GDPR and its Implementation in a Healthcare Facility

MICHAELA ZELENÁ, PETR SVOBODA, JAKUB RAK, MIROSLAV TOMEK
Tomas Bata University in Zlín
Nám. T. G. Masaryka 5555, 760 01
CZECH REPUBLIC
m_zelena@utb.cz, psvoboda@utb.cz, jrak@utb.cz, tomek@utb.cz

Abstract: - This article deals with the implementation of the GDPR in a selected healthcare facility. The theoretical part of the article introduces the legislative framework that regulates issues and the most relevant terms relating to the GDPR. The practical part is focused on the characteristics of the selected facility which is subjected to a GAP analysis. Subsequently, the processes carried out in the facility are described. Based on the information available, appropriate measures are proposed and summarized to protect personal data and to guarantee compliance with the requirements of the GDPR. The last part of the article describes data processing and a security incident report form.

Key-Words: - data, GDPR, implementation, protection, personal.

1 Introduction

The General Data Protection Regulation (hereinafter the GDPR) is a general regulation imposing obligations on all entities that process personal data. The GDPR alternations to the regulations of this issue for all countries of the European Union including Iceland, Norway and Liechtenstein. This guarantees a uniform procedure and universal usability within these countries. [1, 2,3]

In addition, this Regulation constitutes obligations for organisations which process personal data and which are denoted by the generic term "personal data controller" no matter if the data is owned by them or taken over for processing purposes. Therefore, the Regulation also applies to supervisory authorities, such as the Office for Personal Data Protection. However, it does not apply to the activities of natural persons and bodies that investigate, detect or prosecute crimes, secure enforcement of sentence, or perform preventive activities. [1, 2, 4]

Thus, it is important to take into account the character of the data, scope, and context, purpose of data processing, possible impact on the rights and liberties of individuals and also the security of the data. [1,2, 4]

That is why the so-called "collector" has been introduced. The collector is an entity that specifies the purposes and means of processing personal data and is primarily responsible for this activity. The collector can be any entity, including a natural person. The collector can hire a processor to perform the requested data operations. These operations are to be explicitly defined (restricted) by the collector through authorization given to the processor. Both entities may consist of any legal form. [1, 3, 4]

The Regulation is based on principles such as lawfulness, fairness and transparency, and the controller must process personal data on legal grounds and in a completely transparent way in relation to the data subject. There are restrictions on the purposes for which personal data can be collected and therefore, there must be a legal cause. Data minimisation - the data must be adequate and relevant to the purpose for which it is collected and then processed. Accuracy of the personal data is another important factor. Storage limitation - preventing data accumulation and storing for a longer period than is needed to process or fulfil a legitimate reason. Integrity and confidentiality - technical and organisational security of personal data. As proof of compliance with these principles, records of processing activities together with codes and certifications are required. [1,2, 4]

2 Characteristics of the selected building

The selected building is a non-state-run healthcare facility providing services in the field of physical medicine and therapy. At the request of the management of the facility, this article does not provide detailed information with respect to the type of internal information provided. Not only does the manager of the facility deal with the actual management but he is also responsible for the performance of activities in the facility. There are four employees, including a physician who

examines the condition of an incoming patient in order to choose the appropriate therapy. Other employees perform physical therapy tailored to the patient's needs. Then there is an assistant who makes appointments and creates schedules for the patients. [1, 5]

Obviously, during the performance of services the facility deals with a large amount of personal data that not only needs to be processed but also archived for a long period of time pursuant to the law. This data is far from being basic. There is also data falling into a special category, such as the health condition of patients and other information that is necessary to determine the appropriate treatment procedure. It is in particular this data that needs to be protected because it can seriously distress a person or cause discrimination against him or her in the event of a leak. [1, 5]

2.1 GAP analysis

The GAP analysis is a method used to define the difference between the current state and the required state. The method is based on two fundamental questions "Where are we at this point in time?" and "Where do we want to be in the future?" [1, 2]

GAP analysis questions	**Answers of the facility**
Where is the personal data collected in the facility? (collection points)	Appointment diary, two computers in medical offices, printer hardware, card files.
What is the structure of data collection?	Categories of personal data of patients – personal data about their health condition.
What tools are used and what is their content?	Computers, paper documents of patients, working agreements, contracts with third parties. Names, surnames, personal numbers, dates of birth, permanent addresses, telephone numbers, e-mail addresses, bank account numbers, and health condition data.
What is the way of obtaining consent to process personal data?	Verbally, by signing a working agreement, by signing the commercial contracts.
Who has access to the data?	All employees.
Based on what authorisation?	Information is needed for the performance of activities related to the purpose of the facility.
How is the data stored and protected?	Backups, technical security, passwords, pseudonymisation.
What systems and applications are used to process the data?	MS Windows, professional encrypted programmes specially designed for healthcare facilities, data box, and insurance portal.
How is the data processed and how does data processing work?	Making an appointment by a patient, medical check-up, physical therapy, invoice to an insurance company, archiving. Employee data, 3 groups – purchase of material, general practitioners, insurance companies.
Are there any forms and processes related to the GDPR?	Processes do exist but it is important to consider the way in which all employees are allowed access to all personal data.
Checking the contractual obligations related to personal data.	All important contractual obligations are fulfilled dutifully and in a well-organised manner in compliance with the GDPR.

GAP analysis questions	Answers of the facility
Obligations and contracts with third parties?	Archiving of invoices only.
What is the approach to assessing the impact on privacy?	Needs to be drawn up.
What is the incident management process and what is the response?	It is within the remit of the manager to report security incidents. All employees are required to report any suspicion of information leakage.
What are the recommendations in the event of non-compliance with the Regulation?	Change the non-compliant condition into a satisfactory condition by accepting appropriate measures to be used in practice.
Who has access to the data?	All employees.
Based on what author-isation?	Information is needed for the performance of activities related to the purpose of the facility.

Table 1 GAP analysis [1, 2, 5]

2.2 Problem Solution

For the purpose of clarity, obtaining personal data from patients has been divided into several stages. Individual stages define the processes of obtaining personal data and further specify appropriate measures for processing and securing personal data to avoid a security incident.

2.2.1 The first stage of processing the patient´s personal data

The data stored relating to patients includes, for example, birth certificate numbers, insurance companies, dates of birth, permanent residence, telephone numbers, and particularly sensitive data, such as hospital discharge summaries, particulars of their current physical condition and social habits. This personal health data, which includes information about past, current and future health conditions, and results of examinations and tests, was provided during registration in the health facility. [5]

Measures

The initial data, such as names, is obtained from patients at the time they make their appointments with the doctor. This is the minimum amount of information obtained. Even at this point, it is necessary to place the emphasis on data protection; i.e. it is not possible to tell third parties if the patient has an appointment or not. Even this piece of information could be detrimental to the patient. For instance, during the recruitment interview a potential employer could see the potential employee as being physically unfit and thus financially disadvantageous to the company. [4, 5]

There is also the risk of leakage of information through mobile phones. If they are smartphones, they are also vulnerable to malware. However, there exist security solutions that will lead to the categorization of devices in which possible attacks are to be detected more easily. [7]

2.2.2 The second stage of processing the patient´s personal data

Other personal data is processed at the time the patient arrives at the premises of the facility and brings a recommendation from his or her general practitioner or other specialist together with an insurance card. He or she can also bring any previously mentioned discharge summaries or other reports on earlier tests or examinations. This information is partially processed digitally; a physician issues a report that is intended for internal staff to perform the appropriate therapy for the patient. This data already falls within the special category of personal data. Therefore, it needs to be sufficiently protected. [5]

In addition, in compliance with the GDPR, it is necessary to collect only purposeful information. This means that there must be a reason to obtain it and it must be essential for determining the appropriate therapy for a particular patient.

Furthermore, only the minimum amount of necessary information should be processed; this information must be complete and not taken out of the context. [4]

Measures

This information is processed digitally and subsequently printed out. The digital form is backed up to another computer and then to a USB flash drive. It is therefore necessary for the computer to be fully secure. The instance a physician processes personal data, it is advisable not to be connected to the Internet. This prevents the computer from being infected by unwanted malware. It is also recommended to perform computer checks using the installed antivirus software or other specific programs. [4, 8]

In addition, it is also appropriate to use "user accounts" on the computer. There should be a computer administrator, e.g. the manager of the facility who has full access rights to the computer and is authorised to perform any operations. There should also be a "user account" for a physician who can only use the computer. [4, 8]

Moreover, an appropriate safe password has to be chosen consisting of at least 8, 10 or more characters with a combination of upper and lower case, digits and characters. It is possible to use a password generator. However, it is essential that only people who are authorized to handle and process data on the computer have access rights and passwords. Otherwise, it would be in breach of the GDPR. [4, 8]

It is necessary to restrict the access of people to a printer, which is a frequent source of passing personal data to third parties. For these cases delayed printing is used; the printer starts printing only when the employee is physically present at the printer. It often happens that the printed document is left in the printer. [3]

When using laptops, because of their mobility, the potential risks of security incidents increase. It is therefore advisable to secure them against theft, preferably mechanically, outside of working hours. [8]

Because data is backed up to a USB flash drive, it is also necessary to mechanically secure this drive. It is also worth considering encryption or pseudonymisation of this data. The GDPR encourages this type of securing because in the event of a security incident – a minor leak of information, it would not be necessary to report this leak to the Office for Personal Data Protection within 72 hours of its finding. However, this would only apply if the special category of personal data was not stored on the backup. This is because the degree of threat to individuals is likely to be more than considerable. [3, 4]

As far as the paper form of the patient data is concerned, it is necessary to secure its storage – card files – by suitable technical means to restrict access to information. In accordance with the GDPR, only people authorised to view or process the data would be allowed to access the card files. As it is required by law to archive documents with data for 5 years, the area in which this data is found should be well locked. [3, 4]

After 5 years, other storage compartments outside the filing cabinets need to be provided for at least 10 years. For securing these documents the same rules apply. The GDPR assumes that after this period, they will be fully destroyed, and they will not be handled or used contrary to their original purpose, otherwise, additional consent from the patients would be required. The same applies should the data be rendered to third parties (this does not apply to communication with insurance companies). [3, 4, 5]

2.2.3 The third stage of processing the patient's personal data

The third stage of processing the patient data is during communication with the insurance company. It is the time when the facility charges the insurance company for the services performed for individual patients. Most frequently, this communication is online through a data box and a digital signature is needed. The communication can also be done through an insurance portal. However, in some cases insurance companies prefer communications by mail. During this communication, data such as information about services performed or patient birth certificate numbers are shared but there are no names attached. Only particular sums of money are charged. [5]

Measures

Online communication requires using an Internet connection. Mobile devices connect to the Internet by means of Wi-Fi wireless connection. For home network security, there are certain rules to protect computers. The best way to secure the network is through a mechanical device called a router. [8]

However, the wireless network signal extends beyond the so-called controlled space of the household or business premises, which means that a highly experienced user located in the vicinity can access the inadequately secured network and cause

damage. An attacker can access shared folders and files, which can then be deleted, rewritten, or even made public. There is also the risk of misusing the network to send messages, threats, or share illegal files. [7]

Possible protection of the Wi-Fi network can be provided by: [7]

- **Changing the network name** in such a way that it does not attact a potential attacker´r attention.
- **Hiding the network name**; the access point is hidden and the network is not visible. The disadvantage, however, is that when connecting to the network, it is necessary to enter the network name manually, which is not very user-friendly. Nevertheless, a proficient user is still able to find the network.
- **Encryption** is one of the most important network security features. An access password has to be entered to access such a network. If the data communication is sufficiently encrypted, it is much more difficult for the attacker to misuse it. Several variants can be used for encryption. Nowadays, WiFi Protected Access 2 encryption technology ("WPA2") is the best protection.1 [7]

As personal data is pseudonymised, capturing this would not cause serious damage without further intrusion of the facility. However, it is necessary to ensure that this information is not accessible to more internal employees than is necessary. [2, 3, 4]

2.3 Security of personal data of employees

In addition to the patient data, there is also data relating to employees processed in the facility. In particular, these are working agreements. They include personal information such as name, permanent address, birth certificate number, telephone number, and bank account number. This data is kept in paper form and it is ensured that only authorized persons have access to it. The facility does not keep any data on former employees because no employee has left the job in the facility so far. However, if this happens in the future, it is essential that the facility only stores such information on employees that needs to be retained. For example, a bank account number is expendable for the future and should be "forgotten". [2, 3, 4]

[1] Debugged WiFi Protected Access 3 ("WPA3") is already being developed.

Furthermore, it is necessary for the employer to aim to protect employees also on a publicly accessible website. If any information is disclosed, it should be done with the consent of the employee. Information frequently made public includes, for instance, names, e-mail addresses, or employees' photos. [3, 4, 5]

When using e-mail correspondence, it is necessary for employees to consider carefully what information they share. If this was sensitive data about patients or themselves, it is wise to consider encryption of e-mails. [3, 4, 5]

It is also necessary to notice what type of information the facility has about potential employees, for instance, after a job interview when various information is required. However, this information must be reasonable. For instance, this is information about education, capability to work on computer or work experience; in short, information that is required to be known in order to perform the job. [3, 4, 5]

Necessary steps to prevent breach of patient and employee data

All employees should be aware of the importance of personal data protection, and it is also significant for them to be aware of the possible impact on the facility in the event of data leakage. Not only are there pecuniary penalties imposed by the GDPR for violating the rules but also the facility could be discredited. Serious consequences can be expected in the event of leakage of information relating to patients, especially when the category of particularly classified information is concerned.

In addition, the training of employees is now compulsory. Such training should include, for instance, explanation of the password policy, documentation disposal, or keeping documents safe and confidential when leaving one's work space. This training should be as thorough as possible and should be open to inquiries. In addition, the training must be well documented and the employees must be familiar with the GDPR. It is also important for the employees to be capable of recognising any breach. [1, 2, 4]

It should be unequivocally specified by the facility who has access to information and what information it is. Should the current state be maintained it is necessary to justify the reasons. Documents in paper form, such as patient health reports, should only be accessible to physicians and not to the staff who perform the physical therapy. Only a report prepared by a treating physician

should be directly accessible to the staff in the selected facility. This measure should be considered and processed in paper form. [1, 2, 4]

Various Internet sources indicate different responsibilities of facilities with respect to processing data relating to health condition. The web page "Datový ochránce, s. r. o." (The Data Protector) specifies that patients will have to give their consent to data processing. However, s. 54 of the General Regulation states that for reasons of public interest in the field of public health it may be necessary to process special categories of personal data without the consent of the patients. Nevertheless, data relating to health condition must not be processed by third parties, such as employers. The web page further states that it may be necessary to revise the scope of data which the patient is aware of but this data is not kept in paper form. [1, 4, 6]

The patient also now has the opportunity to look into his or her data, and the facility is obliged to allow this. For example, the patient can request for the transfer of some information electronically to a physician or another healthcare facility. He or she may also ask to modify the data processed by the facility and to restrict its scope. In addition, he or she may request a complete statement of the data processing activities in particular to gain a good knowledge of the purpose and time at which the data was being accessed and by whom. Moreover, he or she has the right to know the identity of the data processor of his or her data and who has viewed it. [1, 4, 6]

Therefore, the best possible technical measures to protect data are necessary. The GDPR recommends the pseudonymisation and encryption in order to safeguard the data and services. Although a backup is already being performed, regular tests are needed to ensure that the security is sufficient. [1, 4, 6]

2.4 Summary of recommendations for the selected building

It is necessary to document activities during which personal data is processed and to add the types of processed personal data to the selected activities. In addition, it is important to revise the data for which there is no legal ground for retaining.

Moreover, it is necessary to secure mobile devices (laptops, phones, file systems) and to consider who has access to what data and why. It is also necessary to train employees for the GDPR and newly adopted measures, to review the facility's website and to get approvals for publishing employees' data. [1]

It is essential that the facility is prepared for the possibility that patients may ask for information about their data in electronic form, or they may ask for it to be changed or deleted. Last but not least, it is important to learn the right procedure in the event of a security incident. It is also recommended to monitor the development of national legislation that may make the General Regulation more accurate. [1]

3 Proposal for an investigation of a security incident

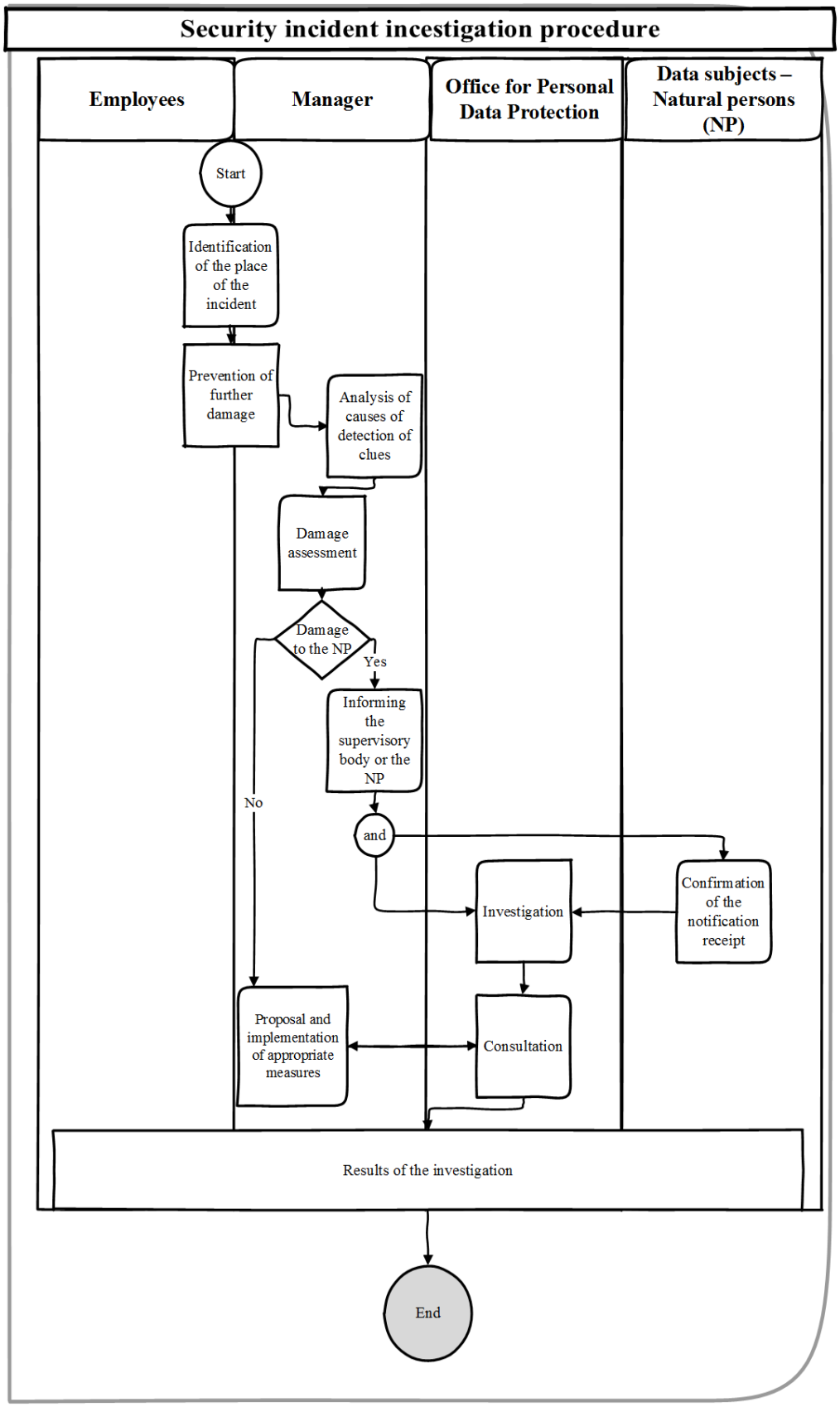

Fig. 1 Scheme of the procedure of the security incident investigation [By the author]

The scheme in Figure 1 introduces a possible procedure in the event of a security incident in the selected facility. The first five steps are assigned to the employees and manager as these activities are within their province. If there is damage detected to natural persons, it is necessary to decide its extent and to choose the correct procedure. It must also be decided if the supervisory body and affected persons should be notified or not. [1]

Based on the process specified in Fig. 2, it is recommended that a template be created for a security incident report. Undoubtedly, this template will speed up reporting to the appropriate authority and ensure completeness of the data.

Explanations of terms from the template are as follows. Information integrity means the completeness of information provided none of it was deleted or modified. Information confidentiality is breached if one cannot be sure whether anyone else has access to this information and if it is not publicly available to unauthorized persons. Similarly, one cannot be sure whether this information can be trusted because it could have been altered or falsified. The availability of information will be breached if it is stolen. The non-repudiation means that someone cannot deny the origin of information. It is acceptable if this information is used for the needs of third parties provided the data subject is aware of this fact. If someone else has access to this information, it is called non-repudiation.

The box titled "Measures overtaken by an attacker" might be misleading. For example, overtaking a physical measure means overcoming the security guards. Logical measures mean encryption and access passwords. Organizational measures mean, for example, employees changing at the workplace. Personnel measure is verification of employees – their credibility or background check. Technical security covers locks on the doors, glass break detector, etc.

The remaining parts are deliberately created as clear and simple as possible for quick and unambiguous identification of the problem and for reporting by any employee. These can be accompanied by brief explanatory notes.

SECURITY INCIDENT REPORT

Facility				
Contact person				
Tel. number		**E-mail**		
Place of incident				
Time of incident				
Offender (if known)				
Incident scenario				
Target of attack				
The following was breached*				
Information integrity	Information confidentiality	Information availability	Information non-repudiation	
Nature of the breach:*				
Intentional		Unintentional		
If intentional:*				
Negligence		Ignorance of security policy		
Measures overtaken by an attacker:*				
Physical	Logical	Organizational	Personnel	Technical security
Breached asset:*				
Hardware	Software	Network	Data	
What is the likelihood of recurrence:*				
Rather low	Medium	High	Certain	
Notes:				

* Delete as applicable

Fig. 2 Template of security incident report [by the author]

4 Conclusion

This article dealt with the implementation of the GDPR in a selected healthcare facility. Significant legislative changes that amend the existing regulatory environment for personal data management were emphasized. In addition, the non-state healthcare facility was introduced, which was first subjected to the GAP analysis and subsequently measures to meet the requirements of the GDPR were proposed. A scheme of the security incident was devised to help solve this situation in a simpler and faster way. In the future, a universal security incident report form will be designed. It will contain essential parameters that the supervisory authority needs to be notified about. [1]

Acknowledgements. This paper is supported by the Internal Grant Agency at Tomas Bata University in Zlin, projects No. IGA/FLKR/2017/003, No. IGA/FLKR/2018/001 and project Excellence of Department of Population Protection.

References:

[1] ZELENÁ, Michaela, Petr SVOBODA, Jakub RAK a Miroslav TOMEK. *The Use of GAP Analysis Method for Implementing the GDPR in a Healthcare Facility: Applied Physics, System Science and Computers III: Proceedings of the 3nd International Conference on Applied Physics, Systém Science and Computers (APSAC2018*. Dubrovnik, Croatia: Springer, 2018. ISSN 978-3-319-75605-9.

[2] NEZMAR, Luděk. GDPR: praktický průvodce implementací. (GDPR: Practical Implementation Guide). Praha: Grada Publishing, 2017, 304 s. Právo pro praxi. ISBN 978-80-271-0668-4.

[3] ČESKO. Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů. (The Czech Republic. Act No. 101/2000 Sb., on the Protection of Personal Data and on Amendment to Some Acts).

[4] EVROPSKÁ UNIE. Nařízení Evropského parlamentu a Rady EU č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (Regulation EU 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) Obecné nařízení o ochraně osobních údajů – General Data Protection Regulation – GDPR.

[5] Rozhovor s jednatelem nejmenovaného vybraného subjektu nestátního zdravotnického zařízení ze dne 5. 4. 2018 (Interview with the manager of the unnamed non-state health care facility of 5 April 2018)

[6] DATOVÝ OCHRÁNCE S.R.O., © Copyright 2018. *Datový ochránce: GDPR ve zdravotnictví* [online]. (The Data Protector: GDPR in Health Services) 2018 [cit. 2018-04-07]. Available at: https://www.datovyochrance.cz/gdpr-ve-zdravotnictvi/

[7] LA POLLA, M, Fabio MARTINELLI a D SGANDURRA. Survey on Security for Mobile Devices. IEEE *Communications Surveys* [online]. IEEE, 2013, 15(1), 446-471 [cit. 2018-04-04]. DOI: 10.1109/SURV.2012.013012.00028. ISSN 1553877X.

[8] KRÁL, Mojmír, Bezpečný internet: Chraňte sebe i svůj počítač. (Safe Internet: Protect yourself and your computer) Prague: Grada Publishing, 2015, 184 p. ISBN 978-80-247-5453-6.