SZILVIA VÁRADI*

Legal challenges of processing health data in the shadow of COVID-19 in the European Union**

I. Introduction

In December 2019, the SARS-CoV-2, which is a new type of coronavirus, was reported first in Wuhan, China. Since then, the infection caused by this virus referred as COVID-19, spread throughout China and all around the world. The speciality of COVID-19 is that it is spreading rapidly, and the human body responds to it differently from no symptoms (asymptomatic) to severe pneumonia, and a severe disease can lead to death.[1] Besides, it can cause unexpected and unusual symptoms as well.

The virus has affected not only our health, but the economy and society. It has changed the forms of social contacts, and the world of work. There is a trend towards the new forms of employment and work, which involves new technologies, and employers and workers are facing in adapting to the new work-from-home environment.[2]

The balance of public safety and the fundamental right to privacy and to the protection of personal data is increasingly being challenged in the context of the fast-developing technology of the 21st century. Some experts suggest that public interest can be a higher priority than privacy issues in certain special circumstances.[3] There is no doubt that the COVID-19 pandemic situation is an extraordinary circumstance, which means enormous challenge to the states and public health risks potentially affecting the life of millions of people around the world.

---

* Senior lecturer, University of Szeged, Faculty of Law and Political Sciences Universitas Scientiarum Szegediensis

** This research was supported by the project nr. EFOP-3.6.2-16-2017-00007, titled *Aspects on the development of intelligent, sustainable and inclusive society: social, technological, innovation networks in employment and digital economy*. The project has been supported by the European Union, co-financed by the European Social Fund and the budget of Hungary.

1 European Centre for Disease Prevention and Control: Coronavirus disease 2019 (COVID-19) pandemic: increased transmission in the EU/EEA and the UK –seventh update. Stockholm, 25 March 2020. p. 1.

2 European Commission: Telework in the EU before and after the COVID-19: where we were, where we head to. Joint Research Centre. 2020. pp. 1–2.

3 BEEBE, GILBERT W.: *Long-term follow-up is a problem*. American Journal of Public Health, vol. 73, no. 3. 1983. pp. 245–246.

There is no doubt that in specific circumstances created by a pandemic, processing personal data is inevitable to introduce appropriate measures to stop the spread of the infection, and to prevent or minimise its impacts. These personal data in question can vary from the "general" types, such as name, address, workplace, other location data or travel information of data subject, which can be useful to discover, whether an individual might have visited affected areas or met with infected people. Besides, processing of special categories of personal data, such as health data (including test results, body temperature, chronic diseases, symptoms and health conditions, etc.) is essential to obtain an early indication whether an individual is infected.

In the European Union, the data protection provisions are laid down in the General Data Protection Regulation (GDPR), which entered into force after a two-year period on 25th May, 2018.[4] In this work we are focusing on the privacy impacts and questions raised by the COVID-19 virus, in the frame of data protection law of the European Union. Since the governments of the states have the enormous task to fight against the pandemic situation, we will analyse how government authorities use personal data rightfully under the provisions of the GDPR. During our investigation, we are focusing on the processing of health data, which is a special category of personal data with sensitive nature. Our aim is that to give an answer to the following question at the end of our paper: how the highest standards of privacy and data protection can still be maintained in exceptional circumstances, such as global health crisis generated by COVID-19 pandemic.

Therefore, in the following section we identify the relevant legal basis for processing health data in the event of the current COVID-19 pandemic.

II. Potential legal basis for processing of health data in COVID-19 pandemic situation

As we mentioned before, it is crucial to maintain the level of the protection guaranteed by the GDPR in each Member State during the pandemic. Therefore, data controllers must follow the basic principles contained in Article 5 of the GDPR.

One of these principles is that personal data should be processed lawfully,[5] which means the data controllers' obligation to rely on a legal basis contained in the GDPR. Regardless of the types of personal data, this requirement remains essential to guarantee the lawfulness of processing operations.

In our view, for processing "general" types of personal data (e.g, name, date of birth, contact information, etc.) the consent of the data subject[6] is not always the best option, especially in a pandemic situation. This category of personal data can be processed in accordance with Article 6 (1) d), when it is necessary *to protect the vital interest of individuals* (i.e., to save the life of the data subject), or under Article 6 (1) e) *to protect public interest* or *in the exercise of official authority* vested in the controller. Recital 46 of the

[4] 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- GDPR), OJ L 119, 4.5.2016. pp. 1–88. (hereinafter GDPR)

[5] GDPR Article 5 (1) a).

[6] GDPR Article 6 (1) a).

GDPR explicitly refers to the monitoring of epidemics and their spread as circumstances, in which the processing may serve both important grounds of public interest and the vital interest of data subjects.

In addition to the above, if the processing is necessary for compliance with *a legal obligation*, which the controller is subject to, Article 6 (1) c) also can be relied upon. According to Article 6 (3) of the GDPR, both public interest and legal obligation can only be determined by the law of the European Union or of a Member State, which the controller is subject to.

An example for the second, is the legal obligation of a given healthcare provider or a doctor in independent medical practice as a data controller. In Hungary, their legal obligation derives from Act XLVII of 1997 on the processing and protection of health care and related personal data, which contains provisions not only for the processing of health data, but for the "general" types of data as well. Personal data from the "general" category, namely the Hungarian Social Security Number (TAJ), date of birth, gender and postal code of the data subject, can be processed for the purpose of epidemiological investigations or analyses and for evaluation and improvement of the quality of health services under Article 18 of the Act.[7]

It is important to emphasize that personal data concerning health require higher protection due to their sensitive nature, and they belong to sub-categories of personal data, which are called the special categories of personal data. The processing of these kind of data is generally not allowed by the Article 9 (1) of the GDPR, unless at least one of the ten conditions of the possible exemptions under Article 9 (2) is met.[8]

At this point, the relationship between Article 6 (1) and Article 9 (2) of the GDPR should be clarified regarding the lawful basis for data processing. One of the possible options to reveal the connection between the two provisions, if we apply the *lex generalis – lex specialis* relationship to them, where Article 9 considered as *lex specialis* compared to Article 6. The consequence of this alternative is that it excludes the applicability of Article 6 as *lex generalis* in its entirety, so this way the special categories of personal data, such as health data, can be processed without satisfying Article 6.[9]

However, we share the opinion of those experts who express the view that the relationship of the two given Articles is more complex. As the original aim is to provide additional and higher level of protection for special categories of personal data, therefore, a controller processing such kinds of data may never rely solely on a legal basis under Article 9 (2) to legitimise a data processing activity. Article 6 must be applied in a *cumulative way* with Article 9 (2) to ensure that all relevant safeguards and measures are fulfilled. The appropriate legal basis laid down in Article 6 shall be applied, only if Article 9 of the

---

[7] Act XLVII of 1997 on the processing and protection of health care and related personal data. (*1997. évi XLVII. törvény az egészségügyi és a hozzájuk kapcsolódó személyes adatok kezeléséről és védelméről*) Article 18.

[8] GDPR Article 9 (2) a)- j).

[9] In its opinion, WP29 analysed a similar relationship within the former Directive 95/46/EC, comparing Article 7 containing the lawful grounds for processing personal data with Article 8 which regulated the processing of special categories of personal data. Article 29 Data Protection Working Party: Opinion 06/2014 on the "Notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC". 9 April 2014. p.14.

GDPR provides for a specific derogation from the general prohibition to process special categories of personal data.

According to the Article 9 (2) a) of the GDPR, one of the possible legal bases for processing special categories of personal data such as data concerning health is the *explicit consent* of the data subject.

Regarding the relevance of the given consent, the European Data Protection Board (EDPB) clarified its position in relation to the applicability of the GDPR for the clinical trials[10] in its opinion.[11] The EDPB has concluded that informed consent (e.g. from participants in clinical research), should not be confused with "consent" as a legal basis under the GDPR. The criterion of obtaining informed consent responds to ethical requirements of research projects involving humans deriving from the Helsinki Declaration, and its aim is to ensure the protection of the right to human dignity and the right to integrity of individuals under Article 1 and 3 of the Charter of Fundamental Rights of the EU. In this context, according to the opinion of the EDPB, it is not an instrument for data protection compliance.[12]

Article 4 (11) and Article 7 of the GDPR require freely given, specific, informed, unambiguous, and explicit consent as a valid legal basis, where data subjects needed to have a free choice and control in whether to give their "consent".[13] These are relevant provisions also when special categories of data are involved and processed, such as health data. But under the Recital 43 of the GDPR, consent cannot be regarded as a valid lawful legal basis in those cases, when there is an imbalance of power between the data subject and the controller. According to the EDPB, this is clearly an issue in the study of the critically ill, where patients might be especially vulnerable and there might be a stark imbalance of power between the investigator and patient providing the data.[14]

Besides, while conducting epidemiological investigations, researchers did not always obtain the explicit consent of the data subjects.[15]

In the light of the above, the EDPB suggested that in most cases the consent is not an appropriate legal basis for the purposes of processing data under GDPR. Instead, data controllers should seek to rely on either public or legitimate interests, and only relying on the consent of the data subject under very specific circumstances, when the consent is freely given, specific, informed, and unambiguous, and withdrawal of the consent will not adversely affect the proposed use of the data.

---

[10] Regulation (EU) No 536/2014 of the European Parliament and of the Council of 16 April 2014 on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC Text with EEA relevance OJ L 158, 27.5.2014, pp. 1–76.

[11] European Data Protection Board (hereinafter EDPB): Opinion 3/2019 concerning the Questions and Answers on the interplay between the Clinical Trials Regulation (CTR) and the General Data Protection regulation (GDPR) (art.70.1.b) Adopted on 23 January 2019.

[12] EDPB Opinion 3/2019. pp. 15–17.

[13] VÁRADI, SZILVIA: *„Hozzájárult. Vagy mégsem?" – A személyes adatok kezeléséhez történő hozzájárulás érvényességének szempontjai*. FORVM: Acta Juridica et Politica vol. 11. No. 1. 2021. pp. 163–179.

[14] EDPB Opinion 3/2019. p. 19.

[15] AHN, NA YOUNG – PARK, JUN EUN – LEE, DONG HOON – HONG, PAUL C.: *Balancing Personal Privacy and Public Safety During COVID-19: The Case of South Korea*. IEEE Access, vol. 8. 2020. pp. 171325-171333. doi: 10.1109/ACCESS.2020.3025971. p. 171325.

To decide, whether the processing of data concerning health is lawful without a valid consent, it should also be analysed in detail, if there are situations where a consent is not needed under the GDPR. The EDPB considers that depending on specific circumstances of a clinical trial, the appropriate basis for all processing operations of data with sensitive nature for purely research purposes could either be under Article 9 (2) (i) of the GDPR: "*reasons of public interest in the area of public health (...) on the basis of Member State law*", or Article 9 (2) (j) of the GDPR: "*scientific ... purposes in accordance with Article 89 (1) based on Union or Member State law*".

In the frame of the COVID-19 pandemic situation, the Member States should activate their emergency plans[16] and conduct administrative procedures or apply contact tracing, which is an effective disease control strategy that involves identifying infected persons and their contacts, then cooperating with them to interrupt disease transmission. According to our opinion, people's trust in the governments, who are adopting emergency measures to fight against COVID-19, is also an important factor.

According to Recital 52 of the GDPR, a derogation is allowed for processing special categories of personal data *on the ground of the public interest*, in particular processing personal data for health security, monitoring and alert purposes, the prevention or control of communicable diseases and other serious threats to health. The Recital 54 of the GDPR states that the processing of special categories of personal data may be necessary for reasons of public interest in the areas of public health[17] without the consent of the data subject. Suitable and specific measures should be taken when processing these type of data, to protect the rights and freedoms of natural persons and to comply with the basic principles of the GDPR, especially with the purpose limitation.[18] Based on this provision, it can be stated that the public safety requires the "right to know" about the patients' personal data regarding e.g. the status of infection.[19] This ground applies if the processing is necessary to protect the population against a serious cross-border threat to health such as COVID-19 pandemic, or ensuring high quality standards and safety of healthcare, medicinal products or medical devices.

In order to decide, which one from the above-mentioned legal grounds will be the appropriate to the specified processing, analysis has to be made on a case-by-case basis.

In the following section we will analyse the relevant legal framework related to the potential restrictive legislative measures, which serve an inevitably legal instruments for the governments of the Member States of the EU in the fight against the COVID-19.

---

[16] WHO Director-General's opening remarks at the media briefing on COVID-19, 5 March 2020. https://www.who.int/dg/speeches/detail/who-director-general-s-opening-remarks-at-the-mediabriefing-on-covid-19—5-march-2020

[17] According to the Recital 54 of the GDPR, the definition of *public health* is the following under the Regulation (EC) No 1338/2008 of the European Parliament and of the Council: "*all elements related to health, namely health status, including morbidity and disability, the determinants having an effect on that health status, health care needs, resources allocated to health care, the provision of, and universal access to, health care as well as health care expenditure and financing, and the causes of mortality*."

[18] GDPR Recital 54.

[19] Some authors share this statement especially in the context of COVID-19 pandemic situation: AHN, NA YOUNG – PARK, JUN EUN – LEE, DONG HOON – HONG, PAUL C 2020. p. 171328.

III. Restrictions in the context of the COVID-19

Privacy and the right to data protection are fundamental rights, the latter was set out in Article 8 of the Charter of Fundamental Rights of the European Union. These are not absolute rights, but they must be balanced against other fundamental rights, therefore there may be circumstances and situations, in which a data subject cannot exercise their data protection rights.

According to Article 52 (1) of the Charter of Fundamental Rights of the European Union (CFR), limitations on the exercise of the rights and freedoms recognised by the CFR may be made only, if they genuinely meet objectives of general interest recognised by the Union and complying with the requirements of necessity and proportionality at the same time.[20]

The GDPR contains new and restated rights of data subjects under the data protection law, although Recital 4 provides that data protection should always be considered in relation to its function in society, and need to be balanced against other fundamental rights. Article 23 of the GDPR prescribes provisions to permit the restrictions of these rights in specific circumstances. With a legislative measure, EU law or national laws of the Members States can restrict the scope of the rights of data subjects and some of the obligations of the data controllers, while respecting the essence of the fundamental rights and freedoms, and if it is a necessary and proportionate measure in a democratic society to safeguard "*other important objectives of general public interest of the Union or of a Member State, in particular (...) public health (...)*."[21]

Analysing Article 23 of the GDPR, it contains provisions for legislative measures, which may restrict the scope of specified and selected obligations and rights, and the legislators are in the position to adopt this type of legal document. Moreover, not only the Member States are able to impose such restrictions, but the EU is also explicitly included in the Article in question. In the case of EU law, the legislators are the institutions of the EU authorised by the founding treaties. On these grounds, we can conclude that the national or the EU legislator will fill the role of the data controller under Article 23.

It is also important to emphasize that since Article 23 contains the lawful requirements for the restrictive legislative measures, this Article also creates an obligation for data controllers which must be to fulfilled. When a Member State fails to comply with these provisions, the national law will be invalid based on the basic principle of the EU, namely the primacy of EU law. According to some of the experts, it is unclear whether the same can be applied to any failure by the EU legislator to follow these requirements when adopting other legislative act, arguing that GDPR is recognised as having special status above other legislative acts of the EU.[22] Our view is that the result of this situation is the

[20] Charter of Fundamental Rights of the European Union. Article 52 (1). OJ C 326, 26.10.2012, pp. 391–407.

[21] GDPR Article 23 1) e).

[22] MOORE, DOMINIQUE: *Article 23 Restrictions.* In: Kuner, Christopher - Bygrave, Lee A. - Docksey, Christopher – Drechsler, Laura (eds.): The EU General Data Protection Regulation (GDPR). A Commentary. Oxford University Press. Oxford. 2020. pp. 552–553.

same invalidity, infringing the fundamental rights of data subjects guaranteed under Article 8 and 53 of the CFR.

We should also mention the importance of the territorial scope of the GDPR.[23] Since it was also implemented by Iceland, Liechtenstein and Norway,[24] which are parties in the European Economic Area (EEA) Agreement and based on its Protocol 1 any reference to the territory of the Union should be understood as references to the territories of EEA countries, the GDPR is applicable for these countries as well.[25]

Moreover, it follows from Article 23 of the GDPR that restrictive legislative measures are only applicable for the limitation of the scope of data subjects' rights specified clearly by Article 23 (1) of the GDPR.[26] Besides, these rights are also related to the data controllers, because their obligation is to ensure them. It is important to underline that those rights and obligations which are not covered by Article 23 cannot be restricted.

The restrictions should be foreseeable to persons subject to them, with precisely limited in time.[27] Besides, in accordance with Article 23 of the GDPR and with the relevant case-law of the Court of Justice of the European Union (hereinafter CJEU), the derogations and limitations in relation to the protection of data must be applied, when it is strictly necessary and proportionate.[28] On these grounds, safeguarding public health in emergency state is a reasonable and legally sound reason, but only accompanied by the abovementioned conditions.

This latter was confirmed in another case of the CJEU where the Court highlighted the specific requirements set out in Article 23 (2) of the GDPR and stressed out that "*Article 23 (1) and (2) of the GDPR cannot be interpreted as being capable of conferring on Member States the power to undermine respect for private life, disregarding Article 7 of the Charter, or any of the other guarantees enshrined therein.*" [29]

Examining the required elements of a restrictive legislative measure under Article 23 (2) it is observed that some of these elements are serving the principle of transparency the same way as the "general" conditions of a data processing in "normal" circumstances. A

[23] GDPR Article 3.

[24] The GDPR shall apply to Guadeloupe, French Guiana, Martinique, Réunion, Saint-Barthélemy, Saint-Martin, the Azores, Madeira and the Canary Islands, to the European territories for whose external relations a Member State is responsible, and to the Åland Islands on the ground of Article 355 (1), (3), (4) of the Treaty of the European Union.

[25] SVANTESSON, DAN JERKER B.: *Article 3. Territorial scope*. In: Kuner, Christopher – Bygrave, Lee A. – Docksey, Christopher – Drechsler, Laura (eds.) 2020. p. 83.

[26] Restrictions can be provided for the following rights under Article 23 1) of the GDPR: the right to transparent information (Article 12 GDPR), right to information (Articles 13 and 14 GDPR), right of access (Article 15 GDPR), right to rectification (Article 16 GDPR), right to erasure (Article 17 GDPR), right to restriction of processing (Article 18 GDPR), notification obligation regarding rectification or erasure of personal data or restriction of processing (Article 19 GDPR), right to data portability (Article 20 GDPR), right to object (Article 21 GDPR), right not to be subject to an automated individual decision making (Article 22 GDPR), communication of a personal data breach to the data subject (Article 34 GDPR), as well as Article 5 "*in so far as its provisions correspond to the rights and obligations provided for in Articles 12 to 22.*"

[27] EDPB: Statement on restrictions on data subject rights in connection to the state of emergency in Member States. 2 June 2020. 3., p. 9.

[28] C-73/07 Satakunnan Markkinapörssi and Satamedia [2008] ECLI:EU:C:2008:727. p. 56.

[29] C-511/18, C-512/18 and C-520/18 La Quadrature du Net and Others v Premier ministre and Others [2020] ECLI:EU:C:2020:791. pp. 209–210.

general Privacy Statement or Privacy Policy should also contain information about the purposes of the processing or categories of processing; the categories of personal data; the specification of the controller or categories of controllers and storage period[30] as it is required in the case of a restriction in pandemic.

In connection with the additional pieces of the information regarding the special situation, we can state that these serve as the principle of transparency on a higher level. In the frame of the scope of the restrictions[31], it should be elaborated that which rights are concerned and how far they are going to be limited.

Concerning the safeguards to prevent abuse or unlawful access or transfer[32], the EDPB suggests organisational and/or technical measures, which means the obligation for controllers to guarantee the security of personal data.[33] These actions can cover in particular the so-called pseudonymisation and encryption of personal data[34], or the application of data protection by design and by default.[35] For these technical solutions and organisational measures it can be observed that they are not one-off measures but their effectiveness need to be regularly tested, assessed and evaluated, in order to ensure the security of the processed data.

Storage periods are standard elements of data processing information, adapted in accordance with the processing activity and the categories of personal data in question. In the context of the restrictive measures, the retention period should be specified together with the applicable safeguards taking into account the nature, scope and purposes of the processing or categories of processing.[36]

When data controllers determine the appropriate storage period, the common practice is that it is calculated as the duration of the processing operation plus additional time for potential litigation. The requirement to inform the data subject about the duration of the retention is essentially a form of the data minimisation principle, therefore, efforts should be made to minimise the period, for which the personal data are stored.[37]

In the case of the pandemic, it is not easy to determine the retention time, since the purpose, for which the personal data are processed, are depending not solely only on legal provisions, but rather on how long the COVID-19 virus will stay and affect the people's life all over the world.

Besides, it is important to mention an exception under Article 5 (1) e) of the GDPR, where data kept in a form enabling identification of data subjects may be stored for longer than is necessary for the purposes, for which the personal data are processed. In this way, they are further stored for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, when appropriate technical and organisational

[30] GDPR Article 23 (2) a), b), e), f).
[31] GDPR Article 23) (2) c).
[32] GDPR Article 23 (2) d).
[33] EDPB: Guidelines 10/2020 on restrictions under Article 23 GDPR. Version 1.0. Adopted on 15 December 2020. 12., p. 54.
[34] GDPR Article 32. (1) a).
[35] GDPR Article 25.
[36] GDPR Article 23. (2) f).
[37] GAWRONSKI, MACIEJ*: Guide to the GDPR*. Wolters Kluwer, The Netherlands. 2019. e-book online.

measures required by the GDPR are implemented, in order to safeguard the rights and freedoms of the data subject.[38]

Another factor under Article 23 (2) g) is that the restrictive legislative measure must contain specific provisions focusing on the risks to the rights and freedoms of data subjects. Under this condition, in accordance with the principle of transparency, data subjects can receive credible information about the potential impact of restrictions on them. The GDPR requests data controllers to carry out the so-called data protection impact assessment (DPIA), when data processing is likely to result in a high risk to the rights and freedoms of natural persons, especially in those cases when new technologies are used.[39] As stated by the EDPB, the preparation of a DPIA is not compulsory under Article 23, but should be considered by the legislator.[40]

Appropriate solution is when the legislator assesses the possible risks in all cases and a DPIA is performed, in particular, when it is necessary in accordance with Article 35 (1). In other cases, the EDPB suggests giving a detailed list about the concrete risks (e.g. profiling leading to discrimination, reduced freedom of speech, the right to privacy and data protection, a bigger impact on vulnerable groups such as children or persons with disability) not only in the impact assessment but in the recitals of the legislative measure as well.[41]

Finally, we should elaborate the condition that the right of data subjects should be informed about the restriction, unless that may be prejudicial to the purpose of the restriction.[42] The first part of the provision is clear and it echoes the basic principle of transparency, but the second part creates an exemption to this principle. According to the EDPB, restrictions may be adopted to protect investigations, therefore, if giving information to the data subject about the reasons for the restriction would hampering the effect of the restriction, information may not be disclosed. The EDPB suggests for data controllers to perform an assessment to check whether informing the data subject of the restriction is prejudicial to the purpose of the restriction, but restrictions must remain necessary and proportionate at the same time. On this ground, applying the exception clause, the controller could decide not to provide information at some point of data processing, if the restriction is lawful and strictly necessary in the specific case, and when it would be prejudicial to the purpose of the restriction. The EDPB proposes that the data controller should submit a data protection notice including this fact and if it is possible, a period in which the rights would be fully restored.[43]

The EDPB adapted another obligation of data controllers provided by the GDPR in the frame of the accountability principle, in the context of the restrictions. Among the obligations of the controllers, there is a requirement to maintain a record of processing activities under their responsibility under Article 30 (1) of the GDPR. This means that the controller should document the application of restrictions on specific cases by keeping a

[38] GDPR Article 5. (1) e).
[39] GDPR Article 35. (1).
[40] EDPB: Guidelines 10/2020. p. 13.
[41] EDPB: Guidelines 10/2020. p. 13.
[42] GDPR Article 23. (2) h).
[43] EDPB: Guidelines 10/2020. p. 13.

record of their application as well. This record should include the relevant reasons based on Article 23 (1), their timing and the outcome of the necessity and proportionality test. Considering Article 31 of the GDPR, it is important to mention that the controller shall cooperate, on request, with the supervisory authority in the performance of its tasks.[44] In connection with the restrictions, the legislator should make available their above-mentioned records to the data protection supervisory authority on its request. When the controller has a data protection officer (DPO), he/she should be informed without delay, whenever data subject rights are restricted in accordance with the legislative measure. The involvement of the DPO in the application of restrictions should also be documented.[45]

In accordance with Article 36 (4) of the GDPR, the national supervisory authority shall be consulted, before the adoption of restrictive legislative measures by the national parliament of a Member State. Under Article 57 (1) (c) of the GDPR, the supervisory authority can provide advice when restriction is needed regarding to the protection of data subject's rights and freedoms, when their personal data are processed. Failing this, the supervisory authority can issue on their own initiative "*opinions to the national parliament, the Member State government or, in accordance with Member State law, to other institutions or bodies as well as to the public on any issue related to the protection of personal data*".[46]

To sum up the above detailed conditions, according to our view, the EU data protection legal framework was designed to be sufficiently flexible and can allow for both an efficient response in limiting the pandemic, and for protecting fundamental human rights and freedoms.

Furthermore, we share the view that the data processing should be performed in a transparent manner in relation to the data subject despite the limitation, so the data controllers' obligation to provide any information in connection with the processing to the data subject under Articles 13 and 14 of the GDPR would remain unchanged. Moreover, we can state that the main principles, the obligations of the data controllers and all the provisions laid down in the GDPR are not allowed to be disregarded or annulled even despite special circumstances. The EDPB confirmed that the preservation of data protection principles is even more important in this difficult situation.[47] In conjunction with the principles of the GDPR, we refer especially to the principle of accountability, where the controller remains responsible to prove its ability to demonstrate to the data subjects his or her compliance with the provisions of the GDPR in the pandemic as well.

[44] GDPR Article 31.
[45] EDPB: Guidelines 10/2020. p. 14.
[46] GDPR Article 58 (3) (b).
[47] EDPB response to Mrs Ďuriš Nicholsonová and Mr Jurzyca's letter on common guidance in the fight against the COVID-19 pandemics. Brussels, 24 April 2020. p. 1. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2020-0030_mep_duris_covid19_en.pdf.

Although, both the Council of Europe[48] and from the side of the EU (the European Data Protection Board and the European Data Protection Supervisor)[49], it was stressed out that data protection cannot be an obstacle for saving lives and that the applicable principles always allow for a balancing of the interests at stake. But on the other hand, the EDPB stated that there is no need to lift the provisions of the GDPR, but just to observe them.[50] Therefore, the protection of personal data must be upheld in all emergency measures, including restrictions adopted at national level, as per Article 23 of the GDPR.[51]

In connection with a Hungarian legal provision,[52] the EDPB explicitly stipulated that any restriction must respect the essence of the restricted right. General, extensive restrictions or which are intrusive to the extent that they void a fundamental right of its basic content, must be considered unlawful. In the case such a restriction, further assessment is not required, whether it serves an objective of general interest or satisfies the criteria of necessity, proportionality. In the context of any restrictions applied by the Member States, their national law must be sufficiently clear by giving citizens an adequate indication on the circumstances and conditions, on which data controllers are empowered to resort to any such restrictions.[53]

In its Guidelines, the EDPB emphasized that the restrictions in the frame of Article 23 of the GDPR should be only exceptions to the general rule with strictly observed conditions, and even in exceptional situations, the protection of personal data cannot be restricted as a whole,[54] and it is not allowed to reach the point of a general suspension of all rights.[55]

Respecting democracy, the rule of law and fundamental rights, on which the European Union is founded, should be borne in mind, and the applied measures shall not be irreversible.[56] It follows that the legislator should lift the restrictions as soon as the circumstances that justify them no longer apply. The lifting of the restriction should be documented in the above-mentioned record, and after the abolition of the restrictions, the data subjects can exercise all their rights under GDPR. If this is not allowed for them by the

[48] Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, Chair of the Committee of Convention 108 and Jean-Philippe Walter, Data Protection Commissioner of the Council of Europe. Strasbourg. 30 March 2020. https://www.coe.int/en/web/data-protection/statement-by-alessandra-pierucci-and-jean-philippe-walter.

[49] EDPB: Statement on the processing of personal data in the context of the COVID-19 outbreak. 19 March 2020.; WIEWIÓROWSKI, WOJCIECH: *EU Digital Solidarity: a call for a pan-European approach against the pandemic*. 06April 2020.

[50] EDPB response to Mrs Ďuriš Nicholsonová and Mr Jurzyca's letter on common guidance in the fight against the COVID-19 pandemics. Brussels, 24 April 2020. p. 1. https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_letter_out2020-0030_mep_duris_covid19_en.pdf

[51] EDPB: Statement on restrictions on data subject rights in connection to the state of emergency in Member States. 2 June 2020. 2., p. 4.

[52] Decree 179/2020 of 4 May 2020 on the derogations from certain data protection and access to information provisions during the state of danger (*179/2020 (V. 4.) Korm. rendelet a veszélyhelyzet idején az egyes adatvédelmi és adatigénylési rendelkezésektől való eltérésről*), which was set aside on 18 June 2020.

[53] EDPB: Statement on restrictions on data subject rights in connection to the state of emergency in Member States. 2 June 2020. pp. 5-8.

[54] EDPB: Guidelines 10/2020 on restrictions under Article 23 GDPR. 15 December 2020. 4., p. 4.

[55] EDPB: Guidelines 10/2020. 6., p. 12.

[56] EDPB: Guidelines 10/2020. p. 5.

legislator, they can lodge a complaint to the supervisory authority against the controller, in accordance with Article 57 (1) f) and Article 77 of the GDPR.

IV. Potential solutions for guarantee data security

Regarding the processing of health-related data by public authorities, relevant recommendations have been issued by the Council of Europe. It has been stressed that communications to the public by health and government authorities should remain a priority, in order to protect, inform and advise the public. Nonetheless, during such communications, the publication of sensitive data (such as health-related data) of specific individuals should be avoided, and it is recommended that the processing of such data is only perform, if additional technical and organisational measures complementing those applied to non-sensitive data are put in place.

Additionally, one of the basic principles of the GDPR, namely data minimisation, has also high importance, since the disclosure of the identity of an infected person is not necessary in most cases.

Under Article 4 (5) of the GDPR, one of the potential solutions to ensure data security is pseudonymisation,[57] which means the removal of data that allow for the identification of a person and their substitution by other identifiers, such as a random code, which does not directly related to that person. It is important to emphasize that pseudonymised data are still considered personal data, as long as the data subject could be identified upon them combined with other information.

If such identification is not possible, and the pseudonymised data are no longer relate to an identified or identifiable natural person, the personal data should be regarded as anonymous information. And according to Recital 26 of the GDPR, the GDPR should not be applied to anonymous information.[58]

According to the EDPB, data cannot be anonymised on their own, only datasets as a whole may be made anonymous. Based on the Guidelines of the EDPB, any intervention on a single data should be deemed as pseudonymisation.[59]

Anonymisation processes and re-identification attacks are active fields of research. It is essential for any controller using anonymisation solutions to follow recent developments in this field, especially concerning location data, which are known to be hard to anonymise. Indeed, a large amount of research has shown that location data thought to be

[57] 'Pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

[58] GDPR Recital 26.

[59] EDPB: Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak. Adopted on21 April 2020. 18.

anonymised may in fact not be. Mobility traces of individuals are inherently highly correlated and unique. Therefore, they can be vulnerable to re-identification attempts under certain circumstances.[60]

The de-identification solutions as pseudonymisation can be suitable answers to the privacy concerns, especially for data processing without a valid consent of the data subject. However, some experts have proved that there are re-identification methods which can accurately estimate the likelihood of a specific person using 15 demographic attributes in any dataset.[61] While other scientists analysed social activity, especially Facebook Likes of 58,000 volunteers, according to which a wide variety of people's personal attributes with sensitive nature were revealed.[62]

In the context of medical research, conditions for third party access should be established. Any personal information provided to a third party should be made available in the form of non-identifying numbers or symbols. In case a third party need to use identified personal information, they should require personal consent. Researchers should design an operating system for personal privacy. Google and Apple recently released a tracking system with privacy features.[63] Other scholars also introduced systems that encrypt data to ensure privacy in applications. These options offer additional safeguards for ensuring personal privacy.

Finally, we should mention one of the possible tools for fighting against the virus, which is the contact tracing for close contacts of COVID-19 patients, and since the outbreak of the pandemic various solutions has been developed. Another tool in this fight is the use of a quarantine. Usually, patients and recent contacts who have no symptoms are quarantined from 10 to 14 days from the contact date of the confirmed patient. In some of the countries, self-quarantined individuals are monitored daily at local government call centres.[64] Thus, isolating individuals tested positive for a disease is imperative to prevent the occurrence and spreading of infectious diseases.

V. Conclusions

In this paper we investigated a complex question raised by the COVID-19 pandemic: how the highest standards of data protection required by the GDPR can be maintained in these exceptional circumstances, during processing personal data, especially health data.

To address this challenge, first we analysed the potential legal bases for processing health data to reveal its speciality. The relation between the original lawful bases under Article 6 (1) and the special exemptions for processing special categories of personal data

---

[60] EDPB: Guidelines 04/2020. 19.

[61] With Rocher et al. model, 99.98% of Americans would be correctly re-identified this way. See ROCHER, L. - HENDRICKX, J.M. – DE MONTJOYE, YA.: *Estimating the success of re-identifications in incomplete datasets using generative models*. Nature Communications10, 3069. 2019. pp. 1–2.

[62] KOSINSKI, MICHAL – STILLWELL, DAVID – GRAEPEL, THORE: *Private traits and attributes are predictable from digital records of human behavior*. Proceedings of the National Academy of Sciences of the United States of America (PNAS). vol. 110, no. 15. 2013. p. 5805.

[63] Source: Apple and Google: Privacy-Preserving Contact Tracing. https://covid19.apple.com/contacttracing.

[64] AHN, NA YOUNG – PARK, JUN EUN – LEE, DONG HOON – HONG, PAUL C. 2020. p. 171326.

under Article 9 were clarified. In this regard, we stated that Article 6 (1) must be applied in a cumulative way with Article 9 (2) to ensure that all relevant safeguards and measures are fulfilled. The appropriate legal basis laid down in Article 6 (1) shall be applied, only if Article 9 (2) of the GDPR provides for a specific derogation from the general prohibition to process special categories of personal data. We found that in most cases the consent is not an appropriate legal basis for the purposes of processing data under GDPR. Instead, especially in the context of the pandemic, the application of Article 9 (2) (i) of the GDPR is recommended, which allows the data processing on the ground of reasons of public interest in the area of public health, on the basis of Member State law.

In the second part of this work, we investigated the elements of Article 23 of the GDPR, which prescribes provisions to permit the adoption of restrictive legislative measures in specific circumstances. We can state that this Article contains clear and detailed provisions, not only for national legislators, but for the EU legislators as well. If the legislators fulfil these requirements, assess the risks for the right of data subjects as it is expected together with the continuous observation of necessity and proportionality, we believe that they can achieve the purpose of fighting against the virus despite the restrictions.

To enhance the tools in fighting against COVID-19, at the end of our work, we analysed some solutions for data security. We suggest that care should be taken in choosing the relevant and more fitting technical solution, and focusing not only on the fight against the virus, but on the need to preserve the protection of personal data.

According to our view, the EU data protection legal framework was designed to be sufficiently flexible and can allow for both an efficient response in reducing the pandemic, and for protecting fundamental human rights and freedoms. With this approach, we can conclude that "*data protection can in no manner be an obstacle to saving lives and that the applicable principles always allow for a balancing of the interests at stake*."[65]

[65] Joint Statement on the right to data protection in the context of the COVID-19 pandemic by Alessandra Pierucci, and Jean-Philippe Walter. Strasbourg. 30 March 2020.

VÁRADI SZILVIA

AZ EGÉSZSÉGÜGYI ADATOK KEZELÉSÉNEK JOGI KIHÍVÁSAI AZ EURÓPAI UNIÓBAN A COVID-19 ÁRNYÉKÁBAN

(Összefoglalás)

A SARS-CoV-2 új típusú koronavírus, amelyet először a kínai Vuhanban jelentettek 2019 decemberében. Az azóta COVID-19 néven „elhíresült" vírus által okozott fertőző megbetegedés nemcsak Kínában, de világszerte elterjedt, pandémiát hozva létre. A vírus az egészségünk mellett az élet minden területére, így a gazdasági életre és a társadalomra is jelentős hatással van, megváltoztatva többek között a társadalmi kapcsolatok formáit és a munka világát is.

Kétségtelen, hogy a világjárvány által okozott különleges körülmények között a személyes adatok feldolgozása elkerülhetetlen a megfelelő intézkedések megtételéhez, éppen a fertőzés terjedésének megállítása, valamint hatásainak megelőzése vagy minimalizálása érdekében. Ezek a személyes adatok pedig nem kizárólag „általános" típusúak lehetnek, mint például az adatalany neve, lakcíme, a rá vonatkozó utazási információk. Kiemelt fontosságú jelen körülmények között a szenzitív jellegű különleges adatok kezelése is, amelyek közé tartozik a megbetegedések kapcsán releváns egészségügyi adat.

Jelen tanulmány az Európai Unió általános adatvédelmi rendeletének szabályai alapján veszi górcső alá azt a kérdést, hogy hogyan hat a COVID-19 a személyes adatok közül az egészségügyi adatok kezelésére. Milyen jogalapok alkalmazhatóak kifejezetten a pandémia esetében ezen adatok jogszerű kezelésére? Figyelemmel arra, hogy az egyes (tag)államok kormányaira hárul a járvány elleni küzdelem embert próbáló feladata, vizsgáljuk azt is, hogy milyen (alapjogi) korlátozásokat tartalmazó jogszabályokat fogadhatnak el a rendelkezésre álló uniós jogi keretek között a különleges jogrend, így például veszélyhelyzet idején. Mindezek vizsgálatát követően a tanulmány az adatbiztonság garantálását célzó leghatékonyabb technikai megoldásokat is felvázolja.