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, Bor,
pstolic@tfbor.bg.ac.rs

The paper presents the implication of the the appearance of coronavirus 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 completely applied in the pandemic circumstances. In this paper some examples of mentioned issues are given 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 has expanded the scope of data that are processed today as well as the way in which these data are 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 generated 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 level.

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 is addopted in November 2018. The application of the mentioned Law on the territory of the Republic of Serbia began nine months after its adoption, at the end of August 2019.

As can be seen, this is a relatively short period of application of these documents, on average about 2 years, 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 situation is not calming down throughout 2020, and it shows the same tendency in 2021 and brings 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 the application of personal data protection is also not immune to these aggravating circumstances and challenges. The great consequences that the pandemic situation brings with it are also felt in this domain.

Legal documents define some special categories of data (Article 6 in EU GDPR): personal data that revealing racial or ethnic origin, data that express political opinions, religious and philosophical beliefs, genetic and biometric data with purpose of uniqely identifying a person, data related to person's sex life or sexual orientation and health data. The processing of these data are forbidden, except in some special cases which are among others are necessary processing for the purpose of preventive medicine or occupational medicine, to assess the working capacity of employees, medical diagnostics of health services and the like, or necessary processing in order to achieve public interest in public health, such as protection from serious cross-border threats to public health or high standards of quality and safety of health care and the like [3,4].

In pandemic conditions, the use of health data and the mentioned special cases of processing is becoming dominant, however, although legally defined, it brings many unknowns with which the protection of personal data is faced with the use in the newly created real conditions. Some of these potential dilemmas are presented in the following lines.

2. "Data Exchange Square" problem

First potential issue related to use of personal data protection during COVID-19 pandemic authors named as Data Exchange Square problem which is illustrated in Figure 1.

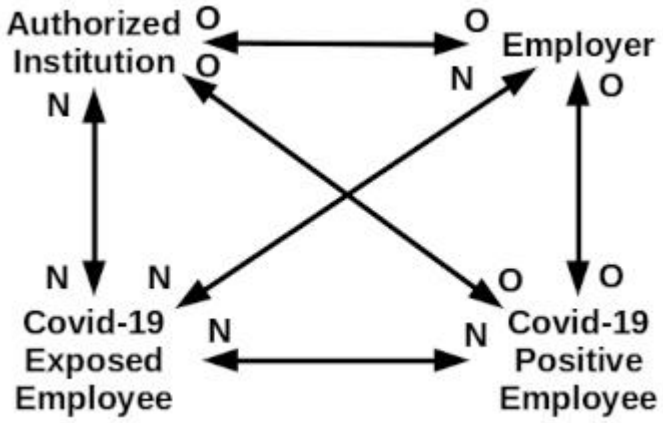

Figure 1. Schematic representation of Data Exchange Square

On the schematic representation in Figure 1, data flows (information flows) among the relevant actors in the process of informing about the occurrence of the infected person within one working collective are shown. Covid-19 Positive Employee (abbr. CPE) represented infected person and Covid-19 Exposed Employee (abbr. CEE) represented the person which has some appropriate contact with the infected person. Also as participants in this process we have an Employer who hires mentioned persons and appropriate Authorized Institution (abbr. AI). In this case Authorized Instution has a multiple role, 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 an appropriate local, regional or state authority with appropriate authorization. Letter O represents obligation of processing personal data, mostly with health data as special personal data category and letter N indicates that there is no such obligation.

If the first triangle is analyzed in whose vertices it is located Employer, CPE and AI it can be seen that the flow of data (information) is with obligations for all parties and that there are no some special 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 CPE status because in this case the sick leave is opened automatically and the employer is automatically sent

a confirmation of temporary incapacity for work. Accordingly to the mentioned we have one balanced structure of processing personal data.

If the second triangle is analyzed in whose vertices it is located CPE, CEE and AI it can be seen that the flow of data (information) mostly is with no obligations. CPE has no legally 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 one unbalanced structure of personal data processing.

Similar to the previous one if the third triangle in whose vertices are Employer, AI and CEE is analyzed it can be seen that the flow of data (information) again mostly is with no obligations. Relations AI-CEE and AI-Employer have already been considered and will not be considered again which brings us to consider the remaining relation Employer-CEE. Despite the fact that the employer has relevant information about CPEs positive test for coronavirus, 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 exposure to CEE because data is entrusted to him for processing as a health data which is special category of data. Again, the structure in domain of personal data processing is unbalanced.

Similar explanation is for the analysis of the fourth triangle in whose vertices are Employer, CPE and CEE. Again, there is situation that the flow of data (information) again mostly is with no obligations. All three relations (Employer-CPE, Employer-CEE and CPE-CEE) have already been considered previosly so it can be concluded that in this case alse we have one unbalanced structure of personal data processing.

Only for one triangle is obtained balanced structure of personal data processing while for the remaining three it is not, which makes the whole square behave as unabalanced structure of personal data processing.

3. Two possible solutions

If we look at three “unbalanced” triangles we find that all three triangles have the common characteristic that CEE is located in one of the vertices. This practically means that the CEE cannot in any way obtain timely, 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 persons who share the common characteristic that in 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 in accordance with normal practice, which means that employees, thinking that they are not at any particular risk, will intensify their contacts with others instead of minimizing them, which leads to the danger that this will be even more one 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 previous, at one moment in pandemic conditions, disable fulfillment of this obligation.

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

First possible solutions is that in the pandemic situations health data be excluded from the special category of data and that health data be given a special, privileged status. Accordingly, the regulations concerning the prohibition of processing this data for their use in pandemic conditions must be much softer. 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, the processing should refer only to those health data that contribute to stopping the spread of the pandemic, and this could be regulated through adequate temporary registers of permitted data 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 missuse 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 be avoided, except when the use of this solution is 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 diclosures, unathorized accesses etc.) [8] in the mentioned conditions.

4. Conclusion

In the previous lines, some specific problems and doubts with the application of personal data protection in pandemic conditions 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 protection of personal data is concerned, these are very "young" laws, so it is to be expected that in the following years adequate analyzes of 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, it should always be guided by the fact that human life has the greatest value, even if it implies a leaving of a certain amount of comfort and security regarding the protection of personal data.

REFERENCES

1. T. Barnett, *The Zettabyte Era Officialy Begins*, Cisco (2016), Available at https://blogs.cisco.com/sp/the-zettabyte-era-officially-begins-how-much-is-that , Accessed on 14th March 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 , Accessed on 14th March 2021

6. Deloitte, *Privacy and Data Protection in the age of COVID-19*, Deloitte Belgium (2020), Belgium

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

8. E. Ventrella, *Privacy in emergency circumstances: data protection and the COVID-19 pandemic*, ERA Forum 21, 379–393 (2020). doi: 10.1007/s12027-020-00629-3

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

Дзахист персональних даних - виклики пандемії COVID-19

У статті представлено наслідки появи коронавірусу на сегменті захисту персональних даних. За останні роки було розроблено багато механізмів, пов'язаних із застосуванням захисту персональних даних, і в усьому світі отримано відповідні правові норми. Певні труднощі виникають при застосуванні законодавства, що стосується захисту персональних даних, коли намагаються повністю застосувати захист персональних даних в умовах пандемії. У цій роботі наводяться деякі приклади згаданих питань на основі чинного законодавства Республіки Сербія, але певні висновки можуть бути загальноприйнятими в інших країнах, де існує правовий аспект захисту персональних даних.

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