MEDICINE, LAW & SOCIETY
Vol. 15, No. 2, pp. 287–304, October 2022

CYBER (IN)SECURITY OF PERSONAL DATA AND INFORMATION IN TIMES OF DIGITIZATION

MIHA DVOJMOČ,[1] MOJCA TANCER VERBOTEN[2]

[1] University of Maribor, Faculty of Criminal Justice and Security, Ljubljana, Slovenia
miha.dvojmoc@um.si
[2] University of Maribor, Faculty of Law, Maribor, Slovenia
mojca.tancer@um.si

CORRESPONDING AUTHOR
miha.dvojmoc@um.si

Accepted
10. 6. 2022

Revised
10. 7. 2022

Published
28. 10. 2022

Abstract In an employment relationship, work and pay are no longer the only important aspects, as importance is increasingly shifting toward obligations concerning the protection of personal data and privacy arising from the prohibition of causing harm to the employer and the duty of loyalty to the employer. The article deals with the constitutionally protected right to privacy and the protection of personal data from the point of view of ensuring cyber security at the employer. The employer is obligated to protect the right to privacy by legal provisions, whereas from the point of view of ensuring the protection of privacy and information, the employer must protect, first and foremost, the personal data of employees. The main purpose of the legal protection of personal data is the lawful and fair processing of the personal data of individuals. Employers are thus facing an increasing number of risks related to the safety of employees and the security of business processes, and it is therefore important to establish comprehensive corporate security to ensure adequate security across all levels.

Keywords
cyber security,
protection of personal data,
protection of privacy,
cyber threats,
protection of business secrets

https://doi.org/10.18690/mls.15.2.287-304.2022

University of Maribor Press

1 Introduction

The development of the information society, new technologies, and now the Covid-19 epidemic have changed the way we work and at the same time highlighted the field of personal data protection, in particular the protection of privacy. In addition to fundamental obligations set out in labor law, the employment relationship itself, as a contractual relationship between the employee and the employer, has given rise to additional obligations that can significantly affect the substance of this relationship, such as the employer's instructions on how to perform work and the prohibition of harmful conduct, ,especially as concerns this article, the protection of personal data, the protection of business secrets and the prohibition of competition. In protecting the right to privacy, there are conflicts between the interests of the employer and the interests and rights of the employee, as well as the interests of third parties (Tomšič, 2016, p. 271).

All of the above raises many questions, such as how safe workers are in the work process, who can use respective data, and how this data is protected, as information science also breaks the boundaries of the known every day and provides access to a wealth of data available to the global public. This data must be carefully protected, especially in cyberspace.

Managing corporate security and, as an integral part of it, information security, is one of the management functions in every company (Dvojmoč & Sotlar, 2021, p. 80). Corporate security is especially important in organizations identified by the state as critical infrastructure, but it is not negligible in all other companies as well. The creation of appropriate plans is critical for the protection of the internal and external security risks of personal data in organizations.

2 Legal regulation of personal data protection

The basis for respecting the personal rights of individuals is defined in fundamental international documents. Article 12 of the Universal Declaration of Human Rights[1] stipulates that no one may arbitrarily interfere with anyone's private life, family, home, or correspondence or insult his honor and reputation and that everyone has

[1] It was adopted and proclaimed by the United Nations General Assembly on 10 December 1948 by Resolution no. 217 A (III). Official Gazette of the RS No 24/18.

the right to legal protection against such interference or attacks. Within the framework of the Council of Europe, Article 8 of the European Convention on Human Rights[2] provides the right to respect for private and family life. Interference with the exercise of this right by the authorities is prohibited unless required by law and necessary in a democratic society for reasons of national security, public security, or the economic well-being of the state, to prevent disorder or crime, to protect health or morality, or to protect the rights and freedoms of others. The Charter of Fundamental Rights of the European Union[3] was adopted in 2000 and includes among the freedoms the respect for private and family life, whereby Article 8 provides for the protection of personal data which must be processed fairly, for certain purposes and with the consent of the person concerned, or on another legitimate basis determined by law.

At the EU level, the first personal data protection regulation was Directive 95/45/EC on the protection of personal data,[4] which aimed to harmonize the protection of fundamental rights and freedoms of individuals regarding the processing of such data and ensure the free movement of personal data between the Member States. The treatment of communication technologies in connection with the protection of personal data was addressed by the later Directive 2002/58/EC of the European Parliament and the Council on the processing of personal data and the protection of privacy in the electronic communications sector.[5]

The first regulation adopted was Regulation 2016/679 of the European Parliament and the Council (2016), on the protection of individuals with regard to the processing of personal data and on the free movement of such data. This Regulation repealed Directive 95/46/EC (General Data Protection Regulation),[6] and lays down rules concerning both individuals in the processing of personal data and with respect to the free movement of personal data.It also protects the fundamental rights and freedoms of individuals and their right to the protection of personal data. The next legal instrument to be adopted was Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with

[2] Official Gazette of the Republic of Slovenia (13.6.1994) MP, No 7-41/1994 (RS 33/1994).
[3] Official Journal of the European Union, No 2012/C-326/02.
[4] Directive 95/46 / EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 321 (hereinafter: "Directive 95/46/EC" or "Directive").
[5] Official Journal L 201, 31/07/2002 p. 0037 - 0047.
[6] Official Journal of the European Union, No L 119/1.

regard to the processing of personal data processed by the competent authorities for the purpose of preventing, investigating, detecting or prosecuting criminal offenses, and on the free movement of such information and repealing Council Framework Decision 2008/977/PNZ.[7]

There are two approaches to EU data protection law, that is, on the one hand, to help facilitate the free movement of personal data and, on the other hand, to allow the free movement of personal data in accordance with legal requirements deriving from fundamental rights, the nature of the right to privacy, and the right to protection of personal data of individuals (Mondschein & Monda, 2019, p. 56). The General Data Protection Regulation has six general principles of data protection: fairness and legality, purpose limitation, data minimization, accuracy, storage limitation and integrity and confidentiality. However, data protection is supported not only through transparency by way of providing complete information to individuals and but also by responsibility (Goddard, 2017, p. 703).

In Slovenia, the general right to privacy is a constitutionally protected category (Krapež, 2020, p. 1168). The need for the right to privacy to have constitutional protection has increased in recent years because of the development of information and communication technologies that can surreptitiously interfere with human privacy and the collection of information about a person (Kaučič & Grad, 2011, p. 128-129). In accordance with Article 35 of the Constitution of the Republic of Slovenia (Ustava Republike Slovenije, URS),[8] the protection of privacy rights and personal rights is guaranteed. Human privacy, guaranteed by Article 35 of the URS, falls within the realm of human movement, which is characterized and constituted by the fact that man forms and maintains it himself.[9] Article 38 of the URS ensures the protection of personal data. The use of personal data counter to the purpose for which it was collected is prohibited. The collection, processing, purpose of use, control, and protection of confidentiality of personal data are determined by law. Everyone has the right to take knowledge of the personal data collected concerning him and the right to judicial protection in the event of their misuse. The goal of personal data protection is not the protection of the personal data per se, but rather

[7] Official Journal of the European Union, No L 119/89.
[8] Official Gazette of the Republic of Slovenia, No 33/91-I, 42/97 - UZS68, 66/00 - UZ80, 24/03 - UZ3a, 47, 68, 69/04 - UZ14, 69/04 - UZ43, 69/04 - UZ50, 68/06 - UZ121,140,143, 47/13 - UZ148, 47/13 - UZ90,97,99, 75/16 - UZ70a and 92/21 - UZ62a.
[9] Item 12 of the USRS Decision Up 32/94 of 16 June 1994, ECLI:SI:CPVO:1995:Ref. 32.94.

the protection of the individual this personal data relates (Kaučič, Grad, 2011, p. 132). The URS provides a basis for special handling of personal data, stipulating that, in the field of personal data processing, everything that is not explicitly permitted by law is prohibited (Lesjak, 2019, p. 11).

The master law in the field of personal data protection in the Republic of Slovenia is the Personal Data Protection Act (Zakon o varstvu osebnih podatkov, ZVOP-1),[10] which is not primarily intended solely for the protection of the personal data of employees (Šetinc Tekavc, 2018, p. 287). This law sets out the rights, obligations, principles, and measures to prevent unconstitutional, illegal, and unjustified interference with the privacy and dignity of the individual in the processing of personal data (Senčur Peček, 2012, p. 80).

3 Protection of privacy and personal data in employment relationships

What separates an employment relationship from other relationships under civil law is that it contains an element of subordination or seniority of one of the parties, which exudes the power or sometimes superiority of the employer that may result in the exploitation of the weaker party (Zupančič, 2015, p. 22).

No binding legal source has been adopted either at the universal or the regional level that would clearly and precisely define the privacy of the employee and the limits of permissible supervision at the workplace (Zupančič, 2015, p. 22). The situation during the epidemic has led to the blurring of the boundaries between public and private even though it is the employer's responsibility to control the worker's work process and work. The field of privacy in the workplace falls within the framework of both labor law and legislation in the field of personal data protection.

To illustrate, video surveillance and biometric measures that employees are subject to are regulated by ZVOP-1, whereas worker protection is regulated primarily by the Employment Relationships Act (Zakon o delovnih razmerjih, ZDR-1)[11] and the Labor and Social Security Records Act (Zakon o evidencah na področju dela in

[10] Official Gazette of the Republic of Slovenia, No 94/07 - official consolidated text and 177/20.
[11] Official Gazette of the Republic of Slovenia, No 21/13, 78/13 - amended, 47/15 - ZZSDT, 33/16 - PZ-F, 52/16, 15/17 - exc. US, 22/19 - ZPosS, 81/19, 203/20 - ZIUPOPDVE, 119/21 - ZČmIS-A, 202/21 - odl. US, 15/22 and 54/22 - ZUPŠ-1.

socialne varnosti, ZEPDSV),[12] which specifies the personal data of employees the employer has the right to process (Tomšič, 2016, p. 275). Due to the absence of legal regulation in this area, the Information Commissioner (IC) recommended that employers adopt internal acts (Krapež, 2020, p. 1169).

The purpose of the IC guidelines was to provide practical guidance and recommendations on how employers should meet the requirements of the General Data Protection Regulation in practice (IC, 2019, p. 4). As noted already by Pirc Musar, this type of preventative action of adopting internal rules means that each employer must consider what individual data represent, which documents are a business secret, and who can access the data (Pirc Musar, 2009, p. 3). In the guidelines, the IC emphasizes that the processing of personal data in the employee-employer relationship must take into account and understand both the interests of the employer and the interests of the employee, as the evaluation of employee performance, use of working time, and work assets to the most rational extent possible, effectiveness and safety of the work process and control thereof, and the prevention of possible abuse are arguments that can drive employers to control their employees (Tovornik, 2017, p. 26).

With the development of digitalization and information and communication technology, this area has developed not only in the direction of personal or physical control by the employer but also in the direction of software control (Polajžar, 2021, p. 274). This means that, in this case, there are two areas or two aspects that need to be regulated; the employer aspect and the protection of data that are within the realm of responsibility of the employer, and the employee aspect and the protection of data that are within the realm of responsibility of the employee as an individual. Information systems and tools allow professional life to intrude into the private sphere. The line between life at home and the workplace and between working time and private life has become increasingly blurred, in part due to developments in the workplace and even more so due to changes in work arrangements during the epidemic. Moreover, it is not always easy to distinguish between the workplace and private information (Mitrou & Karyda, 2005, p. 168).

[12] Official Gazette of the Republic of Slovenia, No 40/06.

Certain duties on the part of the employer and its employees who handle personal data may also be required based on other regulations relating to the employer's activity; for civil servants, for example, based on the Civil Servants Act (Zakon o javnih uslužbencih, ZJU).[13] The system of personal data protection of patients in health care institutions is regulated in the most detail, binding employees to handle such data appropriately, as set out in the Patients' Rights Act (Zakon o pacientovih pravicah, ZPacP)[14] and the Health Care Activity Act (Zakon o zdravstveni dejavnosti, ZZDej).[15] Additional questions arose during the epidemic on the use of official funds due to the system of work for private purposes, which is regulated, at least in the public sector, by the Decree on Administrative Operations (Uredba o upravnem poslovanju, UUP),[16] which emphasizes that the use of information communication equipment for private purposes must not cause information risks and is allowed only to the extent that does not hinder or endanger the work process (Tomšič, 2016, p. 276).

As mentioned earlier, the employer also has a duty toward its employees regarding the protection of personal data that it learns of during the term of the employment relationship as a matter of course. Under Articles 46 and 47 of ZDR-1, the employer is obligated to protect the employee's personality and privacy and his personal data under Article 48 of ZDR-1, as noted in case No Pdp 214/2011[17] (Šetinc Tekavc, 2018, p. 288). Areas where the employee's privacy is interfered with are diverse and appear, for example, in the areas of privacy of the candidate in the recruitment process, protection of personal data of the employee, video surveillance at work, and privacy related to the use of official means of communication, and others (Senčur Peček, 2012, p. 79).

Personal data and privacy are increasingly exposed, which may lead to misuse of data, that is, the use of data in a way that was not foreseen and is not allowed for various reasons, such as personal gain, unlawful data collection, and use of trade secrets. The misuse of personal data or privacy by computer systems is called

[13] Official Gazette of the Republic of Slovenia, No 63/07 - official consolidated text, 65/08, 69/08 - ZTFI-A, 69/08 - ZZavar-E, 40/12 - ZUJF, 158/20 - ZIntPK-C, 203/20 - ZIUPOPDVE, 202 / 21 - odl. US and 3/22 - ZDeb.
[14] Official Gazette of the Republic of Slovenia, No 15/08, 55/17 and 177/20.
[15] Official Gazette of the Republic of Slovenia, No 23/05 - official consolidated text, 15/08 - ZPacP, 23/08, 58/08 - ZZdrS-E, 77/08 - ZDZdr, 40/12 - ZUJF, 14/13, 88/16 - ZdZPZD, 64 / 17, 1/19 - odl. US, 73/19, 82/20, 152/20 - ZZUOOP, 203/20 - ZIUPOPDVE, 112/21 - ZNUPZ and 196/21 - ZDOsk.
[16] Official Gazette of the Republic of Slovenia, No 9/18, 14/20, 167/20 and 172/21.
[17] VDSS decision Pdp 214/2011, ECLI:SI:VDS:2011:PDP.214.2011 of 17.03.2011.

cybercrime, which can occur in a variety of ways on state-of-the-art devices that violate an individual's privacy to a worrisome extent. To improve legal clarity and certainty regarding privacy in the workplace and to enhance security, individual countries are rebuilding their regulatory systems due to epidemic-related phenomena (Chauhan & Kshetri, 2021, p. 129).

4 Protection of privacy, personal data, and cyber security at the employer

Safety is one of the most important aspects of the work environment, and the employer must provide its employees with a safe working environment (Mehl, 2021). Security is a complex concept, but in the age of globalization, it has gained digital insight. This must be ensured in the workplace both systematically and comprehensively, as only such a system enables adequate protection of the privacy and personal data of all employees.

The right to privacy is inalienable to an individual under today's law and beliefs. Its definition is difficult to determine, as it covers a wide range of individual aspects of privacy. Precisely from a legal point of view, privacy is not unambiguously or clearly defined due to its subjectivity. One of the most general definitions of privacy is that a person has the right to be separate from the public and that the individual in privacy has the right to decide on the publicity of their personal affairs (Lampe, 2004, 94).

Teršek (2006) divides the sphere of privacy into three mixed levels of privacy. The most sensitive segment is the sphere of intimacy, the intermediate segment is the stage where an individual establishes contact with other people, and the author defines the third segment as the intertwining of privacy with the public where an individual establishes a certain private-intimate connection with other people. In all three situations, an individual can justifiably expect privacy at work as well (Teršek, 2006, p. 23).

The absolute nature of the right to privacy does not mean that it is also absolutely protected. Interference with the right to privacy is allowed, but it must meet certain criteria. According to the law, it can only be interfered with by state authorities, the police, law enforcement agencies, intelligence services, and partly also detectives and

employers. The interference must be lawful and necessary. Interference must be appropriate for achieving the desired and constitutionally permissible goal, where proportionality must be taken into account (Lampe, 2004, p. 361). An individual is protected from disclosure of his/her privacy wherever he/she can reasonably expect to be alone. We call this the concept of expected privacy. Even if the individual is not alone, his right to privacy is not only protected in private relationships within his home but it is understood that the private sphere is unique to the individual and "moves" with him. Wherever it is located, even in the workplace, one can expect protection of the right to privacy (Sotlar & Trivunovič, 2012, p. 328).

The employer is obliged to protect the right to privacy by the legal provisions defined in the previous chapter. From the point of view of ensuring the protection of privacy and information, the employer must protect the personal data of employees. The main purpose of the legal protection of personal data is the lawful and fair processing of the personal data of individuals. Personal data is any information relating to a particular individual, regardless of the form in which it is expressed. Personal data is also other information that does not in itself constitute personal data, but in combination with each other can lead to the identification of a specific person, as set out in the 2018 EU General Data Protection Regulation (GDPR). GDPR was adopted in 2016 and has been in force since 2018. Because one's personal information is so broad, it is essential for the employer to lawfully secure the processing of this information so as to preserve the dignity and integrity of the employee.

Today, information has also become an important strategic business tool, and at the same time, information security threats are increasing daily. Employer security thus requires a strategic approach and must be regulated comprehensively. The security of personal data and information is subordinate to corporate security (Dvojmoč, 2019, p. 208).

As employers face increasing risks related to the safety of employees and the security of business processes, it is important to establish comprehensive corporate security to ensure adequate security at all levels. Ensuring adequate corporate security in an organization is a complex process, but it requires comprehensive knowledge and approaches, which are implemented in interdependence with all other key business functions. The role of corporate security is to protect organizations, their

technologies, employees, technical resources, and customer data from internal and external threats (Dvojmoč, 2022, p. 10). The organization of corporate security in organizations requires special knowledge, which is reflected in six main processes:

1) legal provision of lawful and uninterrupted operations,
2) legal provision of security "know-how" specific to the organization,
3) legal and physical protection of technologies and information systems (IT security),
4) legal protection of property rights and intellectual property rights,
5) ensuring private security activities, as determined by a government and
6) ensuring safety activities (Dvojmoč, 2022, p. 10).

Awareness of the need for integrated risk management and implementation of integrated security solutions are essential components that allowing organizations more flexibility and better prepared to meet global requirements. In this system, corporate security must play an extremely important role in every organization (Čaleta et al., 2014, p. 14). In addition to reducing risks, the goal of the corporate security system is primarily to ensure the internal security of the institution, and this is achieved through a series of measures. Measures are enforced at the legal, organizational, functional, technical, and personnel levels, but must be in accordance with compliance with laws and internal records and with ensuring the safety of people and property (Čaleta & Vršec, 2013, p. 8).

We live in a time when technology is evolving at an incredible rate. At the same time, increasingly sophisticated attack techniques are being developed, which, if carried out, can jeopardize the security of the company and the individuals employed there. Most often, attackers strike employees' data or business secrets (McBride et al., 2012, p. 14). Cybersecurity refers to the security of networks and information against risks and incidents. Risks are understood as circumstances or events that may hurt safety, and incidents are circumstances or events that have a negative effect on safety (Ilievrski & Bernik, 2013, p. 328). We must be aware of both and formulate appropriate security plans to thwart them. Most well-informed organizations believe that cybersecurity is becoming a key business issue, and countries that have already issued national cybersecurity strategies and guidelines are also aware of its importance.

The fundamental task of cybersecurity is to strengthen and systematically regulate the field of security in the company concerning the development of the company, its activities and areas of activity, and the maturity of the internal environment of processes and information and communication infrastructure. It must ensure the security of employees, management, partners, and stakeholders in cyberspace ecosystems, with security being the least of these dimensions (Wahid, 2022, p. 2).

5 Cyber threats to personal data and information

Cyber-attacks are becoming more advanced; inviolability is almost gone. Companies frequently are victims of the attacks. Many security experts observe that it is the rare company that has yet to experience a cyber-attack. Indeed, many companies that have been attacked failed to even realize it (Humayun et al., 2020, p. 3181).

In digital networks, a cyber-attack is an attempt to disclose, modify, disable, destroy, steal, or gain unauthorized access to a resource or its unauthorized use (Bernik & Meško, 2011, p. 243). An attack targets computer information systems, infrastructures, or computer networks, and attackers most often attempt to access data and functions with malicious intent (Bossler, 2021, p. 932). Attackers are increasingly focusing their attacks so as to cause as much damage as possible in the processes. These more damaging attacks severely degrade the ability of victim companies to operate smoothly and they also pose an extremely high threat to other sensitive information and can lead to significant financial loss, as they access important data in the computer system (Humayun et al., 2020, p. 3183).

Since security threats change every day, so too must the protection of personal data be constant and flexible so as to be able to effectively meet the emerging threats (Fransen et al., 2015). Information has become the most important strategic business tool, but because threats in the cyber system are increasing daily, it is crucial that we adequately protect ourselves from security risks. Organizations are, and always will be, reliant on their information systems. In order to prevent cyber-attacks it is necessary to raise awareness and train users in the use of information technology and to protect vulnerabilities in information systems (Morrow, 2021, p. 184).

From the standpoint of endangering personal theft and theft of personal data in the work environment, phishing attacks and directorial fraud pose the greatest threat. The latter is a very common example of social engineering and fraud targeting companies and other organizations. Online fraudsters look for specific director and accounting information. Here, a fraudulent employee who is authorized to make payments by trickery deceives him into paying a fake account or making an unauthorized transfer from a commercial bank account. Perpetrators use a fake e-mail in which they falsify the sender's address and falsely present themselves as the company's director. Such fraud is characterized by transfers to foreign bank accounts. Account fraud, where the company is approached by someone who claims to represent the supplier/creditor/provider and requests that the bank details for the payment be changed, is also common. The proposed new account, however, is under the control of fraudsters. Frauds from fake online banks are also very common. The individual receives a message that contains a link to a fake bank website demanding disclosure of the individual's financial and personal information. Currently, the most common scam is an investment. These are often seemingly profitable investment opportunities such as stocks, bonds, cryptocurrencies, precious metals, real estate investments abroad, or alternative energy sources (URSIV, 2022, p. 6).

SI-CERT (Slovenian Computer Emergency Response Team) is a designated national computer security incident response team. SI-CERT estimates that phishing attacks have not decreased and that they represent an increasing share of the incidents in the work environment. Phishing is a very simple social engineering technique, where the appearance of the authenticity of the message is created and the addressee is tricked into disclosing its login information and/or credit card number. With phishing, online fraudsters obtain personal data and data that we use in information systems (usernames, passwords to social networks, e-mails ...). The greatest damage resulting from phishing attacks is caused by the disclosure of data pertaining to online banking, as fraud can also harm us financially (SI-CERT, 2020, p. 12). Since cyber-attacks have become part of our daily lives, it is imperative that companies understand the importance of establishing and strengthening cyber security for the protection of both employees and work processes. The failure to acknowledge, understand and take action to prevent cyber attacks will severely endanger the privacy rights of employees and their personal data.

6 Protection and solutions - ensuring cyber security of personal data and information

In recent years, we have seen a marked increase in cyber-attacks on businesses. In addition to financial gain, attackers want to gain access to the personal data of employees and customers (SI-CERT, 2020, p. 44). Perpetrators target both large and small companies, but the latter are usually easier targets because they often lack sufficient knowledge regarding cyber-security and therefore fail to institute proper (or any) counter-measures to thwart the inevitable fraudulent attacks.

Most cyber-intrusions are preventable through proper education. Understanding the nature of cyber-attacks is the critical first step required to prevent them or to at least mitigate their harmful consequences. Slovenia has developed a Cyber Security Strategy[18], which was created precisely to establish a system for ensuring a high level of cyber security for all entities and businesses in Slovenia. To strengthen the system for ensuring cyber security, the country is encouraged, and at the same time committed to, adopting strategic documents at the national and international levels The are: The Resolution on the National Security Strategy of the Republic of Slovenia[19], the Cyber Security Strategy of the European Union "Open, Secure and Secure Cyberspace"[20] and the proposal for Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 on measures for high common level security of networks and information systems in the Union.[21] With this strategy, Slovenia has defined measures for the establishment of a national cyber security system that will be able to respond quickly to security threats and will provide effective protection of information and communication infrastructure and information systems, thus ensuring uninterrupted operation of both public and private sectors (Security, 2016, p. 4).

However, cyber-attacks can also be successfully avoided through a series of measures. The most important steps include having an awareness of our human vulnerabilities, establishing and choosing a secure wired or wireless network, avoiding open networks or using open networks, simultaneously using Virtual

[18] Retrieved from: https://www.gov.si/assets/ministrstva/MJU/DID/Strategija-kibernetske-varnosti.pdf
[19] Official Gazette of the Republic of Slovenia, No. 59/19.
[20] Retrieved from: https://digital-strategy.ec.europa.eu/en
[21] Official Gazette of the EU, 16.12.2020 COM(2020) 823 final, 2020/0359(COD).

Private Network (VPN) services, and regularly updating software. In addition to education and awareness, theft of personal data and information through fraudulent schemes can be prevented by installation of appropriate hardware and software. It is important that companies have a new generation firewall properly installed and managed and that appropriate anti-virus programs are in place. In addition to viruses, most antivirus programs today can detect and remove other types of malware, including worms, trojans, adware, spyware, ransomware, browser hijackers, keyloggers, and rootkits.

7 Conclusion

Aside from fundamental obligations, several other obligations arise in the employment relationship as a contractual relationship between the employee and the employer, which can significantly affect the substance of this relationship, such as the employer's instructions on how to perform work, prohibition of harmful conduct, personal data protection, protection of business secrets, and non-competition. The basis for respecting the personal rights of individuals is defined in basic international documents; in the Republic of Slovenia, the right to privacy is a constitutionally protected category. Personal data and privacy are increasingly exposed, and data may be misused and used in ways that are not permitted by law.

Ensuring the security of employees' information and personal data entrusted to and in the hands of the employer is thus crucial not only for the effective protection of risks but also for protecting employees' privacy rights. Corporate security and cyber security, with appropriate placement within the organization's system, significantly contribute to reducing risks, including in the field of personal data security. The already listed duties of the employer and the pitfalls of new information technologies are not just different security policies, but a living organism that must constantly adapt to new threats and situations. In any case, when implementing new technologies that impact personal data, including the self-protection of personal data, we must not forget the GDPR or its provisions on the preparation of personal data protection.

Legal Acts

Civil Servants Act, Official Gazette of the Republic of Slovenia, No 63/07 - official consolidated text, 65/08, 69/08 - ZTFI-A, 69/08 - ZZavar-E, 40/12 - ZUJF, 158/20 - ZIntPK-C, 203/20 - ZIUPOPDVE, 202 / 21 - odl. US and 3/22 - ZDeb.

Decree on Administrative Operations, Official Gazette of the Republic of Slovenia, No 9/18, 14/20, 167/20 and 172/21.

Council Framework Decision 2008/977/PNZ, Official Journal of the European Union, No L 119/89.

Constitution of the Republic of Slovenia, Official Gazette of the Republic of Slovenia, No 33/91-I, 42/97 - UZS68, 66/00 - UZ80, 24/03 - UZ3a, 47, 68, 69/04 - UZ14, 69/04 - UZ43, 69/04 - UZ50, 68/06 - UZ121,140,143, 47/13 - UZ148, 47/13 - UZ90,97,99, 75/16 - UZ70a and 92/21 - UZ62a Official Gazette of the Republic of Slovenia, No 94/07 - official consolidated text and 177/20.

Directive 95/45/EC on the protection of personal data, Official Gazette of the Republic of Slovenia (13.6.1994) MP, No 7-41/1994 (RS 33/1994).

Directive 2002/58/EC of the European Parliament and the Council on the processing of personal data and the protection of privacy in the electronic communications sector, Official Journal L 201, 31/07/2002, p. 0037 - 0047.

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, OJ L 281, 23.11.1995, p. 321 (hereinafter: "Directive 95/46/EC" or "Directive").

Employment Relationships Act, Official Gazette of the Republic of Slovenia, No 21/13, 78/13 - amended, 47/15 - ZZSDT, 33/16 - PZ-F, 52/16, 15/17 - exc. US, 22/19 - ZPosS, 81/19, 203/20 - ZIUPOPDVE, 119/21 - ZČmIS-A, 202/21 - odl. US, 15/22 and 54/22 - ZUPŠ-1.

General Data Protection Regulation, Official Journal of the European Union, No L 119/1.

Health Care Activity Act, Official Gazette of the Republic of Slovenia, No 23/05 - official consolidated text, 15/08 - ZPacP, 23/08, 58/08 - ZZdrS-E, 77/08 - ZDZdr, 40/12 - ZUJF, 14/13, 88/16 - ZdZPZD, 64 / 17, 1/19 - odl. US, 73/19, 82/20, 152/20 - ZZUOOP, 203/20 - ZIUPOPDVE, 112/21 - ZNUPZ and 196/21 - ZDOsk.

Labor and Social Security Records Act, Official Gazette of the Republic of Slovenia, No 40/06.

Patients' Rights Act, Official Gazette of the Republic of Slovenia, No 15/08, 55/17 and 177/20.

Personal Data Protection Act, Official Gazette of the Republic of Slovenia, No 94/07 - official consolidated text and 177/20.

Universal Declaration of Human Rights, Official Gazette of the RS No 24/18.

The Charter of Fundamental Rights of the European Union, Official Journal of the European Union, No 2012/C-326/02.

References

Bernik, I. & Meško, G. (2011). Internetna študija poznavanja kibernetskih groženj in strahu pred kibernetsko kriminaliteto. *Revija za kriminalistiko in kriminologijo*, 62(3), 242-252.

Bossler, A. M. (2021). Neutralizing Cyber Attacks: Techniques of Neutralization and Willingness to Commit Cyber Attacks. *American Journal of Criminal Justice*, (46), 911-934.

Chauhan, P. S. & Kshetri, N. (2021). State of the Practice in Data Privacy and Security. *Computer*, 54(8), 125-132. doi: 0.1109/MC.2021.3083916.

Čaleta, D. & Vršec, M. (ur.) (2013). *Management of Corporate Security – New Approaches and Future Challenges*. Ljubljana: Institute for Corporative Security Studies.

Čaleta, D., Vršec, M. & Ivanc, B. (ur.) (2014). *Corporate Security – Open Dilemmas in the Modern Information Society*. Ljubljana: Institute for Corporative Security Studies.

Dvojmoč, M. & Sotlar, A. (2021). Zasebno varovanje in korporativna varnost v času epidemije covida-19 v Sloveniji. *Revija za kriminalistiko in kriminologijo*, 72(1), 79-90.

Dvojmoč, M. (2019). Corporate intelligence as the new reality: the necessity of corporate security in modern global business. *Varstvoslovje*, 21(2), 205-223.

Dvojmoč, M. (2022). *Integralna korporativna varnost, 2 letnik: magistrski študijski program Varstvoslovje*, Zbrano študijsko gradivo. Ljubljana: Fakulteta za varnostne vede.

Goddard, M. (2017). The EU General Data Protection Regulation (GDPR): European regulation that has a global impact. *International Journal of Market Research*, 59(6), 703-705. doi: 10.2501/IJMR-2017-050.

Humayun, M., Niazi, M., Alshayeb, M. & Mahmood, S. (2020). Cyber Security Threats and Vulnerabilities: A systematic mapping Study. *Arabian Journal of Science and Engineering*, 45, 3171-3189.

Ilievski, A. & Bernik, I. (2013). Boj proti kibernetski kriminaliteti v Sloveniji: organiziranost, način, pravna podlaga in njeno izpolnjevanje. *Varstvoslovje*, 15(3), 317-337.

Informacijski pooblaščenec (2019). *Varstvo osebnih podatkov v delovnih razmerjih, Smernice informacijskega pooblaščenca*. Retrieved from https://www.ip-rs.si/fileadmin/user_upload/Pdf/smernice/Smernice_-_Varstvo_OP_v_delovnih_razmerjih_verzija_1.1_koncna.pdf (May 31, 2022).

Kaučič, I. & Grad, F. (2011). *Ustavna ureditev Slovenije*, 5th ed. Ljubljana: GV založba.

Krapež, K. (2020). Posegi v zasebnost (pedagoških) delavcev med epidemijo covid-19 in po njej – kje so meje dovoljenega. *Podjetje in delo*, 46(6-7), 1166-1177.

Lesjak, A. (2019). Article 38. In: Avbelj M. (ed.) *Komentar Ustave Republike Slovenije*. Nova Gorica: Nova Univerza, Evropska pravna fakulteta.

McBride, M., Lemuria, C. & Merrill, W. (2012). Exploring the role of individual employee characteristics and personality on employee compliance with cybersecurity policies. *RTI International*, 6-41.

Mehl, B. (2021). The State of Employee Privacy and Surveillance in 2021. Retrieved from https://www.getkisi.com/blog/state-employee-privacy-surveillance (May 18, 2022).

Mitrou, L. & Karyda, M. (2005). Employees privacy vs. employers security: Can they be balanced?. *Telematics and Informatics* 23(3), 164-178. doi: 10.1016/j.tele.2005.07.003.

Mondschein, C. F. & Monda, C. (2019). The EU's General Data Protection Regulation (GDPR) in a Research Context. *Fundamentals of Clinical Data Science*, 55-74.

Morrow, A. B. (2021). Information security and cyber threats and vulnerabilities. In: *Intermodal Maritime Security. Supply Chain Risk Mitigation* (pp. 169-193). Elsevier. doi: 10.1016/B978-0-12-819945-9.00010-1.

Pirc Musar, N. (2009). Zasebnost na delovnem mestu – jo imamo ali ne, naj jo imamo ali ne?. *Pravna praksa*, 28(9), 3.

Polajžar, A. (2021). Varstvo zasebnosti delavca v dobi digitalizacije: GDPR in vloga delavskih predstavnikov. *Delavci in delodajalci*, 21(2-3), 273-293.

Senčur Peček, D. (2012). Varstvo zasebnosti v delovnem razmerju. *Anali PAZU,* 2(2), 78-83.

SI CERT (2020). Poročilo o kibernetski varnosti. Retrieved from https://www.cert.si/wp-content/uploads/2021/07/Si-CERT-e_porocilo-o-kibern-varnosti-2020.pdf (May 18, 2022).

Sotlar, A. & Trivunovič, J. (2012). Detektivi in varstvo zasebnosti v Republiki Sloveniji, *Varstvoslovje*, 14(3), 307-330.

Strategija kibernetske varnosti Republike Slovenije (2016). Retrieved from https://www.gov.si/assets/ministrstva/MJU/DID/Strategija-kibernetske-varnosti.pdf (May 16, 2022).

Šetinc Tekavc, M. (2018). Pregled sodne prakse s področja varovanja osebnih podatkov, zaupnosti in poslovne skrivnosti. *Delavci in delodajalci*, 18(2-3), pp. 285-307.

Teršek, A. (2006). Svoboda medijev in varstvo zasebnosti: Kritika dveh precedensov, predlog razvrstitve »javnih oseb« in predlog ustavnopravnih standardov, Dnevi civilnega prava, Portorož.

Tomšič, A. (2016). Varstvo delavčeve informacijske zasebnosti. *Delavci in delodajalci*, 16(2-3), 269-282.

Tovornik, T. (2017). Smernice za varstvo osebnih podatkov v delovnih razmerjih. *Pravna praksa*, 36(2), 26.

Urad vlade Republike Slovenije za informacijsko varnost (URSIV) (2022). Polletno poročilo o kibernetskih incidentih in napadih. Retrieved from https://www.gov.si/assets/organi-v-sestavi/URSIV/Datoteke/Porocila/Polletno_porocilo_2_2021_fin1.pdf (May 31, 2022).

Wahid, W. (2022). Cyber Security, Text-based password security. *Air University Islamabad*, 1-2.

Zupančič, L. (2015). Meja dopustnega nadzora uporabe interneta in elektronske pošte na delovnem mestu. *Pravna praksa*, (1), 22.