PERSONAL DATA PROTECTION: CHALLENGES OF THE COVID-19 PANDEMIC

Predrag Stolic[1], Zoran Stevic[1], Misa Stevic[2], Ilija Radovanovic[3], Milan Radivojevic[4], Sanja Petronic[5]

[1]Technical faculty Bor – University of Belgrade [2]Elsys, Belgrade;
[3]Innovation center of School of Electrical Engineering in Belgrade;
[4]Mining and Metallurgy Institute Bor;
[5]Innovation Centre of Faculty of Mechanical Engineering in Belgrade
Serbia
pstolic@tfbor.bg.ac.rs

The paper presents the effect of the coronavirus pandemic on the segment of personal data protection. In recent years, many mechanisms related to the application of personal data protection have been developed and adequate legal regulations have been obtained worldwide. Certain difficulties are encountered in the application of legislation related to personal data protection when personal data protection is attempted to be applied in a pandemic. The authors give some examples of mentioned issues based on the existing legislation of the Republic of Serbia, but certain conclusions can be universally applied to other countries where there is a legal aspect of personal data protection.

Keywords: COVID-19, data exchange square, pandemic, personal data protection, public health.

1. Introduction

The digital transition and digital transformation have expanded the scope of data that is being processed today, as well as the ways in which this data is processed and the obtained information is generated. In the period defined as The Zetabyte Era [1], which best describes the volume of data that has been in circulation globally in recent years, it is expected that two thirds of the total data will be generated by individuals [2]. Accordingly, several years ago, one of the primary focuses was on the protection of personal data, defining appropriate mechanisms for personal data protection and their introduction into appropriate legal flows at the local, regional and global levels.

Although many global companies have recognized the importance of personal data protection and adopted a certain set of rules for handling personal data earlier, only the adoption of the legal framework enabled a unique set of rules and a certain degree of protection for data controllers and processors on one hand and for individuals on the other. In this sense, one of the key moments is certainly the adoption of Regulation No. 2016/679 of the European Union [3] in April 2016, better known as the GDPR (General Data Protection Regulation), which had a strong implication not only for European Union member states but also for other European countries. The application of the mentioned Regulation on the territory of the European Union began two years after its adoption, at the end of May 2018. As already mentioned, the application of the GDPR has implications beyond the borders of the European Union. In the Republic of Serbia, the Law on Personal Data Protection, which largely relies on the mentioned GDPR and copies very large number of its articles was adopted in November 2018 and came into effect nine months later, at the end of August 2019.

As can be seen, these documents have a relatively short application period, about 2 years on average, and the context of implementation has already been placed in extraordinary circumstances. In early 2020, the world faced a global pandemic situation caused by the emergence of a new coronavirus disease (COVID-19) [5]. The global pandemic did not subside in 2020 and is showing the same tendency in 2021, bringing new challenges to the whole world. These challenges are primarily reflected in the adequate responses of health systems to the preservation of public health and life in very difficult pandemic conditions. Also, the new

challenges are facing the world economy, industry, education system and every aspect of modern human society that must get used to living in the new pandemic reality. The aspect of personal data protection is also not immune to these aggravating circumstances and challenges. The great consequences of the pandemic are felt in this domain as well.

Legal documents define some special categories of data (Article 6 in EU GDPR): personal data revealing racial or ethnic origin, political opinions, religious and philosophical beliefs; genetic and biometric data uniquely identifying a person; data related to person's sex life or sexual orientation and health. Processing of these data is forbidden, except in some special cases, for example when the processing is necessary for the purposes of preventive or occupational medicine, to assess the working capacity of employees, for medical diagnostics of health services and the like. Another example is when data processing is necessary for reasons of public interest in the area of public health, such as protection from serious cross-border threats to public health or ensuring high standards of quality and safety of health care and the like [3, 4].

In a pandemic, the use of health data and the mentioned special cases of data processing become dominant. However, although legally defined, the current situation introduces many uncertainties into the field of personal data protection. Some of these potential dilemmas are presented in the following paragraphs.

2. "Data Exchange Square" problem

The first potential issue related to the personal data protection during COVID-19 pandemic the authors named the Data Exchange Square problem (Fig. 1).

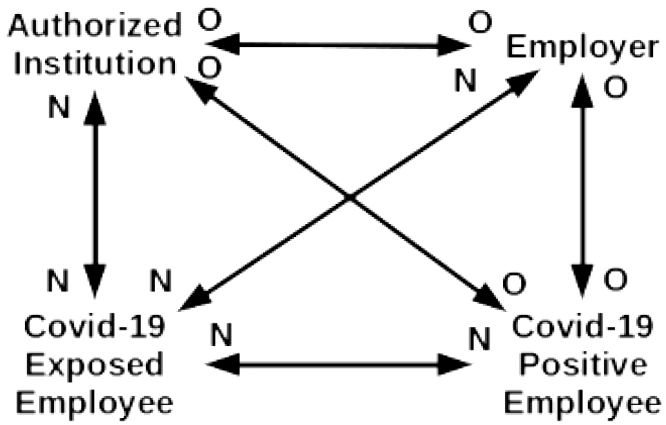

Fig. 1. Schematic representation of Data Exchange Square

Fig. 1 shows the data flows (information flows) among the relevant actors in the process of informing about the appearance of an infected person within one working team. Covid-19 Positive Employee (CPE) represents the infected person and Covid-19 Exposed Employee (CEE) represents the person which has some appropriate contact with the infected person. Other participants in this process are the Employer who hires the mentioned CPE and CEE, as well as the appropriate Authorized Institution (AI). In this case, the Authorized Institution has multiple roles. It can be an appropriate medical institution or an institute for the protection of public health, but it may also be a municipal, regional or state crisis headquarters, as well as a local, regional or state authority with appropriate authorization. The letter O represents obligation of processing personal data, mostly health data, and the letter N indicates that there is no such obligation.

If we analyze the first triangle with Employer, CPE and AI at its vertices, we can see that the data flow connecting these vertices are labeled O (obligation) for all parties and that there are no particular doubts about those flows. CPE must inform Employer about COVID-19 results since he is unable to fulfill his work obligations. AI must inform CPE about positive COVID-19 results and also must inform Employer about the status of the CPE because in this case the sick leave is opened automatically and the employer is

automatically sent a confirmation of employee's temporary incapacity for work. Thus we have one balanced structure of processing personal data.

In the second triangle with CPE, CEE and AI at the vertices, the data flows are mostly non-obligatory. CPE has no legal obligation to inform about positive COVID-19 results any person with whom he had been in contact recently although that person (CEE) becomes potentially exposed to the virus. Also, if it has knowledge of a person's exposure to the virus, the AI must not inform that person (CEE) about the potential risk, as well as the conditions that led to that risk because it would have to reveal some personal data that can easily be put in the right context and identify CPE. So in this case we have an unbalanced structure of personal data processing.

Similar to the previous one, in the third triangle with Employer, AI and CEE at the vertices, the data flows are again mostly non-obligatory. Relations AI—CEE and AI—Employer have already been considered, which brings us to the remaining relation between Employer and CEE. Despite the fact that the employer has relevant information about CPE's positive coronavirus test, as well as about the fact that CPE and CEE were in direct contact at a critical time, he must not disclose any information about the exposure to CEE because the data is entrusted to him for processing as health data, which is a special category of data. Again, this structure of personal data processing is unbalanced.

The fourth triangle with Employer, CPE and CEE at the vertices is a similar case. Here, too, the data flow is mostly non-obligatory. We have already considered all three relations (Employer—CPE, Employer—CEE and CPE—CEE) and can conclude that in this case we have an unbalanced structure of personal data processing.

Only one triangle presents a balanced structure of personal data processing, while the remaining three do not. This makes the whole square behave as an unbalanced personal data processing structure.

3. Two possible solutions

If we look at three "unbalanced" triangles, we find that all three triangles have the common characteristic: all three have CEE located in one of their vertices. This practically means that CEE cannot in any way obtain timely and accurate information on the potential risk within the existing legal framework. If we now look at CEE not as one person, but as a potentially large group of people who share the common characteristic, i.e. that within a certain time interval they came into contact with CPE and thus potentially became exposed to the virus, then we can say that the problem of CEE ignorance is no longer a partial problem. It becomes serious threat to public health. Without timely information, employees tend to behave as usual, which means that employees, thinking that they are not at any particular risk, will intensify their contacts with others instead of minimizing them. This leads to the danger that this will become another growth factor of the pandemic curve.

Employers have an obligation to inform employees of any health and safety hazards [6], but in this case the consistent application of personal data protection rules greatly limits this obligation, and, as can be seen from the said above, can disable the fulfillment of this obligation in a pandemic.

In order to avoid the previously mentioned side effects, and in terms of more efficient response during the pandemic, there are two possible ways to overcome the problems.

First possible solutions is to exclude health data from the special categories of data during the pandemic and given it a privileged status. Accordingly, the regulations that prohibit processing health data must be much softer during a pandemic. In pandemic conditions, data processing related to health data should not be limited to special processing cases, but current special processing cases should be permanent and implemented in a much broader sense to provide accurate, adequate, meaningful and timely information in the fight against the pandemic. Of course, this does not mean that absolutely all health data should be processed. On the contrary, it is necessary to allow processing only the health data that could contribute to stopping the spread of the pandemic. This process could be regulated through adequate temporary registers of data allowed for processing, which could change after gaining new knowledge about the virus. In this way we would have a solution that could meet some strict conditions in terms of preventing privacy breaches or potential misuse of personal data which nowadays are some of the leading concerns about health data processing [7].

Second solution is more extreme and implies the suspension of certain articles of the law during the pandemic situation in order to speed up the processing of health data as one of the crucial instruments in the fight against the pandemic. The use of this solution is not recommended and should only be used as a last resort, or when all other means in the fight against the pandemic have been exhausted. If such an answer to the aspect of personal data protection in pandemic conditions should be resorted to, then additional efforts would certainly have to be made in order to minimize the risks of personal data breaches (unallowed alterations, unauthorized disclosures, unauthorized accesses etc.) [8] in the mentioned conditions.

4. Conclusion

In this paper, some specific problems and doubts as to the application of personal data protection in pandemic were pointed out. These issues arose during the fight against the COVID-19 pandemic as the world absolutely did not expect large-scale pandemics and was not adequately prepared for them. Also, as far as the personal data protection is concerned, these are very "young" laws, so it is to be expected that in the following years adequate analyses of their implementation can be performed, especially those related to pandemic conditions.

At the moment, the maneuverability related to personal data protection is quite limited. However, it should be kept in mind that certain annexes will have to be adopted as a matter of urgency regarding the use of medical data if the pandemic does not end soon. Finally, we should always be guided by the fact that human life has the greatest value, even if it implies a certain loss of comfort and security regarding the protection of personal data.

REFERENCES

1. Barnett T. *The Zettabyte Era Officialy Begins*, Cisco, 2016, https://blogs.cisco.com/sp/the-zettabyte-era-officially-begins-how-much-is-that (access date: 14.03.2021).

2. Deloitte, *The Data Landscape*, Deloitte LLP (2017), London, UK

3. *EU General Data Protection Regulation (GDPR):* Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

4. *Law on Personal Data Protection,* Službeni glasnik Republike Srbije No. 87/18, Službeni glasnik, 2018, Belgrade, Republic of Serbia.

5. *A year without precedent: WHO's COVID-19 response,* World Health Organization (2020), Available at https://www.who.int/news-room/spotlight/a-year- without-precedent-who-s-covid-19-response (access date:14.03.2021)

6. *Privacy and Data Protection in the age of COVID-19*, Deloitte Belgium, 2020. https://www2.deloitte.com/be/en/pages/risk/articles/privacy-and-data-protection-in-the-age-of-covid-19.html (access date: 14.03.2021)

7. Ahmad N., Chauhan P. State of Data Privacy During COVID-19. *Computer*, 2020, vol. 53, no. 10, pp. 119-122. https://doi.org/10.1109/MC.2020.3010549

8. Ventrella E. Privacy in emergency circumstances: data protection and the COVID-19 pandemic, *ERA Forum* 2021, pp. 379–393. https://doi.org/10.1007/s12027-020-00629-3

П. Столич, З. Стевич, М. Стевич, И. Радованович, М. Радивоєвич, С. Петронич

Захист персональних даних: виклики пандемії COVID-19

Розглянуто вплив коронавірусу на сегмент захисту персональних даних. За останні роки було розроблено багато механізмів захисту персональних даних, і в усьому світі було прийнято відповідні правові норми. Певні труднощі виникають при застосуванні законодавства щодо захисту персональних даних в умовах пандемії. У роботі наводяться деякі приклади згаданих проблем на основі чинного законодавства Республіки Сербія, але певні висновки можуть бути застосованими і для інших країнах, де існує правовий аспект захисту персональних даних.

Ключові слова: COVID-19, квадрат обміну даними, пандемія, захист персональних даних, громадське здоров'я.