic in virtually all countries around the world, which was based on the introduction of various types

of constraints, from school closures, through office closures, cancellation of sporting and cultural events or restrictions on travel, to the introduction of curfews, has not been backed by the results of ongoing studies (Yanovskiy, Socol, 2022).

The pandemic has shown how important the processing of personal data, or rather, the proper protection of this type of data during a pandemic is. According to the Regulation of the European Parliament and of the Council (EU) 2016/679 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, repealing Directive 95/46/EC (General Data Protection Regulation, hereinafter GDPR), the term 'personal data' refers any information about an identified or identifiable natural person ('data subject'). The same directive defines an identifiable natural person as one who can be identified directly or indirectly, in particular by means of such an identifier as a name, an identification number, location data, an online identifier, or by one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the natural person (Parlament Europejski i Rada Unii Europejskiej, 2016). Such data therefore can be a person's first name, last name, identification number, location data, Internet identifier, as well as National Identification Number or bank account number (Dörre-Kolasa, 2020). This type of data also includes health information, i.e., information on whether a given person is infected with Sars-Cov-2 or has been vaccinated.

The GDPR imposes a number of obligations on Controllers - that is, natural or legal persons, public bodies, individuals or other entities that alone or jointly determine the purposes and means of personal data processing (Parlament Europejski i Rada Unii Europejskiej, 2016) Chapter IV of the GDPR is devoted to data security, i.e., Article 32(1). This chapter imposes an obligation on Controllers to implement technical and organizational measures to ensure an adequate degree of security, in relation to the identified risk of infringement of the rights and freedoms of natural persons (Dziennik urzędowy, 2020, pp. 1-17).

In order to understand the principles of personal data protection, the sources of this data need to be known. This is especially true for those who are required to apply these principles in practice. The times when an individual's privacy was defined and secured by the extra-legal, customary, cultural or religious norms shaping human conduct will not return. The changing environment, shaped by the development of information technology in particular, leads to the fact that the only way to ensure the protection of personal rights is through legal regulation of this area (Kopff, 1972). The issue of information security is not a new topic, nevertheless, attempts to systemically standardize the practices in this domain have only been undertaken since the early 1990s. Comprehensive attentiveness to information security is a new subject in business practice, but the scale and scope of the problems arising from failure to take, inter alia, the risks arising from the loss of information assets into account, cannot go unnoticed by executives (Odlanicka-Poczobutt, Szyszka-Schuppik, 2018).

Due to the existing research gap, the Authors undertook analysis of the issue of information security and, more specifically, the protection of personal data during the Covid-19 pandemic in Poland, by which they also indicated what problems entrepreneurs have faced during the pandemic.

The article thereby has been intended to establish a catalog of risks and develop guidelines, with respect to personal data protection, for operation during the COVID-19 pandemic.

An attempt was also made to develop priority recommendations.

2. Materials and methods

The basis of the research methodology entailed a historical review of various related events, analysis of the practices used, and overview of the legislation in force. The data protection system inadequacies identified during the research and described in this article such as the unclear legal basis for such system operation, the deficiencies in the organization of interaction and coordination of activities, the drawbacks in the adopted procedures and rules of operation, but above all the lack of knowledge on how to proceed and the lack of awareness of the consequences - can inspire improvement of the Data Protection Management System (DPMS), as part of crisis management.

Employers have faced a crisis no one had expected. Practically overnight, some organizations were shut down, while others faced problems of proper protection of their employees against contagion.

Literature studies indicate that a crisis management system should substantially encompass:

- identification of crisis threats, by establishment of a catalog of possible threats, conduction of a risk assessment, determination of the negative consequences for people, property, the environment and critical infrastructure;
- development of a catalog of structural-organizational and functional undertakings aimed at preparing the state and local government administration, including the state resources, for effective response to the resulting threats;
- development of procedures for dealing with the emergent crisis situation;
- preparation and maintenance of resources (forces and means), for use in crisis situations;
- establishment of the principles of interaction for the entities involved in crisis response.

The process of crisis management should involve the following stages (Michałowska, Stankiewicz, Danielak, 2015):

1. Goal formalization - precise definition of the intended objective. During a pandemic, the goal is to ensure the safety of employees and the continuity of company operations.
2. Diagnostic stage - identification of key problems and risks. At the beginning of the pandemic, this mainly pertained to the problems with the supply of personal protective

equipment and disinfectant fluids, as well as the challenges associated with reorganization of work, such as implementation and coordination of remote work, the need to develop new work, cleaning or disinfection schedules.

3. Decision stage - this includes assessment of the alternatives selected and selection of an optimal solution. At this stage in the pandemic, a fair share of employers decided to introduce employee rotation or remote work, faced the need to provide disinfection of premises, and/or reduced working hours so that employees at a given shift did not come into contact with other shifts, making additional changes to increase the workstation spacing.
4. Design stage - in most companies, this stage was limited to mere establishment of a schedule for the upcoming few days. It was not until a few weeks after the introduction of the restrictions that employers began to realize the situation was not temporary and the coronavirus was here to stay for longer.
5. Implementation stage – carried out on an ongoing basis, as new guidelines from the Ministry of Health and the Chief Sanitary Inspector emerge.
6. Control and correction stage - as of today, it is hardly fair to talk about control and conclusion drawing. The scientific knowledge on the coronavirus is still insufficient; the World Health Organization (WHO) has been issuing new guidelines every so often. Inspections by the State Labor Inspectorate are more regular, however, including verification of 'occupational risk assessment' topicality (whether the risk of coronavirus has been taken into account) as well as verification of adherence to the rules of social distancing, mouth covering or disinfectant availability for employees.

Efficient effectiveness of a crisis management system depends on a number of factors, the main ones among which include: appropriate legal regulations, effective structural solutions and organizational linkages, adequate competence powers of key system functionaries, relevant planning that enables development of crisis management plans, taking the forces and means available for use in a crisis situation into account, as well as the procedures for action, the means of resolving hypothetical crisis situations, the rules for activity coordination and cooperation, or proper monitoring, to ensure timely provision of complete and reliable information about threats. Systematical training of the system managers and coordination of the system elements as well as optimal decision making in an accurate and timely manner are important determinants as well. A crisis management system cannot be established once and for all, as it requires systematic improvement, resultant from research and analyses, due to the aforementioned unpredictability and variability of potential threats, the technological development and the changes in legal acts.

Construction of a crisis management system should incorporate phases of prevention, preparation, response and reconstruction, and encompass such problem areas as: the challenges and threats, legal solutions, organizational structures, planning, the decision-making process, organization of interaction, coordination of activities, organization and conduct of training,

acquisition and exchange of experience, the consequences of negligence and omission, people's behavior in crisis situations, possible ways of limiting the effects of crises, or the scope of functionaries' competence and responsibility.

The President of the Data Protection Office (DPO) has announced that the processing of health data, in connection with the measures to prevent the spread of the COVID-19 virus, is regulated by specific legislation, inter alia, by the so-called 'special purpose Act'. The regulations indicated do not conflict with the principles of data processing and do not violate the GDPR. What is more, they correspond with the regulation, which also provides for situations related to the protection of health and prevention of the spread of infectious diseases, i.e., Article 9(2)(d) and Article 6(1)(d). Nevertheless, various situations have been arising in other countries, which result in penalties for violations in this regard. The Danish Data Protection Agency submitted a report to the police regarding the magistrates of Gladsaxe and Hørsholm, following a finding that the magistrates failed to ensure an adequate, in accordance with the GDPR, level of data security. Fines of 100 000 Danish kroner (about 13 380 euros) and 50 000 Danish kroner (about 6700 euros) were proposed to be imposed on the magistrates of Gladsaxe and Hørsholm, respectively (Urząd Ochrony Danych Osobowych, 2020a).

For the purpose of the article, multiple case studies were conducted in various organizations, where one of the co-authors acted as a professional Data Protection Officer. The research involved 20 organizations of different business profiles. The main problems identified entailed body temperature measurement consents, virus test result or immunization data sharing, introduction of COVID-19 questionnaires and visiting regulations, social distancing and remote work.

3. Analysis of the crisis situation in Poland with regard to data protection

3.1. Pandemic crisis in Poland - genesis

The news of a mysterious disease spreading across China emerged in early 2020. The first cases of diagnosed Covid-19, caused by the SARS-CoV-2 virus, emerged in province of Wuhan. Television reports informed about increasing numbers of deaths, the closing down of cities and the introduction of additional protective measures – face masks were ubiquitous, just as the use of the apps monitoring the citizens' movements or their disease symptoms. Some countries attempted short-term forecasting of the COVID-19 pandemic trend (e.g., South Korea) to gain insights on effective response strategies, (Ko, Yoon, 2021) while other attempted effective research on containing the spread of the pandemic (Farhadi, Lahooti, 2021).

In January 2020, the first case of Covid-19 was confirmed in Germany (Majewska, 2020). At the same time in China, the official death toll was already at 106, with 4000 people infected. There were still no confirmed cases of coronavirus in Poland at the time. The Chief Sanitary Inspector Jaroslaw Pinkas continued his assurances that Poland was prepared for the arrival of the virus and there was no reason to panic. New Chief Sanitary Inspectorate recommendations were announced - enhanced hand hygiene, rest, outdoor activity, healthy diet and reduction of stress (Informacyjna Agencja Radiowa, 2020).

As the time passed, new Government announcements emerged regarding, inter alia, restrictions on travel to China, Italy, South Korea and other countries affected by the SARS-CoV-2 outbreak. Poland's borders, however, remained open, and no restrictions were imposed on the movement of citizens. The Chief Sanitary Inspectorate did, however, advise the citizens returning from affected areas to be vigilant about self-observation and frequent hand washing. The Inspectorate published infographics with instructions on proper handwashing procedure (Czub-Kiełczewska, 2020). Poland was slowly preparing for the arrival of the epidemic; e.g., on March 5, an Official Journal of the Minister of Health was published, containing a list of medicinal products, foods for special medical purposes and medical products at risk of unavailability in Poland (Dziennik urzędowy, 2020, pp. 1-17). The list included a number of drugs - painkillers and antipyretics. Despite the Government's appeals - Poles were buying up the medicines in the pharmacies, in fear of limited availability. The panic was also visible in stores - groceries were disappearing from store shelves (rice and pasta were probably the most popular products), as well as canned and tinned goods or toilet paper.

Disturbing news were coming from Italy, which had recorded its first case of SARS-CoV-2 infection on January 31, 2020. On February 24, based on a decision by Prime Minister Giuseppe Conte, a lockdown of 11 municipalities in the Lombardy and Veneto regions was imposed. As of March 8, Italy introduced additional prevention and control regulations, including a ban on mass events and restrictions on the operation of restaurants, fitness clubs and other places where Italians gathered in large crowds, subsequently declaring a nationwide quarantine (Mann, 2020). On the same day, the death toll in Italy stood at 827, while the number of infected people was 12462.

Poland already had certain procedures in place at the time, but only for passengers arriving from the People's Republic of China (e.g., location forms or passenger cards and temperature measurement). The forms the returning citizens were obliged to fill out contained such data as, inter alia, the first name, last name and the National Identification Number. Alas, from the perspective of personal data protection, these forms contained many irregularities. Essentially, it was not clear who was to act as the Controller of the data contained therein, or how long, and for what purpose, was the data going to be processed. The Controller did not fulfil the information obligation resulting from Article 13 of the GDPR.

The first testing for the virus among the Polish population began on January 31, 2020. ‘Patient zero’ was confirmed on March 4, 2020 - the man, who had returned from Westphalia, Germany, (Bucea-Manea-Ţoniş, Andronie, Iatagan, 2018) was admitted into a hospital in Zielona Góra. Along with the first COVID-19 patient, the subject of privacy and personal data processing in light of the GDPR surfaced.

During a broadcasted press conference, the State District Sanitary Inspector released information about ‘patient zero’, which it was not authorized to disclose, based on, inter alia, the patient's family relations (Polska Agencja Prasowa, 2020). The press conference recording initially brought smiles to the faces of the Data Protection Officers, followed by consternation - at a time when all Poles were already familiar with the GDPR regulations, such announcements should not be taking place. The most disappointing aspect of the entire incident, however, entailed the fact that the author of the whole commotion herself was not too aware of the committed disclosure of the patient’s private information which should have never seen the light of day.

Poland, just like other countries around the world, found itself in a crisis, which may have been foreseeable (it was predicted by Bill Gates) (Dziennik Zachodni, 2020), but it was such an absurd vision that no one took it seriously. The situation in which the whole world, including Poland, found itself, resulted in the need for implementation of crisis management during a pandemic.

The beginning of March saw the introduction of further restrictions in Poland. Perhaps the biggest surprise was the pace of the introduction thereof – as early as March 11, the Prime Minister of the Republic of Poland Mateusz Morawiecki announced educational institution closure for a period of two weeks. On March 12 and 13, parents were still able to use the childcare provided by schools, kindergartens and nurseries, but on March 15, complete closure of those institutions until March 25 was announced. Shopping mall closure and border closure were announced as well, followed by closure of hairdressers, massage parlors, beauty salons and other services. The Government introduced senior citizen's hours (between 10:00 a.m. and 12:00 p.m. stores were open for people over 65 only) and restrictions on the number of persons in stores, as well as ordered hand disinfection or use of disposable gloves. These orders, along with the obligation to wear masks introduced on April 16, 2020, remained in force even after some of the restrictions were lifted, as part of the restrictions imposed unfortunately had to be endured by citizens for a few subsequent months.

The subject of the GDPR was put on the back burner for a while. New Covid-19 death statistics in Europe were announced daily, while Poland was preparing for a war with the ‘invisible enemy’. The forces of the Polish state were directed at ensuring adequate amounts of protective equipment for medical personnel and ensuring an adequate number of hospital beds and respirators. Long-forgotten words - quarantine or isolation – reappeared. The number of infected people was rising systematically, and the fatalities count was increasing.

3.2. Absence or inadequacy of official guidelines regarding information on morbidity

In the early days of the pandemic, employers were not able to employ any official guidelines. In the absence of the Government's position on extending the validity of existing medical certificates and the limited operation of Occupational Medicine Clinics which suspended medical examinations for employees, they first needed to face the struggle of dealing with the problems concerning employee medical examination (initial and periodic examinations as well as check-ups). Similar problems employers had to face regarding health and safety training - it was only after a few weeks that the Government changed the law, extending the validity of health and safety examinations and trainings until post pandemic (selected tests and trainings remain valid for a period of 60 days from the date of an official announcement of the end of the epidemic).

Employers were considering introduction of COVID surveys for employees and visitors. In the first days of March 2020, the questionnaires were aimed at obtaining information regarding travel abroad; the Controllers were particularly interested in whether the surveyees' had recently visited China or Italy. Such questionnaires also included questions about the surveyees' health and possible symptoms of infection, i.e., cough, shortness of breath or elevated temperature. All the questionnaire and statement forms included personal data, i.e., in addition to the person's name, the respondents were asked to provide a contact telephone number. The phone number requirement was justified by the potential need to inform a given person of a possible case of a SARS-CoV-2 virus carrier among the Controller's employees, in which case the Sanitary Inspectorate would need to track down the persons who were in contact with the infected employee.

Regrettably, employers did not always consult the content of the questionnaires introduced with Data Protection Officers, who very often only found out about such data processing activity, when they visited the premises of a given organization and were then asked by a security officer to fill out such a questionnaire. The questionnaires did not include the information obligation directly required by Article 13 of the GDPR; the questionnaire retention (storage) period was not specified either - there were no procedures for handling and storing such questionnaires after they had been filled out. Currently, many Controllers are questioning the validity of introducing such questionnaires at all, since, firstly, the pandemic had already been declared and acquisition of information regarding the country of residence is pointless, and secondly, it is unlikely that a person who was actually sick or showed Covid-19 symptoms would provide accurate, complete and true information. Keep in mind, however, that late March and early April 2020 was a period of more questions than answers, when new, terrifying new numbers of virus victims worldwide were announced on the news daily. Under these specific conditions, somewhat in a panic, Controllers were trying to implement solutions which they thought would increase the health security of their employees.

With the emergence of the virus, on the 30th of January 2020, the Chief Sanitary Inspectorate published guidelines for airports, which clearly stated what body temperature (i.e., 38°C) indicates a possible respiratory infection (Grupa Robocza…, 2018). Employers, fearing for the lives and health of their employees, were thus considering introduction of temperature measurements for visitor and/or employees. Visitors were allowed in extremis only – the cult of remote work reigned around, in accordance with the Government's 'stay-at-home' recommendation.

More and more employers introduced temperature measurements. The issue of temperature measurement, however, was just one of the challenges employers had to face in the age of coronavirus. Many introduced temperature measurements without considering its compliance with the GDPR, and without a plan for a situation when an employee/visitor actually had elevated temperature. GDPR experts were deliberating on whether body temperature was personal data. Claims emerged that it could constitute personal health data, within the meaning of Article 4 of the GDPR, i.e., the personal data concerning an individual's physical or mental health, including the provision of healthcare services, which reveals information about the individual's health status (General Data Protection Regulation (GDPR), 2020). In the early days of the outbreak, however, no DPO guidance indicating the solutions to be adopted in order to make the data processing compliant with the GDPR was provided. The laconic information posted on the DPO website did not provide answers to the questions troubling the Controllers and Data Protection Officers (Urząd Ochrony Danych Osobowych, 2020b). According to the law in force, Controllers, who are obliged to comply with the information obligation, must clearly indicate the legal basis for data processing. If a Controller decides to regard information on body temperature as ordinary data, the legal basis should be sought in Article 6(1) of the GDPR. Some Controllers resorted to indicating Article 6(1)(c) of the GDPR in conjunction with Articles 207 §1 and 304 of the Polish Labor Code as the legal basis justifying their right to process temperature measurement data. The first of these Articles specifies that employers are responsible for the health and safety at work establishments and thus are obliged to protect the life and health of their employees, by ensuring safe and hygienic working conditions, in particular through organization of work in a manner ensuring such working conditions and enabling response to occupational safety and health needs (Article 207 §2 of the Polish Labor Code). Article 304, on the other hand, refers to the employer's obligation to contractors and other persons employed under civil law contracts: "The employer is obliged to ensure the conditions of health and safety at work as referred to in Article 207 §2 to individuals performing work on a basis other than an employment relationship in a work establishment or in a place designated by the employer, as well as to anyone conducting business activity on their own account in the work establishment or in a place designated by the employer." The legal basis quoted does not apply to visitors. Here, the legal basis to be used by Controllers is Article 6(1)(f) - i.e., the Controller's legitimate interest, which is to ensure the safety of employees and others on premises. One very important element, which most

Controllers have forgotten about, needs to be addressed in this regard though – each Controller who invokes the provisions of Article 6(1)(f), must conduct the so-called balancing test, prior to the data processing. The test involves an analysis comparing the legitimate interests pursued by the Controller in connection with specific personal data processing activities, with the interests or fundamental rights and freedoms of the person whose data is being processed.

The above-indicated legal basis can be used by Controllers who claim that the data they are processing as not special category data within the meaning of the GDPR. The issue, however, was complicated by an announcement of the President of the DPO, published on the Office website, in which he stated that: "In the case of, for example, a body temperature measurement or collection of data on a person's health, followed by recording, transmission and collection thereof, such activity will be qualified as special category data processing" (Urząd Ochrony Danych Osobowych, 2020a) [translated from the original by MOP]. As the supervisory body recognized this type of information to be special category data, the Controllers had to resort to seeking the legal basis for personal data processing in Article 9 of the GDP in conjunction with Article 6 of the GDPR. First, the Controllers were deliberating on the issue of informed consent. According to Article 4 of the GDPR, such consent must be voluntary, specific, informed and unambiguous. In the case of employee personal data processing by an employer, the voluntariness of such consent is questionable, due to the imbalance of the employment relationship (Chief Sanitary Inspectorate, 2020). Moreover, as per the wording used in Article 221b of the Polish Labor Code, employers may process special category data based on the employee's consent, provided that the processing takes place on the initiative of the employee. The authors of a comprehensive study on enterprise operation in the era of the coronavirus, have indicated that data are processed on the basis of Article 207 of the Polish Labor Code, in accordance with Article 9(2)(b) of the GDPR (Koronawirus a prawo, 2020).

The DPO specified that Controllers may process personal data on the basis of Article 9(2)(i) - that is, special category data may be processed when "processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices" (General Data Protection Regulation (GDPR), 2020), if its provided for by the law. This provision thus corresponds to the national regulations on combating the COVID-19 pandemic, as per Article 17 of the Act of March 2, 2020 on Special Solutions for Preventing, Counteracting and Combating COVID-19, Other Infectious Diseases and Emergencies Caused by Them (Journal of Laws, item 374, as amended) (Urząd Ochrony Danych Osobowych, 2020b).

The announcement published on the DPO website contained a very important statement: "In a situation where, for example a person's body temperature is measured, or data concerning his or her health is collected, and then this information is recorded, transmitted and collected, a special category of personal data will be processed" (Urząd Ochrony Danych Osobowych, 2020a). Analysis of this provision, as well as analysis of the wording in Article 2(1) of the

GDPR: "[t]his Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system" (General Data Protection Regulation (GDPR), 2020), allows a thesis that no personal data processing takes place, as long as the temperature measurement results are not recorded, in which case the GDPR does not apply. This is probably the most common solution, which the Authors of this article consider suitable.

An interpretation that the legal basis for the processing of temperature measurement data lies in Article 9(2)(b) in conjunction with Article 6(1)(b) - i.e., the processing is necessary for the fulfillment of the legal obligation incumbent on the Controllers, which results from the employment contract concluded with the employee, (Rodomaniacy, 2020) is common. Another, much different, interpretation points to the fact that this issue raises very many doubts and Controllers should receive support from the President of the DPO in this regard.

On April 23, 2020, Guidelines for the operation of industrial plants during the COVID-19 epidemic in Poland (Leśniak, 2020) were published on the Chief Sanitary Inspectorate's website, and then on the websites of the Provincial Sanitary and Epidemiological Stations (Chief Sanitary Inspectorate, 2020), which explicitly, under priority recommendations, suggested: "Implementation of non-contact employee/visitor temperature measurement at work establishment entry. Temperature measurement shall be carried out outside the work establishment building, if possible, and the queuing employees must maintain a distance of at least 1.5 meters. If an elevated temperature (above 38 degrees C) or obvious signs of illness, such as persistent coughing, malaise, difficulty breathing, are detected, the person in question must not be allowed to enter the work establishment. In such a case, the Chief Sanitary Inspectorate's recommendations must be followed. In the interim period, before the facility purchases thermometers, it is recommended that employees measure the temperature on their own." [translated from the original by MOP].

An Epidemiological Risk Assessment Questionnaire template - a form used to collect such data as name, information on quarantine or diagnosed Coronavirus infection, including information on detailed symptoms – was made available. Unfortunately, the author of the form failed to reflect on the protection of personal data. The main problem here was not the non-fulfillment of the information obligation itself, which the GDPR indicates explicitly in Article 13, but the fact that the form lacked guidelines ensuring respect for the privacy of those subjected to temperature measurement. This primarily pertained to cases of elevated temperature results. Such information was immediately shared and, sadly, 'took on a life of its own', which in turn could have caused harassment of that particular person. The problem seemed to be noticed only in mid-May 2020. The checklist published by the Central Institute for Labor Protection (CILP), i.e., Occupational Safety and Health during the COVID-19 epidemic, included a point posing an important question: Are there procedures in place to prevent exposure to stigmatization of persons who are/were COVID-19 positive

(Urząd Ochrony Danych Osobowych, 2020; Jaroszewska, Ołdak, 2022). Another problem arose in the context of occupational health and safety, namely the question of securing the people carrying out the temperature measurements, i.e., what personal protective equipment should be arranged for them? What should be the procedure for not allowing a person suspected of being infected to enter the premises? What should follow in terms of dealing with a suspected virus carrier? Should he/she be detained, and the appropriate services notified, or should he/she be sent home? It was not until the aforementioned CILP publication that the need for specific, employer-dedicated solutions was made clear. Employers needed to focus not only on the actual temperature measuring, but, above all, on ensuring the privacy of employees and others, as the phenomenon of social stigma, against not only those infected, but even those in quarantine, emerged (Derda, 2020).

Regrettably, the entry quickly disappeared from the Chief Sanitary Inspectorate's website. The Inspectorate mitigated this fact by pleading that the document published was only a draft version, which had seen the light of day due to human error (Chief Sanitary Inspectorate, 2020). Guidelines providing a basis for development of dedicated solutions for specific employers were still non-existent.

The issue of informing the employees at a particular work establishment that a virus positive person has been identified among the employees posed a very significant problem as well. Controllers were wondering whether they were authorized to inform the other employees that a case of coronavirus had been detected, and whether they could disclose the infected person's name. They split into two groups: those who believed that disclosure of the infected person's name could, first of all, be in conflict with the GDPR and, secondly, it could end up exposing this person to harassment from other employees – risking possible panic among employees, they decided not to disclose the names of infected persons; and those who decided to disclose such data for the sake of the public, based on Article 6(1)(e) of the GDPR - processing is necessary to act in the public interest. The same legal basis, i.e., Article 6(1)(e) of GDPR, was used by employers who decided they had the right to use an employee's private phone number or private email address to provide them with information about an identified case of Covid-19 (Czub-Kiełczewska, 2020). It should be noted, however, that the DPO's position acknowledges the fact that employers have the right to use an employee's private contact information only with his/her consent (Article 6(1)(a) of the GDPR). The DPO also stresses that without an employee's express, preferably written consent, employers cannot use the contact data provided by e.g., a job candidate whom they hired, in which case, the purpose of data processing has changed, and the employee's consent is required for further data processing (Urząd Ochrony Danych Osobowych, 2020c). The guidelines of the European Data Protection Board (EDPB), published on the DPO website, do not explicitly indicate what specific actions Controllers should take. The EDPB merely accentuates the need to respect the dignity of employees. Even a thorough study of the guidelines does not provide any ready-made solutions, as in most part, the document refers the reader to the norms under national law (Urząd Ochrony Danych Osobowych, 2020c).

3.3. Remote work

The Act of March 2, 2020 on Special Solutions for Preventing, Counteracting and Combating COVID-19, Other Infectious Diseases and Emergencies Caused by Them introduced the concept of remote work into the Polish legal system. As employers began to implement remote working solutions, new risks emerged. Firstly, many employers were not prepared for the remote work option - one major problem transpired in the scarcity or lack of computer equipment, in which case, the only option was to bypass the existing ban on the use of private equipment. The Bring Your Own Device principle, consisting in the use of private computers for business purposes, was thus introduced. The main problem the DPO and IT departments had to face entailed proper configuration of hardware, which proved to be quite a challenge when it came to private computers, as appropriate technical measures had to be put in place to prevent outsiders from accessing data - such as Virtual Private Networking (VPN).

These changes also necessitated risk analysis with regard to the processing of personal data in the form of remote work. Such analysis should be carried out by a team of experts who would correctly identify the possible risks, as well as determine what preventive measures should be taken to minimize the risk of violating the rights and freedoms of data subjects. The results of the analysis would need to be documented. Many organizations proceeded to conduct such analyses in accordance with the procedures in force in Companies, while other resorted to implementing ready-made solutions (Ochocki, 2020).

One very good solution, also implemented by the DPO, was to disseminate appropriate guidelines reminding the users of proper personal data processing when working remotely. Such guidelines were developed by the DPO and made available on 17.03.2020 (Urząd Ochrony Danych Osobowych, 2020). The first DPO guidelines in this respect, however, lacked information on the processing of personal data in paper form; such guidelines were only published on 04.05.2020. Those guidelines emphasized the importance of, inter alia, proper transfer, storage and destruction of documents. Employers, however, needed to normalize their remote work conduct policies in more detail – the internal regulations defining the principles of remote work needed to include not only the rules for personal data processing, but also the rules for work attendance verification, the rules for accounting treatment of overtime, the employee and employer rights and obligations, as well as the health and safety aspects covering, inter alia, the rules for post-accident proceeding in a remote work system.

The subsequent months of the fight against the pandemic only added to the chaos. The autumn of 2020 brought further disturbing news - almost every day, more countries, including Poland, hit record morbidity and, sadly, reported record death tolls. Virtually no week went by without new solutions, recommendations, definitions and ultimately restrictions being introduced. On the day we finished writing this article, Poland was on the eve of another ‘Lockdown’, i.e., a ‘national quarantine’ along the lines of what had happened at the beginning of the year. Other European countries had already either introduced such ‘mini-Lockdowns’ or

were planning to do so in the near future. Each country determined its own strategy, however - unlike at the beginning of the pandemic. Everyone was wondering whether such a lockdown would be effective and whether the scale of the pandemic could be slowed down by even a bit. Certainly, introduction of further restrictions was much more difficult, as coronasceptics and people who claimed outright they would not go into a lockdown a second time were growing in numbers. It was the people's attitude, their self-discipline, the specter of penalties for not complying with the recommendations, as well as the general fear, which could have played a key role in combating the threat.

4. Discussion and recommendations

The advent of Sars-Cov-2 vaccines had significant impact on the curbing of the pandemic. The subsequent months brought waves that impacted the affected countries with greater or lesser force. Governments were imposing restrictions that were no longer as restrictive. Gradually, the coronavirus began to be treated as a seasonal disease, such as influenza.

Work is currently underway to permanently introduce provisions on remote work into the Polish Labor Code, which will in turn eliminate telework from the Code, as the concept of remote work is a much broader term (Pokutycka, 2023). Despite the passage of months, employers still have not been provided with clear guidelines indicating whether the actions undertaken are accurate or not. Even the social distancing guidelines are not the same – recommended distance ranges from 1.5 to 2 meters. The steps for organizations to follow when developing a threat catalog should entail the following:

- identification of actual crisis risks;
- performance of risk assessment (identification of negative effects on people, property, the environment and critical infrastructure);
- establishment of a catalog of pragmatic actions for effective response to the resulting threats;
- establishment of procedures for dealing with each crisis situation;
- making provisions for and maintenance of the forces and resources to be used in crisis situations;
- development of principles of interaction for the entities involved during a crisis response and establishment of the responsibilities thereof;

The action plan should include the following scheme:

1. Precise definition of the intended goal – assurance of employee safety and company operation continuity;
2. Identification of key problems and threats;

3. Assessment of selected alternatives and selection of an optimal solution (e.g., decision on employee rotation, introduction of remote work, disinfection of premises, reduction of working hours, spacing between workstations, etc.);
4. Development of day-by-day, week-by-week, month-by-month schedules;
5. Implementation of recommendations and guidelines on an ongoing basis - as new guidelines from the Ministry of Health and the Chief Sanitary Inspector emerge;
6. Control and correction - including verification of occupational risk assessment topicality, and verification of adherence to the rules, with regard to the optimal solution alternatives used (e.g., social distancing, mouth covering, disinfectant availability, remote work).

The only thing left for employers is to keep their procedures up to date and under review with the Chief Sanitary Inspectorate and the Ministry of Health guidelines. The catalog of possible treats is not a closed catalog and must be updated on an ongoing basis. The Authors' experience shows that a pervasive chaos still reigns, and only establishment of a catalog of risks, followed by development of guidelines for operation during the COVID-19 outbreak, with regard to personal data protection, can support the activities of organizations wishing to comply with the rules and regulations imposed.

It seems that crisis management should be viewed as management under pressure, resolving various types of emergencies and restoring stability to the functioning of a community, organization, state or group of states. It should be oriented at averting the emergence of a crisis situation through preventive and preparatory crisis management, and, in the event of crisis emergence - at responding effectively, in order to minimize its negative impact on the subject of the security measures undertaken.

The need to reduce the risks associated with emergence of possible threats and a crisis situation, as well as to establish efficient mechanisms for controlling those threats through reasonably planned actions, and thus ensure security, calls for employers to create such catalogs of threats and develop guidelines for operation during the COVID-19 epidemic, with particular regard for personal data protection

Employers should, therefore, first determine what solutions they wish to put in place to ensure employee safety and business continuity. They can choose between organizational and technical measures. The organizational measures include introduction of mandatory temperature measurements for employees and work establishment visitors. The measurement procedures should be communicated beforehand. Employers should deliberate on and decide whether the measurement results are to be recorded or not. From the perspective of the GDPR, it is better not to record the measurement results - no processing of personal data takes place in such case. Very often employers forget about the privacy of the people subjected to temperature measurement. In fact, the problem only arises when the measurement shows a result above the standard set by the employer. In practice, temperature measurements are made by security workers, and as employees are subjected to the measurement, there is no way to keep the

information about possible elevated temperature case a secret - all other employees will, sooner or later, find out about the person in question. The person's privacy will be severely violated, plus the person may become a target of harassment and heckling. There are no DPO guidelines for employers on how to protect the privacy of such a person.

Employers should also ponder on introduction of Covid surveys. Introduction of such a questionnaire is very controversial from the perspective of the GDPR, which the Authors of the article have already indicated. In the Author's opinion, introduction of visiting regulations, which would precisely define the rules of entering company premises during a pandemic, would be a better solution. The content of such regulations should include, inter alia, provisions requiring the persons showing symptoms of coronavirus infection, as well as those who have had contact with an infected person, to cancel any meetings planned. This would help avoid problems with the legality of data processing under GDPR.

Internal regulation of remote work constitutes an important element of management during a pandemic. Employers should therefore introduce regulations that complexly regulate the principles of such a work system. Such regulations should first and foremost set out the rules for secure processing of data - many employers have so far allowed employees to work on a 'home office' basis, but for other this work arrangement has proved to be quite a novelty. Many employers had to modify their security regulations, by allowing employees to use private equipment, which, in turn, involved the need to configure the equipment accordingly. Specification of the rules for handling printed documents is another important element such regulations should include - employers should specify the rules for securing and destroying paper documents. As already mentioned, such regulations need to be comprehensive, i.e., they should define the organization of remote work, including the rules for work attendance verification and work accountability. Another important element to be included entails regulation of such health and safety issues as possible site visiting if an employee suffers an accident.

Employers should additionally deliberate on the rules for returning to offices after remote work. They should take the current guidelines for maintaining person-to-person spacing or the rules for equipping employees with face and nose shields into account. Non-standard measures should be introduced in certain situations. Additional shifts, breaks or employee rotation, remote work or hybrid work (remote work alternating with regular work) can be taken into consideration as well.

5. Conclusion

The article was aimed at establishing a catalog of risks and development of guidelines for operation during the COVID-19 outbreak, with regard to personal data protection. An attempt was also made to develop priority recommendations. The Authors have indicated what problems entrepreneurs have faced during the pandemic. Despite the fact that the pandemic has lasted for more than two years - specific guidelines for employers, which would clearly indicate what is allowed and what would contradict the current regulations, have still not been developed. Currently, the Poland is at the stage of 'loosening the restrictions', with the only the order to cover the mouth and nose in health facilities and pharmacies in place. We do not know, however, whether the situation is just temporary and whether restrictions, of one kind or another, will be re-announced.

The Authors, driven by their interest in the subject, declare to continue to follow the legislative changes and seek optimal solutions for organizations. As of the date of writing this article, we are still awaiting the anticipated update of the Polish Labor Code provisions, which, after the two years of the pandemic, is expected to finally regulate remote work.

References

1. Baker, S.R. et al. (2020). *Covid-induced economic uncertainty*. National Bureau of Economic Research. Retrieved from: https://www.nber.org/papers/w26983, 20 November 2023.
2. Bucea-Manea-Ţoniş, R., Andronie, M., Iatagan, M. (2018). *e-Learning in the Era of Virtual Reality*. The International Scientific Conference eLearning and Software for Education. 'Carol I' National Defence University, pp. 363-369. Retrieved from: https://search.proquest.com/openview/34ab81585845f697b3a84d371fa81b2b/1?pq-origsite=gscholar&cbl=1876338, 3 May 2020.
3. Centralny Instytut Ochrony Pracy – Państwowy Instytut Badawczy w uzgodnieniu z Głównym Inspektoratem Pracy (2020). *Bezpieczeństwo i ochrona zdrowia osób pracujących w czasie epidemii COVID-19. Ogólne wytyczne i lista kontrolna*. Retrieved from: https://m.ciop.pl/CIOPPortalWAR/appmanager/ciop/mobi?_nfpb=true&_pageLabel=P530002293515888667057 66&html_tresc_root_id=300011301&html_tresc_id=300011382&html_klucz=77777&html_klucz_spis=
4. *Coronavirus disease (COVID-19): Mass gatherings* (2023). Retrieved from: https://www.who.int/news-room/questions-and-answers/item/coronavirus-disease-covid-19-mass-gatherings, 20 May 2020.

5. Czech, K. et al. (2020). *Polska gospodarka w początkowym okresie pandemii COVID-19*. Warszawa: Wydawnictwo SGGW. Retrieved from: https://www.researchgate.net/profile/Michal-Wielechowski/publication/348448943_Polska_gospodarka_w_poczatkowym_okresie_pandemii_COVID-19/links/60003740a6fdccdcb8518e2c/Polska-gospodarka-w-poczatkowym-okresie-pandemii-COVID-19.pdf
6. Czub-Kiełczewska, S. (2020). *Okiem IOD: ochrona danych osobowych osób skierowanych na izolację i chorych*, *LEX/el*. Retrieved from: https://sip.lex.pl/komentarze-i-publikacje/komentarze-praktyczne/okiem-iod-ochrona-danych-osobowych-osob-skierowanych-470129429, 3 May 2020.
7. Derda, D. (2020). *Koronawirus. Hejt i ataki na pracowników ochrony zdrowia niepokoją RPO*. Retrieved from: http://bip.brpo.gov.pl/pl/content/koronawirus-hejt-i-ataki-na-pracownikow-ochrony-zdrowia-niepokoja-rpo, 20 July 2020.
8. Dörre-Kolasa, D. (2020). *Ochrona danych osobowych w zatrudnieniu*. Warszawa: CH Beck. Retrieved from: https://ruj.uj.edu.pl/xmlui/handle/item/267936
9. *Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych* (1995). Retrieved from: http://data.europa.eu/eli/dir/1995/46/oj/pol
10. Dziennik urzędowy (2020). *Dziennik Urzędowy*, pp. 1-17.
11. Dziennik Zachodni (2020). *Bill Gates przewidział koronawirusa pięć lat temu. Proroczych słów Gatesa wówczas nikt nie wziął sobie do serca*, *Dziennik Zachodni*. Retrieved from: https://dziennikzachodni.pl/bill-gates-przewidzial-koronawirusa-piec-lat-temu-proroczych-slow-gatesa-wowczas-nikt-nie-wzial-sobie-do-serca/ar/c1-14876555, 20 May 2020.
12. *Europejska Rada Ochrony Danych – EROD* (2018). Retrieved from: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/european-data-protection-board-edpb_pl
13. Falecki, J. (2016). *Dylematy zarządzania kryzysowego w Rzeczypospolitej Polskiej*. Sosnowiec: Wyższa Szkoła Humanitas.
14. Farhadi, N., Lahooti, H. (2021). Pandemic Growth and Benfordness: Empirical Evidence from 176 Countries Worldwide. *COVID, 1(1),* pp. 366-383. Retrieved from: https://doi.org/10.3390/covid1010031, 3 October 2021.
15. Ferraro, F.V. et al. (2020). Distance learning in the covid-19 era: Perceptions in Southern Italy. *Education Sciences, 10(12),* p. 355. Retrieved from: https://doi.org/10.3390/educsci10120355, 20 May 2020.
16. *General Data Protection Regulation (GDPR)* (2020). *General Data Protection Regulation (GDPR)*. Retrieved from: https://gdpr-info.eu/, 20 May 2020.
17. Golinowska, S., Zabdyr-Jamroz, M. (2020). Zarządzanie kryzysem zdrowotnym w pierwszym półroczu pandemii COVID-19: analiza porównawcza na podstawie opinii

ekspertów z wybranych krajów. *Zeszyty Naukowe Ochrony Zdrowia, Zdrowie Publiczne i Zarządzanie, 18(1).* Retrieved from: https://www.ceeol.com/search/article-detail?id=986968.

18. Golińska, P.B. et al. (2021). Mental Health and the Symptoms of PTSD in People with Depression and Anxiety Disorders during the COVID-19 Pandemic. *International journal of environmental research and public health, 18(11),* p. 5542. Retrieved from: https://doi.org/10.3390/ijerph18115542, 20 June 2021.
19. Grupa Robocza Art. 29 ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (2018). *Grupa Robocza Art. 29 - Wytyczne w sprawie przejrzystości na podstawie rozporządzenia 2016/679. 1,* 1-30.
20. Informacyjna Agencja Radiowa (2020). *GIS: w Polsce nie ma koronawirusa*. Retrieved from: https://radioszczecin.pl/6,401790,gis-w-polsce-nie-ma-koronawirusa, 3 May 2020.
21. Jaroszewska, E., Ołdak, M. (2022). Ochrona zdrowia, zdrowie i życie ludzkie jako kluczowe obszary zagrożenia w czasie pandemii COVID-19 w Polsce. *65VOL.*, p. 29.
22. Kancelaria Sejmu (2007). ©Kancelaria Sejmu, p. 1/20. ISAP, pp. 1-20.
23. Keogh-Brown, M.R., Smith, R.D. (2008). The economic impact of SARS: how does the reality match the predictions? *Health policy, 88(1),* pp. 110-120. Retrieved from: https://doi.org/10.1016/j.healthpol.2008.03.003, 20 May 2020.
24. Keogh-Brown, M.R. et al. (2010). The possible macroeconomic impact on the UK of an influenza pandemic. *Health Economics, 19(11),* pp. 1345-1360. Retrieved from: https://doi.org/10.1002/hec.1554
25. Ko, G.S., Yoon, T. (2021). Short-Term Prediction Methodology of COVID-19 Infection in South Korea. *COVID, 1(1),* pp. 416-422. Retrieved from: https://doi.org/10.3390/covid1010035, 21 August 2021.
26. Kopff, A. (1972). Koncepcja praw do intymności i do prywatności życia osobistego. Zagadnienia konstrukcyjne. *Studia Cywilistyczne, XX*, p. 14.
27. *Koronawirus a prawo* (2020). *Must Read Media*. Retrieved from: Koronowirus-a-prawo_raport_6_4_2020.pdf, 20 July 2020.
28. Leśniak, G. (2020). *GIS: Wytyczne dla zakładów przemysłowych to wersja robocza*. Retrieved from: https://www.prawo.pl/kadry/wytyczne-dla-zakladow-przemyslowych-byly-wersja-robocza-i,499782.html, 20 July 2020.
29. Litvinova, T.N. (2022). Risks of Entrepreneurship amid the COVID-19 Crisis. *Risks, 10(8),* p. 163. Retrieved from: https://doi.org/10.3390/risks10080163, 20 June 2022.
30. Majchrzak, D. (2018). O zarządzaniu kryzysowym inaczej. Zarządzanie kryzysowe czy zarządzanie bezpieczeństwem? *Kwartalnik Bellona, 695(4),* pp. 39-61.
31. Majewska, M. (2020). *W Niemczech potwierdzono pierwszy przypadek nowego koronawirusa.* Retrieved from: https://pulsmedycyny.pl/w-niemczech-potwierdzono-pierwszy-przypadek-nowego-koronawirusa-980899, 3 May 2020.

32. Mann, M. (2020). Coronavirus (COVID-19) guidance for schools. *National Association of Independent Schools*, pp. 3-32. Retrieved from: https://www.nais.org/articles/pages/additional-covid-19-guidance-for-schools/, 3 May 2020.
33. Michałowska, M., Stankiewicz, D., Danielak, W. (2015). Zarządzanie sytuacją kryzysową w przedsiębiorstwie. *Zeszyty Naukowe Polskiego Towarzystwa Ekonomicznego w Zielonej Górze, 2(2),* pp. 110-126.
34. Ochocki, T. (2020). *Analiza ryzyka RODO dla pracy zdalnej*. Retrieved from: https://odo24.pl/blog-post.analiza-ryzyka-dla-operacji-przetwarzania-realizowanych-zdalnie, 20 October 2022.
35. Odlanicka-Poczobutt, M., Szyszka-Schuppik, A. (2018). Bezpieczeństwo danych osobowych w świetle nowych przepisów (RODO)–przegląd historyczny. *Zeszyty Naukowe. Organizacja i Zarządzanie/Politechnika Śląska*, *118*, pp. 419-432. Retrieved from: https://doi:10.29119/1641-3466.2018.118.31, 21 May 2020.
36. Oswald, T.K. et al. (2021). Mental health of young australians during the COVID-19 pandemic: Exploring the roles of employment precarity, screen time, and contact with nature. *International journal of environmental research and public health, 18(11),* p. 5630. Retrieved from: https://doi.org/10.3390/ijerph18115630, 20 July 2020.
37. Parlament Europejski i Rada Unii Europejskiej (2016). *Art. 4. - Rozporządzenie Parlamentu Europejskiego I Rady (UE) 2016/679 w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (RODO)*. Retrieved from: https://lexlege.pl/ochr-danych/art-4/, 21 May 2020.
38. Pokutycka, P. (2023). Praca zdalna jako nowa instytucja prawa pracy. *Z Problematyki Prawa Pracy i Polityki Socjalnej*, *4(21),* pp. 1-18. Retrieved from: https://doi.org/10.31261/zpppips.2023.21.01, 21 January 2023.
39. Poláková, P., Klímová, B. (2021). The perception of Slovak students on distance online learning in the time of coronavirus—A preliminary study. *Education Sciences, 11(2),* p. 81. Retrieved from: https://doi.org/10.3390/educsci11020081, 20 May 2021.
40. Polska Agencja Prasowa (2020). *Inspektor sanitarna ze Słubic może stracić stanowisko. Chodzi o zaskakujące wystąpienie ws. koronawirusa*. Retrieved from: https://www.tokfm.pl/Tokfm/7,171710,25760873,inspektor-sanitarna-ze-slubic-moze-stracic-stanowisko-chodzi.html, 20 May 2020.
41. Rodomaniacy (2020). *Alkomat, badanie temperatury – a jednak można?* Retrieved from: https://rodomaniacy.pl/rodowarsztat/covid-i-badanie-temperatury/, 20 July 2020.
42. Urząd Ochrony Danych Osobowych (2020). Oświadczenie Przewodniczącej EROD ws. przetwarzania danych podczas pandemii COVID-19. *Legalis Administracja*. Retrieved from: https://uodo.gov.pl/pl/138/1463, 25 May 2020.

43. Urząd Ochrony Danych Osobowych (2020a). Ochrona danych osobowych podczas pracy zdalnej. *Krajowa Izba Radców Prawnych*. Retrieved from: https://uodo.gov.pl/pl/138/1459, 25 May 2020.
44. Urząd Ochrony Danych Osobowych (2020b). *Oświadczenie Prezesa UODO w sprawie koronawirusa*. Retrieved from: https://uodo.gov.pl/pl/138/1456, 25 May 2020.
45. Urząd Ochrony Danych Osobowych (2020c). *Czy pracodawca może korzystać z prywatnych danych kontaktowych do pracownika?* Retrieved from: https://uodo.gov.pl/pl/138/1636, 25 May 2020.
46. Wikarjak-Górzna, M. (2020). *Pomiar temperatury pracowników a RODO*, *KPMG*. Retrieved from: https://kpmg.com/pl/pl/blogs/home/posts/2020/05/rodonews-pomiar-temperatury-pracownikow-mozliwy-wylacznie-na-podstawie-decyzji-sluzb-sanitarnych.html, 25 May 2021.
47. Wróblewski, D. (2007). Komunikacja kryzysowa – wybrane aspekty komunikacji z mass mediami. *Bezpieczeństwo i Technika Pożarnicza*, *No. 1*. Retrieved from: http://yadda.icm.edu.pl/baztech/element/bwmeta1.element.baztech-4040b0e6-7fb5-4d6d-a6e6-c8389d4528b0, 25 May 2021.
48. Yanovskiy, M., Socol, Y. (2022). Are Lockdowns Effective in Managing Pandemics? *International Journal Of Environmental Research And Public Health*, *19(15)*, p. 9295. Retrieved from: doi: 10.3390/ijerph19159295, 21 August 2022.