

VULNERABILITIES OF IT INFRASTRUCTURE IN THE MEDICAL FIELD. LEGAL FRAMEWORK ON DATA BREACH LIABILITY

*Rodica-Diana APAN**
*Dan PERJU-DUMBRAVĂ***
*Fineas BORA****

Abstract

One of the worst challenges of today is cyber security. An area where there are a number of breaches of this security is, both at European and national level, the area of medical services. The indication of concrete situations of breach of computer security, presented in this research, opens the way to reflection in the field. The way forward is that set out in the provisions of the Regulation on the protection of individuals with regard to the processing of personal data and the free movement of such data (GDPR). Based on them, the legal framework is established in case of personal data breach and liability steps in data security mission by operators.

Keywords: *computer systems; cyber incidents; security breaches; breach of medical data security*

JEL Classification: [J118, 119]

Introduction

The current context in which society finds itself globally, influenced by the emergence of a major medical crisis, has led to an acceleration of the transition to a hybrid lifestyle at the intersection of real and virtual. This hybrid environment, in which information circulates globally and reaches users through a significant number of devices, has brought about major changes in the way users perceive society and security in general.

1. The general framework of information security

In terms of cyber security, these global events, with a significant impact on the majority of the population, represent one of the highest periods of risk, and the recent medical crisis has favored the emergence of cyber attacks, based on vulnerabilities and fears of a new category. *Lock-down* measures

* PhD, Associate professor, “Dimitrie Cantemir” Christian University, Faculty of Law, Cluj-Napoca, Attorney-at-law, Cluj Bar Association.

** PhD, Professor, “Dimitrie Cantemir” Christian University, Faculty of Law, Cluj-Napoca.

*** PhD Candidate, “Babeş-Bolyai” University, Faculty of History and Philosophy, Doctoral School of International Relations and Security Studies.

imposed globally have overcrowded online networks, thus developing a new niche in terms of attacks on the integrity of information systems.

Remote jobs and the use of a single device for both professional and personal activity are the factors that led to the emergence of new security breaches. Also, working from home has meant connecting to a less secure internet network than the secure network at your place of business, where network integrity is ensured and managed by a network administrator.

At the institutional level, a number of factors such as the poor management of funds for IT infrastructure, or lack of interest in ensuring the integrity of IT infrastructure, have led to situations in which IT incidents have caused the most significant damage. In most cases, cyber attacks have highlighted the existence of reactive behavior, complemented by the lack of technical security measures to ensure the protection of the IT infrastructure and data used and stored on insecure devices.

There are also many situations in which a number of cyber attacks, such as *Ransomware* attacks, have caused material damage and loss of data, lack of computer security measures and lack of training of staff in the use of IT infrastructure.

For this reason, these cyber events have generated a new attitude in the case of those who have suffered such an attack, leading them to reanalyze the way in which professional activity is managed in the virtual environment and the security of the networks used. Even today, reactive behavior in ensuring the integrity of computer systems seems to be at the forefront when it comes to preventing cyber attacks.

2. Vulnerabilities in the IT infrastructure of healthcare providers

With regard to healthcare providers, an analysis of how the IT infrastructure works raises some questions about the IT integrity of the entire system. In order to identify possible vulnerabilities and security breaches, it is important to highlight some of the responsibilities and importance of the institutions providing medical services, in terms of the activity they perform.

By way of example, we indicate the activity of the National Institute of Forensic Medicine. Among the main specific activities of special importance carried out by the institution are: examination of persons and finding of traumatic injuries as a result of assaults, examination of persons and finding of traumatic injuries as a result of road accidents, examination of persons and finding of injuries in sexual assaults, examination of persons consequences of medical malpractice (medical malpractice), forensic examination for postponing or interrupting the execution of the custodial sentence, for medical reasons, examination of persons and collection of biological samples to

determine blood alcohol level, examination of persons and collection of biological samples for toxicological examinations, sampling and preservation of biological samples and criminal bodies for DNA analysis, processing of biological samples and criminal bodies for DNA analysis.¹

By extrapolation, taking into account the activity of the institute and its role in the judiciary, we can identify a potential interest of hackers in penetrating the computer system of the institution. The classic way of influencing the results of an expertise can today have a form adapted to the easy context through which a hacker can intervene in this process by simply accessing the computer systems of the institute to produce the desired effects. Moreover, the existence of this mode of action removed the difficult method of classical corruption which involves direct or indirect access to the staff of the institution. Thus, through *phishing* attacks, attackers can penetrate the computer system of the institute, either to encrypt reports with toxicological values or reports containing medical conclusions, or even to modify the values or conclusions of some expertises, in order to favor the person subject to a judicial investigation.

An organizational analysis of the system procedures for each healthcare provider is a strictly necessary step and is, in fact, a first step in identifying the main vulnerabilities and aims to identify appropriate solutions and measures to combat cyber attacks, or to recover information following such an attack.

The parallel use of personal devices or personal correspondence or social media accounts in connection with the institution's computer systems is a vulnerability in any institution. Awareness of the situation of each health care provider, in relation to the activity they provide, is a starting point in achieving the goal of computer security, and the legal analysis of security breaches creates the possibility for them to take protective measures are required.

Reviewing relevant cyber incidents in the medical field is a way to raise awareness of the scale and repercussions that a cyber attack can have at the institutional level.

3. Relevant cyber incidents on medical information systems

In 2021, the ENISA - European Cybersecurity Agency reports on the state of cyber threats for the period 2019-2020 showed that the most targeted sectors from the perspective of cyber attacks were digital services, government institutions, technology industry, financial sector and healthcare services.²

¹ <https://www.inml-mm.ro/>, accessed on 24.02.2022.

² ENISA, *ENISA Threat Report. Major incidents in the EU and worldwide*, from <https://www.enisa.europa.eu/publications/report-files/ETL-translations/en/etl2020-incidents-ebook-en-en.pdf>, accessed on 24.02. 2022.

Another extremely relevant aspect in this respect, which reflects, on the one hand, a growing trend, but not a novelty, is the fact that the basis of these attacks is social engineering in the proportion of 84% according to the report.³ In terms of penetration techniques, one of the most widely used technical methods of attacking and delivering malicious content is still phishing, and the most relevant finding is that 71% of the organizations that were attacked by cybercriminals were victims of spread attacks from one employee to another.⁴

Also, this reference period, influenced of course by the pandemic period, exacerbated the occurrence of multiple and various cyber incidents, in increasingly diverse fields, which aimed at obtaining either strategic information or personal data, financial data, but also blocking activities of some institutions of public interest, among which was found the medical system.⁵

Regarding the national cyberspace, in 2019 a series of computer attacks were registered targeting various health institutions. The involvement of the protection and defense institutions against cyber attacks made the difference in terms of restarting the activity of these institutions, or the protection of the data managed by them. Some of these cases involved hospitals, such as Clinical Hospital no. 1 Witting in Bucharest, where the attackers managed to encrypt the data and request a ransom. Although the institution's computer systems were encrypted, the hospital's work continued with the use of offline registers. Similar to this attack, also during 2019, the "Phobos" virus targeted other medical institutions that lacked antivirus protection of the IT infrastructure.⁶

Although these recent attacks are not new, employees' computer behavior still reflects a lack of a culture of computer security. The effects of this negligent behavior were most severely felt in 2017, when one of the most notorious and prolific computer attacks on a medical system took place, when a significant number of computers in more than 150 countries were targeted by ransomware "Wanacry".⁷

Among the infected computers were those of FedEx in the United States, the Deutsche Bahn in Germany, and the computer systems of the NHS state medical system in the United Kingdom.

³ *Idem.*

⁴ *Ibidem.*

⁵ *Ibidem.*

⁶ SRI, „*Atac ransomware asupra Spitalului Clinic Witting din București*” [„Ransomware attack on the Clinical Witting Hospital in Bucharest”], 30.07.2021, from <https://www.sri.ro/articole/atac-ransomware-asupra-Spitalului-Clinic-Witting-din-Bucuresti.html>, accessed on 24.02.2022.

⁷ National Audit Office, „*Investigation: WannaCry cyber attack and the NHS*”, from <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>, accessed on 24.02.2022.

In terms of malicious behavior, “Wanacry” is a ransomware virus that, once it manages to enter the victim's computer, usually via e-mail, encrypts all identified files and restricts access until the victim attack pays a ransom to regain access to these files, or to reinstall the operating system, a technical process that leads to the loss of all files held up to that point.⁸

As in the case of medical pathologies, computer viruses have also evolved, with new, more efficient and dangerous variants being identified on the black market of computer viruses. Compared to the initial variants of the ransomware class virus, the current variants are able to execute the infection of the computer systems by more and more sophisticated methods and more and more difficult to detect and fight. Currently, modern variants are built to penetrate the victim's computer system, to block the use of the keyboard and cursor, which leads to the victim's inability to take control of their own computer system. Once the files are encrypted, the virus is built to erase all technical data from the access logs of the infected computer system, highly relevant data that is an electronic record of activity on a particular device, site, or network in which they are recorded, all IP addresses that connect to a computer system.

Finally, the balance of the attack on the British NHS health system revealed a number of vulnerabilities. On the one hand, from a technical point of view, the vulnerability was reduced to the existence of a computer network composed of outdated computers, which worked with old operating systems, such as Windows XP - an obsolete operating system since 2014, and on the other hand, from a human point of view, the vulnerability has been the existence of untrained medical staff in terms of computer security culture. Following the attack, the encryption of the computer network and the computers of the British health system, forced the relocation of a significant number of patients from hospitals, as well as the discharge or postponement of operations. Employees were forced to return to the classic method of sorting patients, moving back to paper. Moreover, in some hospitals, many medical equipments have been taken out of use by the attackers, among these devices being refrigerators for storing blood or other biological materials.

Subsequent analysis of the attack revealed that a combination of human and technical factors contributed exponentially to the effects of this large-scale computer incident. Given the way in which the virus managed to infect the NHS computer system, it was found that a number of human errors in the management of e-mail were the basis for the infection and spread of the virus in the system. This was complemented by a technical system unprepared to deal with a virus.

⁸ *Idem.*

Returning to the Romanian cyberspace and the cyber attack campaigns identified in 2019 and 2020 by CERT-RO and SRI specialists, it was observed that this intensification of phishing attacks on medical institutions in Romania was not limited to central level institutions such as Ministry of Health, but also targeted the Public Health Directorates at the county level and county hospitals. In view of the increasing number of e-mails with malicious attachments apparently necessary for the day-to-day running of hospitals, a reaction has been generated from CERT-RO to prevent a major blockage in hospital activity during this extremely difficult pandemic period.⁹

It was this report from CERT-RO that highlighted a security breach similar to that encountered in the case of the computer system used by the UK national healthcare system. The same combination of technical and human factors is found in the case of internet and technology users in Romania, and the cultivation of a unitary system for protection and use of IT&C infrastructures is the starting point in achieving the goal of computer security.

4. Violation of personal data security - legal framework regarding liability

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC¹⁰ (General Data Protection Regulation-GDPR) sets out obligations for healthcare providers in terms of individuals, patients, employees, etc. Data protection is subsumed by the concept of privacy protection provided by art. 8 of the ECHR Convention¹¹, aspect that results from the doctrine (Apan R. D., 2021 and Ploșteanu N. D., Lăcătuș V., Fărcaș S., 2018).

⁹ National Directorate of Cyber Security, „*Informare referitoare la vulnerabilități și atacuri cibernetice privind spitale și clinici din România*” [„*Information on vulnerabilities and cyber attacks on hospitals and clinics in Romania*”], from <https://dnsc.ro/vezi/document/prezentare-sesiune-online-spitale-octombrie-2020>, accessed on 22.02.2022.

¹⁰ To be seen <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679>; hereinafter referred to as GDPR. The explanation of the Regulation can be consulted online at <https://www.itprotection.ro/page7.html>https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_ro, accessed on 24.02.2022; see also *Regulamentul general privind protecția datelor [General Regulation on Data Protection]*, 2018, Ed. Universul juridic, <https://www.itprotection.ro/page7.html> https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_ro, accessed on 24.02.2022.

¹¹ ECHR Convention accessible online at https://www.echr.coe.int/Documents/Guide_Art_8_ROM.pdf, accessed on 24.02.2022.

One of the constant challenges of the current period is considered the implementation of GDPR, a goal for which, at national level, Law no. 190/2018 on measures for the implementation of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing the Directive 95/46 / EC.¹²

A constant challenge in medical units is to avoid security breaches, developed in the doctrine (Opre A.G., Șandru S., 2018(1); Opre A.G., Șandru S., 2018(2)). The definition of personal data breach is given to the provisions of art. 4 of the GDPR and means that breach of security which leads, accidentally or unlawfully, to the *unauthorized destruction, loss, alteration, or disclosure of personal data transmitted*, stored or otherwise processed, or to unauthorized access to such data.

Concern for the security of personal data lies in the principles regarding the processing of personal data, as it results from the doctrine (Feldihan D., 2020), enunciated in art. 5 of the GDPR which requires: - legal, fair and transparent processing of the data subject - legality, fairness and transparency; -collection for specific, explicit and legitimate purposes and not further processing in a manner incompatible with these purposes; - keeping in a form which allows the identification of the data subjects for a period not exceeding the period necessary to fulfill the purposes for which the data are processed; -processing in a manner that ensures *adequate security* of personal data, including *protection against unauthorized or unlawful processing* and against accidental loss, destruction or damage, by taking appropriate technical or organizational measures.

We note that in art. 5, para. (1), point (f) provides for the processing of personal data in such a way as to ensure *adequate security* of the data. Moreover, we note that, in accordance with art. 5, para. (2), the responsibility of the operator is provided, including for the security of the processing. Therefore, the operator and the person empowered by it have the obligation to implement, as it results from art. 32, of the GDPR *appropriate technical and organizational measures*, a regulated obligation to remove the risks of data security breaches.

The operator and the person empowered by it shall implement appropriate technical and organizational measures *to ensure a level of security appropriate to this risk*, including, *inter alia*, as appropriate, in accordance with the provisions of art. 32, paragraph (1) of the GDPR: pseudonymization and encryption of personal data; the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and

¹² Published in the Official Monitor, Part I, no. 651 on July 26th, 2018, in force on July 31st, 2018, hereinafter referred to as Law 190/2018.

services; the ability to restore the availability of and access to personal data in a timely manner in the event of a physical or technical incident; a process for periodic testing, evaluation and assessment of the effectiveness of technical and organizational measures to ensure the security of processing.

Consequently, the first obligation of the controller and the person empowered by it under the GDPR is to ensure adequate data security, an obligation in conjunction with that of taking appropriate technical and organizational measures to maintain security, otherwise subject to sanctions, as the doctrine holds (Suca C., 2019).

Another obligation of the operator is to assess the appropriate level of security, an obligation in which the operator is responsible for carrying out the assessment and takes into account in particular the risks posed by processing, accidentally or illegally generated, destruction, loss, modification, disclosure, authorized or unauthorized access to personal data transmitted, stored or otherwise processed (Țilimpea A., 2021).

So far, we have identified as steps of responsibility of the operator and the person empowered to comply with the security of processing and the implementation of appropriate technical and organizational measures to eliminate the risks of data security breaches.

A third stage of responsibility of the operator is the one regarding the natural persons acting under the authority of the operator, stage provided by art. 32, para. (4), in the sense that the controller and the person authorized by him shall take measures to ensure that *any natural person acting under their authority and having access to personal data only processes them at their request*.

Considering the seriousness of the consequences of the personal data breach, as a security breach, the situation attracts the obligation for the operator to notify the supervisory authority, in accordance with the provisions of art. 33 of the GDPR. The notification of the competent supervisory authority shall be made pursuant to art. 55, without undue delay and, if possible, within a maximum of 72 hours from the date on which he became aware of it, unless it is unlikely to pose a risk to the rights and freedoms of individuals. If the notification to the supervisory authority does not take place within 72 hours, it shall be accompanied by a reasoned explanation for the delay.

The data controller shall also notify the controller without undue delay after becoming aware of a breach of the security of personal data concerning his activity. The notification of the authority is made by using the standard form issued by the authority¹³ itself, which will include at least:

¹³ Decision no. 128 of 22nd June 2018 of the National Authority for the Supervision of Personal Data Processing on the approval of the standard form of notification of personal data breach in accordance with Regulation (EU)2016/679 on the protection of individuals with

- describe the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned, as well as the categories and approximate number of personal data records concerned;
- communicate the name and contact details of the data protection officer or other contact point where more information can be obtained;
- describes the likely consequences of a personal data breach;
- describe the measures taken or proposed to be taken by the controller to remedy the breach of the security of personal data, including, where appropriate, measures to mitigate any possible adverse effects.

The operator is also obliged to keep documents relating to all cases of breach of security of personal data, in order to prove that he has fulfilled his obligations in accordance with the steps of responsibility indicated *ut supra*. These documents shall include a description of the factual breach of the security of personal data, its effects and the remedial measures taken.

Another obligation of the operator, if the security breach has taken place, is to inform the data subject about the security breach of personal data, according to the provisions of art. 34 of the GDPR, if the violation is likely to pose a high risk to the rights and freedoms of the individual, information that is made without undue delay. Exceptionally, the information of the data subject is not required if any of the following conditions are met:

- the operator has implemented adequate technical and organizational protection measures, and these measures have been applied to personal data affected by personal data breach, in particular measures to ensure that personal data become unintelligible to any person is authorized to access them, such as encryption.
- the operator has taken further steps to ensure that the high risk to the rights and freedoms of data subjects is no longer likely to materialize.

If the supervisory authority is notified, if the controller has not already communicated the personal data breach to the data subject, if it considers the likelihood that the breach of personal data security would pose a high risk, it may inform the data subject or may decide that any of the conditions mentioned in the previous paragraph are met.

Conclusions

On cybersecurity, doctrine (Mihai I. C., Ciuchi C., Petrică G. M, 2018) retains the following relevant guidelines:

- (i) “The European Union's Cyber Security Strategy 2016-2020 and the adopted national strategies reflect the *need for a unified approach to cybersecurity*, the need for collaboration / dissemination and the continuous updating of policies and mechanisms to ensure the security of the European cyberspace.”;
- (ii) “Numerous cyber security incidents and the recent evolution of cyber attacks have necessitated the adoption of cybersecurity policies and strategies at the international level. These strategies emphasize the need to *develop country-specific capabilities to counter cyber attacks* and establish a general framework for action and cooperation to limit their effects.”

In conclusion, the concern for this field, the same doctrine, note that it is justified because, “According to CERT-RO’s annual reports, Romania is not only a country generating cyber security incidents or a transit role for external attackers, outside the national space, but has also become a target in recent years. APT, DDoS or ransomware cyber attacks.”

Although, the above examples of security breaches concern the work of medical service providers - hospitals, both nationally and abroad, it is extremely important that these examples represent a landmark and a warning signal to all government institutions and especially in the case of healthcare providers. In the case of these institutions, the lack of major cyber events does not indicate a lack of interest from cyber attackers. The lack of a unitary IT infrastructure management system, the lack of basic knowledge in the use of IT systems, the lack of a data back-up system and a system of control and verification in the use of infrastructure are key factors in ensuring a continuous, efficient activity. and fair to provide high quality services.

In relation to those analyzed in this article, our proposal is to strengthen the advisory activities in the field of GDPR and to apply protection measures against computer fraud ordered by consultants. We also remind you that the obligation to hire consultants and to order the application of the measures proposed by them rests with the manager of the unit providing medical services.

The lack of measures in the field, within the unit providing health services can cause its damage, as well as to the patients and attract the responsibility of the manager. For these reasons, this article has a practical

purpose, being an alarm signal regarding the legal aspects that include obligations and related responsibilities.

(Points 1 and 2 were drafted by PhD Perju Dumbravă Dan, point 3 was drafted by PhD Bora Fineas, point 4 was written by Phd Apan Rodica Diana)

Bibliography

1. Apan R.D., *Personal Data Protection in Health: A Perspective of the European Court of Human Rights* JOLPA 2/2021, available online at https://sjea-dj.spiruharet.ro/images/secretariat/sjdea-2016/JoLPA_V7_I_13_2021.pdf.
2. Feldihan D., *GDPR este sistemul medical din România pregătit* [GDPR is the prepared medical system in Romania], Romanian Magazine for the protection and security of personal data 1/2020, p. 138 -141.
3. Mihai I.C. (coordonator), Ciuchi C., Petrică G.M., *Provocări actuale în domeniul securității cibernetice – impact și contribuția României în domeniu* [Current challenges in the field of cyber security - impact and contribution of Romania in the field], article available online at http://ier.gov.ro/wp-content/uploads/2018/10/SPOS-2017_Studiul_4_FINAL.pdf.
4. Opre A.G., Șandru S.; 2018; *The legal regime of the processing of personal data in the public sector, in the context of the general data protection regulation*, Revista Fiat Iustitia, p 224-235, vol. 12, nr. 1/2018, <http://fiatiustitia.ro/wp-content/uploads/2021/03/359-Article-Text-698-1-10-20180517.pdf>.
5. Opre A.G., Șandru S.; 2018, *Transparency, an essential element of the right to personal data protection*, Revista Fiat Iustitia, p 127-135, vol. 8, nr. 1/2014 <http://fiatiustitia.ro/wp-content/uploads/2021/03/162-Article-Text-305-1-10-20150302.pdf>.
6. Ploșteanu N.D., Lăcătuș V., Fărcaș S., 2018, *Protecția datelor cu caracter personal și viața privată. Jurisprudența CEDO și CJUE* [Protection of personal data and privacy. ECHR and CJEU case law], ed. Universul Juridic.
7. Suca C., *Cele mai grave 10 încălcări ale GDPR, în 2019, au presupus sancțiuni de peste 400 de milioane de euro* [The 10 worst violations of the GDPR, in 2019, involved sanctions of over 400 million euros], article available online at <https://www.lasig.ro/Cele-mai-grave-10-incalcari-ale-GDPR-in-2019-au-presupus-sanctiuni-de-pest-400-de-milioane-de-euro-articol-3,117-62379.htm>.
8. Țilimpea A., *În 2021 breșele de securitate au devenit mai greu de rezolvat și depistat: de ce să-ți faci griji* [In 2021 security breaches have become more difficult to solve and detect: why worry], article available online at <https://playtech.ro/2021/in-2021-bresele-de-securitate-au-devenit-mai-greu-de-rezolvat-si-depistat-de-ce-sa-ti-faci-grji/>.

Cytography

9. A Preliminary FTC Staff Report on Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers, article available online at <https://www.ftc.gov/reports/preliminary-ftc-staff-report-protecting-consumer-privacy-era-rapid-change-proposed-framework>.

10. ENISA, ENISA Threat Report. Principalele incidente din UE și din întreaga lume [Major incidents in the EU and around the world], article available online at <https://www.enisa.europa.eu/publications/report-files/ETL-translations/ro/etl2020-incidents-ebook-en-ro.pdf>.
11. ENISA, ENISA Threat Report. Ransomware (programele de șantaj digital) [Ransomware (digital blackmail programs)], article available online at <https://www.enisa.europa.eu/publications/report-files/ETL-translations/ro/etl2020-ransomware-ebook-en-ro.pdf>.
12. SRI, Atac ransomware asupra Spitalului Clinic Witting din București [Ransomware attack on the Witting Clinical Hospital in Bucharest], published on 30.07.2021, available online at <https://www.sri.ro/articole/atac-ransomware-asupra-Spitalului-Clinic-Witting-din-Bucuresti.html>.
13. National Audit Office, Investigation: WannaCry cyber attack and the NHS, available online at <https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf>.
14. National Directorate of Cyber Security, Informare referitoare la vulnerabilități și atacuri cibernetice privind spitale și clinici din România [Information on vulnerabilities and cyber attacks on hospitals and clinics in Romania], available online at <https://dnsc.ro/vezi/document/prezentare-sesiune-online-spitale-octombrie-2020>.
15. ECHR Convention, accessible online at https://www.echr.coe.int/Documents/Guide_Art_8_ROM.pdf.
16. <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX%3A32016R0679>.
17. <https://www.itprotection.ro/page7.html>.
18. https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_ro.
19. GDPR. Protecția datelor cu caracter personal. Regulamentul general privind protecția datelor [GDPR. Protection of personal data. General Data Protection Regulation], 2018, Ed. Universul juridic, available online at <https://www.itprotection.ro/page7.html> https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-does-general-data-protection-regulation-gdpr-govern_ro.
20. WORKING GROUP “ARTICLE 29” DATA PROTECTION, Orientări privind notificarea încălcării securității datelor cu caracter personal în temeiul Regulamentului 2016/679 [Guidelines on the notification of personal data breaches under Regulation 2016/679], 18/RO WP250rev.01, 2018, available online at <https://www.dataprotection.ro/servlet/ViewDocument?id=1603>.
21. <https://www.inml-mm.ro/>.

Legislation

22. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, accessible online at <https://eur-lex.europa.eu/legal-content/RO/LSU/?uri=celex%3A32016R0679>, consulted on 24.02.2022.
23. Directive 95/46/EC (General Data Protection Regulation), available online at <https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=celex%3A31995L0046>, consulted on 24.02.2022.
24. Decision no. 161 of October 9, 2018 of the National Authority for the Supervision of Personal Data Processing regarding the approval of the Procedure for conducting

investigations, accessible online at <https://legislatie.just.ro/Public/DetaliiDocument/206155>.

25. Decision no. 128 of 22 June 2018 of the National Authority for the Supervision of Personal Data Processing on the approval of the standard form of notification of personal data breach in accordance with Regulation (EU) 2016/679 on the protection of individuals with regard to data processing personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation), available online at <https://legislatie.just.ro/Public/DetaliiDocument/202190>.