Institutiones Administrationis – Journal of Administrative Sciences Vol. 2 (2022) No. 1, 36–47
DOI: 10.54201/iajas.v2i1.30

Implications of digitalization during the COVID-19 pandemics[1]

Daniela Dzuráková*

* Paneuropean University Faculty of Law PhD student, European Commission Directorate-General legal assistant.
E-mail: dzurakovadaniela@gmail.com

Abstract

The article provides an analysis of the proposal of the Regulation on European Digital Identity with regard to processing of personal data, particularly those that concerns health. It examines the Mobile Tracing Application and Digital Green Certificate, which were established in order to combat COVID-19. Finally, it lists the main challenges and critical positions, as well as proposals on how to tackle some of them.

Keywords

Mobile Tracing Application, Digital Green Certificate, European Digital Identity, GDPR, processing of personal data, health data, COVID-19.

1. Introduction

Digitalization is part of our every-day life and its development has become immense. The idea of creating a "Digital Europe" was originally put in place by the previous Commission's mandate under the name "A connected digital single market" (Bassot & Wolfgang, 2018). The current Commission supported and broadened this idea when publishing point 2 of the Commission Priorities 2019-2024.[2] The latter was accelerated by the existence of the COVID-19 pandemics. In order to keep our lives functioning, the digital world became inevitable. Apart from a non-exhaustive list of justice, school systems, consumer activities communication with private and public bodies and safeguarding the free movement of EU citizens during COVID-19 pandemic, the European Union started to come up with possible ways of addressing these via digital tools.

The pandemic was unprecedented in the history of the European Union and revealed various necessary measures for tackling similar situations in the future. The lack of scientific knowl-

[1] As a disclaimer, the article provides information exclusively stemming from the author's PhD studies and under no means presents any position of the European Commission.

[2] The European Commission's Priorities for 2019-2024. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age_en

edge of the virus itself and the non-exclusive competence of the European Union in dealing with COVID led to the creation of digital tools, first using recommendation and a Commission implementing decision, later through a regulation.

It is hoped that the virus is under control, but digitalization is still moving forward. The European Commission provided a proposal for a Regulation on European Digital Identity,[3] which should enable EU citizens to communicate with private and public bodies on various aspects, such as loans, insurance, tax returns, etc. The proposal also mentions data concerning health in the form of QR codes and ePrescriptions. It is not specified whether any other personal data concerning health, and particularly COVID-19, would be included. On the other hand, creating a digital tool that would hold such a large amount of personal data brings many risks.

In its first chapter, the article provides information concerning Mobile Tracing Applications and Digital Green Certificates, as the digital tools used with regard to combatting the spread of the COVID-19 pandemics, yet still enabling free movement of EU citizens. It assesses the legal basis for both digital tools, explains their main functions and mentions some of the bottlenecks with regards to processing personal data.

The third chapter is dedicated to an assessment of the proposal of the Regulation on the European Digital Identity. Apart from evaluating the legal basis and comparing it to the other two digital tools, it offers an analysis concerning the risks and future challenges with regards to personal data, particularly those on health.

2. Mobile Tracing Applications

2.1. Legal basis

Since COVID-19 was the very first pandemic observed within the EU, the legal framework concerning cross-border health threats and yet also the competences of the EU in the health sphere were rather limited. It is to be noted that the EU however had various legal acts at its disposal for regulating possible cross-border health threats in the form of a communication system between the Member States. Such an approach had been established by a Commission Implementing Decision (EU) 2019/1765. Its main aim was to create an e-health digital information system across the EU. Through a network of national authorities, the idea was to exchange best practice on one hand and provide for a smoother transfer of data in the event of providing cross-border health care. Mutual recognition was to be established on the basis of an interoperable system, whereby national authorities would be responsible of their own properly designed digital tools at the national level and implement such technical measures that would enable communication with other national schemes of the Member States relating to eHealth.

However, this Decision (EU) 2019/1765 did not establish a system that would be operable in the event of cross-border health threats in the sense of pandemics, rather than a system that would enable and facilitate the application of patients´ rights to cross-border healthcare.

[3] Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final.

As the imminent threat of the COVID-19 pandemics appeared and an urgent response was expected at the EU level, the European Commission first responded with a Recommendation,[4] which referred to the existing legal framework concerning e-Health. With the use of such a legal tool, the European Commission applied the logic that the free movement principle of the EU concept should be the prevailing factor in creating an interoperable system. Since no similar systems had been established previously, the decision to apply the closest provision applicable to the situation in the absence of a real one demonstrated not only a proper legal choice from the point of view of legal theory, but particularly with regards to the necessity for acting rapidly.

Before having the Commission Implementing Decision (EU) 2019/1765[5] amended, the Commission went through various procedural steps. Firstly, it provided Interoperability guidelines (European Commission, 2020), through which it defined and explained the functioning of the mobile tracing applications system, and also established the roles of key players. Further, a more technical specification was issued, which included the IT and key specifications in order to set up a system that would function at the interoperable level.

As a consequence, Commission Implementing Decision (EU) 2020/1023 was adopted as an amendment, although not repealing Commission Implementing Decision (EU) 2019/1765 which has remained equally in force. Apart from new definitions concerning mobile tracing applications, it focused mainly on the protection of personal data. Commission Implementing Decision (EU) 2020/1023 included all the recommendations provided by Guidelines 4/2020 (European Data Protection Board, 2020) of the European Data Protection Board (hereinafter "EDPB").

It established that personal data shall be transferred to a pseudonymised gateway from the national authorities and, due to a key attached to the data, another system of a different Member State should be able to decide the data by unlocking the pseudonymisation of the data.

One full Annex[6] of Commission Implementing Decision (EU) 2020/1023 has been dedicated to the division of roles with regard to processing personal data, and it was established that all the national authorities separately should be in the position of a controller. As a consequence, the creation of an interoperable network would lead to joint controllership.

In line with EDPB Guidelines 4/2020, the text of the Commission Implementing Decision (EU) 2020/1023 comprises the main principles, such as transparency, full control of the personal data by data subjects and no geographical location, as well as the establishment of privacy by design and by default via the pseudonymised transfer. Unlike the text of the legal act itself, the EDPB Guidelines in question provide the legal basis for processing of personal data for the purpose of public interest.[7] In addition, it enables the controllers to base their processing on the consent of data subjects; however "to ensure that strict requirements for such legal basis to be valid are met".[8] The processing of health data, classified as special categories of personal data pursuant to Regulation (EU) 2016/679 (hereinafter "GDPR"),[9] is established on the legal basis of public health interest, occupational medicine or consent.[10]

---

4 Commission Recommendation of 8.4.2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, C(2020) 2296 final.

5 Commission Implementing Decision (EU) 2020/1023.

6 Annex II to the Commission Implementing Decision (EU) 2020/1023.

7 Paragraph 30 of EDPB Guidelines 4/2020.

8 Paragraph 32 of EDPB Guidelines 4/2020.

9 Article 9 of GDPR.

10 Paragraph 33 of EDPB Guidelines 4/2020.

Interestingly, the European Commission did not put itself in the position of a controller, but as a processor, acting strictly under the instructions of the Member States. Such an approach is in line with the logic of the competences of the EU in the health sphere. Its main aim is to establish free movement of persons and the market, rather than dictate what tools the national authorities should or should not use. By creating the "Federation Gateway" system, it provides for harmonized criteria in order to enable the free movement of persons. As a consequence, and in line with the EU competencies in the area of health yet respecting the competencies of the Member States themselves, such a scenario seemed to be the most efficient in order to react quickly to slowly extending border closures. On the other hand, as the Member States had anticipated the existence of mobile tracing applications way before any legal form at the EU level, the response of the European Union might raise some concerns with regards to the efficiency of the system.

From the perspective of the legal basis stemming from the Treaty of Functioning of the European Union (hereinafter "TFEU"), the reference was made indirectly via the applicability of Directive 2011/24/EU. In its preamble, it is stated that the legal basis is Article 114[11] and Article 168[12] of TFEU.

2.2. Mobile Tracing Applications in practice

Looking into the practicalities of the usage of mobile tracing applications and in order to find out their efficiency at the European level, it is important to verify various criteria, particularly their interoperability and the speed of their deployment. Concerning the latter, one may observe that some Member States (e.g. Malta) had already deployed their mobile tracing applications before the idea of the interoperable system at the European level. On the other hand, there were countries which deployed their mobile tracing applications rather late, or not at all (e.g. Sweden, Bulgaria or Luxembourg, which did not even envisage creating mobile tracing applications). Greece and Romania, for instance, started to develop the application, but, by the time the second wave of pandemics, their applications were still not put in place.

With regards to the interoperability criteria, the vast majority of the Member States, even if not at the same time, provided for the interoperable functioning of the applications within the EU. In contrast, Estonia, Hungary, Portugal and Romania did not set up the interoperable functions at the moment of their deployment and they were still not applicable for the second wave of pandemics. As such, they could not have been compatible with other EU applications (European Commission, 2022).

It is also important to mention that Austria was the only Member State of the EU to discontinue its mobile tracing applications. This approach would seem a very reasonable as the EU COVID certificate (see chapter 2 of this Article) replaced the existence of mobile tracing applications at a later stage.

The privacy matter in relation to mobile tracing applications was at stake from the very beginning of the discussions of their deployment. It was established that these applications might be put in place, but not intruding into the privacy of data subjects. Such a position was applied both by the European Parliament, as well as the European Commission (European Parliament, 2020). The compromise approach was also confirmed by the European Data Protection Board,

[11] Approximation of laws.

[12] Competences of the EU in the area of health.

which meant that the deployment of mobile tracing applications was considered to be as an exceptional tool to safeguard the free movement of EU citizens within the territory of the European Union, yet not contributing to the spread of the virus. On the other hand, the need for this tool was balanced by privacy matters, namely data minimisation, no transfer of personal data as such, no geographical tracing and the voluntary download and use of these applications by data subjects.

On the basis of the paragraph above, looking strictly into the existence of the mobile tracing applications, it could be observed that the necessity of a tool on one hand and ensuring privacy measures on the other created a rather balanced platform which could be viewed as proportionate. However, looking into this matter from a broader perspective, an interoperable system at the EU level could not have functioned properly unless the Member States would have safeguarded interoperability and deployed these mobile tracing applications at the same time. This unfortunately was not the case. Member States were either unable to provide such a technical system in a short period of time, or could not even see the added value in their usage. One could also see that the form of a legal instrument might not have been very convincing for the Member States either. Last but not least, it is important to emphasise that, especially in the post-communist countries, the lack of trust in using these mobile tracing applications resulted in their restricted use. The lack of consistency and universality of the system led to inefficiency; it was not applicable throughout the EU territory. Whether its inefficiency could have been predicted stays remains a question. One can only presume that the voluntary approach of the Member States from the very beginning to creating platforms of these types would not establish a solid mechanism.

Consequently, the question whether such a mechanism could have been proportionate seems to be answered negatively. The processing of personal data, knowing that they are not to be evaluated in an interoperable way in any other member State only leads to the conclusion that data subjects would have to be exposed to supplementary processing of personal data and their choice of not uploading these systems came only naturally.

3. EU Digital Green Certificates

The existence of the first vaccines brought optimism not only to the area of health as such, but also promised better and easier regulation of the free movement of EU citizens. The idea was to provide a solidly functioning system of digital certificates that would demonstrate who was vaccinated and who was not. Even though the vaccination against COVID-19 was not a long-term-based vaccine, the SaRs-CoV (Varga, 2020) emerging in 2001 and 2003 is of the same family. Therefore, the Member States agreed to admit vaccination as one of the preconditions for enabling EU citizens to move freely within the EU.

The system was again envisaged as being established on the basis of the pre-existence of interoperable mechanisms, which would enable admitting and confirming the validity of a certificate issued in one Member State by another Member. The data within the certificate was expected to be pseudoanonymized, as in the case of mobile tracing applications. The processing of personal data in the COVID certificates was to be done under the controllership of the Member States with the European Commission acting as the processor when providing the Gateway system.

Since the vaccination system is considered to be a strong intrusion into the privacy of individuals and regardless of the judgment concerning the obligation of vaccination, *Vavřička*, of 8 April 2021, the proposal of the Regulation on Digital Green Certificates (European Data Protection Board, 2021a) also envisaged the possibility of having been tested or provided with a certificate on overcoming the corona. In this way, the Digital Green Certificate would not only

hold information about the vaccination, but also about testing and overcoming of the virus. In addition, the certificate should hold the name, surname, date of birth and, in the case of vaccination, the type and number of the vaccine.

3.1. Legal basis

Unlike with Mobile Tracing Applications, the European Union took a more active approach and opted to create a regulation. It seems that, by availing of such a legal tool, it envisaged eliminating the voluntary aspect and thus avoiding a malfunctioning system. It was imposed in this form on all Member States.

Regulation (EU) 2021/953 (hereinafter the "Regulation on the Digital Green Certificate") was expected to deviate from the already existing system created by the Decision of the European Parliament and Council 1082/2013/EU which served also as the legal basis for the Commission Implementing Decision (EU) 2020/1023 on mobile tracing applications. However, in this case, the very first recital of the Regulation on Digital Green Certificate refers to free movement as also outlined in the very first legal reference of the regulation providing for Article 21(2) of TFEU. This article enables the European Parliament and the Council to act in an ordinary legislative procedure when attaining the right to move and reside freely within the territory of the Member States.

Further recitals of the Regulation on Digital Green Certificate refer to the Council recommendation (EU) 2020/1475,[13] which actually served as the legal basis for the Council Decision 1082/2013/EU on cross border health threats as well. We can observe that, although Council Recommendation (EU) 2020/1475 is mentioned in both legal acts, the Decision of the European Parliament and Council 1082/2013/EU on cross-border health threats refers to health matters as set out in Article 168 of the TFEU concerning health while the Regulation on the Digital Green Certificate's purpose is to facilitate free movement only.

With regards to the Regulation on the Digital Green Certificate, it is important to mention that no impact assessment was performed prior to its adoption. The lack of impact assessment was justified by the urgency of the need to establish a well-functioning system. On the other hand, with regard to the extent of intrusion into the human right to privacy and taking into consideration the fact that the virus had already been there for approximately 6 months, it seems to be difficult to imagine not undertaking any kind of assessment on these terms.

On the other hand, the matter was discussed with the EDPB and the European Data Protection Supervisor (hereinafter as "EDPS") which provided a joint opinion (European Data Protection Board, 2021a). They welcomed the initiative but pointed out various elements to be considered. It mentioned that the basic principles concerning processing personal data, such as data minimization, transparency, adoption of adequate technical and organizational privacy and security measures, would have to be applied. They also emphasised that the personal data may only be processed and stored within a certain period of time, particularly during the existence of the purpose of their processing.

It is interesting that the Regulation on Digital Green Certificate does not prevent Member States from defining other purposes for which the personal data may be processed. It is true that the GDPR rules apply in general and any additional purpose for which a Member State might be

[13] Council Recommendation (EU) 2020/1475 of 13 October 2020 on a coordinated approach to the restriction of free movement in response to the COVID-19 pandemic (Text with EEA relevance), OJ L 337, 14.10.2020, p. 3–9.

able to process the personal data concerning the Digital Green Certificate should be in line with these rules. However, it is also important to point out that these data are supposed to be processed exclusively during pandemics and it is difficult to imagine what other purposes would be justified enough to deviate from the short-term exceptional derogation of processing personal data.

In addition, as already mentioned, the system of joint controllership could be considered the right one; however, with an unlimited and unknown number of purposes for processing by the member States, the clear identity of the controllership, thus the responsibility for the processing of personal data, may easily be faded out. This could lead to violations of transparency principles, as well as the inability to exercise the data subject's rights.

3.2. European Digital Green certificates in practice

Digital Green Certificates operated on a very similar principle to the Mobile Tracing Applications. It included the creation of a federation gateway in order to make the personal data interoperable between the Member States. As originally stated, the personal data were envisaged to be somehow encrypted in a QR-code, which, using the interoperable communication between the national systems of the Member States, would only provide information on whether the person was "green" to pass or not. However, many codes, when being scanned, displayed the data of name, surname, date of birth, possibly address and information about the vaccination/recovery/test.

At later stages, an obstacle to free movement arose in the form of an additional measure to the vaccination, a test for COVID-19, in some Member States. Not only were citizens required to undergo a supplementary intrusion into their privacy in the form of a medical intervention, but also intrusion by collecting additional personal data. One could question the real efficiency of such a system and also its proportionality vis-a-vis the privacy matters.

4. European Digital Identity

The idea of creating a European Digital Identity stems from the European Commission's priority for digitalization, namely Digital Compass 2030. As the survey shows, 63% of the EU citizen population wishes to have a single digital identity. This would enable its users to facilitate private and public relations, such as loan requests and tax returns, including electronic signature and eStamp. From the perspective of "digital citizenship", one could imagine that the digital identity would enable a citizen to perform any or selected operations from a single user's digital identity, even cross-border within Member States.

However, electronic operations around the EU territory are not a novelty and one can observe them via Regulation (EU) No 910/2014 (hereinafter "eIDAS Regulation"). Under this legal act, the idea was to secure electronic interaction between citizens, businesses and public authorities, thereby increasing the effectiveness of public and private online services.[14] The digital single market was envisaged to facilitate the cross-border use of online services.

The main legal basis mentioned in the eIDAS Regulation is Article 114 TFEU, on the approximation of laws. As a consequence, the principle of subsidiarity was applied as set out in Recital 76 of the eIDAS Regulation. Regarding health data, the applicable legal basis as mentioned is Directive 2011/24/EU.

The system was based on creating a public key infrastructure at pan-European level that

[14] Recital 2 of Regulation 910/2014.

would lead to an interoperable gateway across the national borders of the Member States. In practice, a new system of electronic signatures that would be able to communicate through an interoperable infrastructure would be established. In addition, rules for trust services were defined.

It was deemed that the trust service providers would be liable for any damage (intentional or negligent[15])caused to any natural person from failing to fulfil the obligations stemming from the eIDAS Regulation;[16] that is, the controllers responsible for the processing of personal data would be the trust service providers. Information about any breaches was to be notified to the Commission and the European Union Agency for Network and Information Security (hereinafter "ENISA"). If a security breach or loss of integrity was likely to affect a natural person adversely, the trust service provider would also be obliged to notify the harmed data subject. Although the applicable rules concerning personal data protection were previously guaranteed by Regulation 45/2001, hence the system of protection for data subjects was different from the one established by the GDPR, it reflects a similar practice.

However, the system has not achieved its potential. Only 59% of the EU population enjoys the schemes arising from the eIDAS Regulation. The problem is partly caused by the fact that the vast majority of electronic identities are being used in the private sector, by banks, mobile phone operators etc.

European Digital Identity will be established by a proposal for a Regulation (European Data Protection Board, 2021b) (hereinafter as "Regulation on Digital Identity"), which shall amend the above existing legal framework on eIDAS. According to its explanatory memorandum, it was important to support a trusted and secure digital identity solution, because those solutions which fall outside the scope of eIDAS were very often offered by social media providers, which raise privacy and data protection issues. It emphasised that the eIDAS system should be expanded by three new services, electronic archiving, electronic ledgers and remote electronic signature/seal.

4.1. Legal basis

The legal basis for this Regulation on Digital Identity is Article 114 TFEU. Although there is no mention of the legal basis concerning health, the newly established system is planned to include medical certificates and ePrescriptions, as well as QR-codes.[17] The principles of subsidiarity and proportionality are clearly indicated, justifying the EU's competence to act as the Member States would not be able to create such an interoperable system, thereby not being able to reach the objective.

The proposal has gone through the stakeholders' consultation and is at the stage of the first reading. The proposal was also shared with the Member States. It is mentioned that the secure digitalization on mobile devices is the technological future, justifying why the private and public sector have already moved towards technologically-developed systems. Those of the private sector mentioned in the explanatory memorandum are non-exhaustively Apple, Google and Thales. Last but not least, an impact assessment was made with regard to the proposal. The very first draft received a negative opinion from the Scrutiny Board. After the Commission's follow-up, the Scrutiny Board provided a positive opinion.

In practice, the application of the Regulation on Digital Identity should include three stages. The first one should include an imposition of a mandatory notification of the eIDs. In that way

15 Article 13 of Regulation 910/2014.

16 Recital 37 of Regulation 910/2014.

17 Recital 9 of the proposal.

the mutual recognition of the national systems would be established. The second level would require the exchange of data linked to identity. The last stage, aiming at the full regulation within the EU territory, includes mutual recognition of eID means, as well as full legal recognition of electronic attestations.

4.2. Practical aspects concerning personal data

The explanatory memorandum creates some guarantees concerning full compliance with the data protection legislation, hence the application of the GDPR or Regulation (EU) 1725/2018. It emphasises that the eWallet[18] function would enable the data subjects to control their personal data better. Concerning health data, it clarified that they would only be processed in accordance with national law.

However, it is not clarified how the transfer of personal data concerning health would be made interoperable between the Member States, as their national laws on health could be totally different. Transfers to third countries outside the EU territory, are not consulted more concretely within the proposal. Considering for instance cloud-based solutions, as well as the probability that the eWallet would be used by the American platforms of Apple, Google etc., questions arise as to how secure digitalization, in light of the Schrems II ruling, could be established. In addition, some of the platforms could be also stored on handsets created by third countries that are on the "black list" when it comes to the protection of data subject rights, e.g. Huawei and consequently the transfer of personal data to China (EDPS, 2021).

Transfer of personal data is not considered as the only bottleneck. The collection and processing of personal data with regards to eWallets includes an undefined list of personal data, including biometrics. Although the data minimization principle is mentioned in the recitals as well as the main text of the proposal, it is difficult to imagine, how data minimization would be ensured in reality. One device and an application can hold huge amount of personal data. This could lead to easier profiling and a greater risk of incorrect identities.

To ensure legal certainty, the long-term preservation of electronic documents is envisaged.[19] Since no clear distinction between storage periods with regard to type of personal data is mentioned, it is very difficult to envisage how one of the main principles of lawful processing of personal data, storage limitation, will be applied properly.

As part of the legislative procedure,[20] the EDPS was also consulted. One of the important comments concerned the physical and logical separation of the personal data relating to the eWallet from the rest of the personal data.[21] This part of the comment has been reflected in the text of the Proposal.[22]

---

[18] Newly inserted point 42 into the existing Article 3 of 910/2014: "European Digital Identity Wallet' is a product and service that allows the user to store identity data, credentials and attributes linked to her/his identity, to provide them to relying parties on request and to use them for authentication, online and offline, for a service in accordance with Article 6a; and to create qualified electronic signatures and seals".

[19] Recital 33 of the proposal of Regulation on Digital Identity.

[20] Article 42 (1) of Regulation (EU) 2018/1725.

[21] Bullet 5 of the part 2 of the Formal comments of the EDPS on the proposal of the Regulation on European Digital Identity.

[22] Newly inserted Article 6a, paragraph 7.

5. Conclusions

Although the idea of digitalization is more than welcomed by governmental authorities, as well as majority of EU citizens, one needs to take into consideration the possible risks arising from the soon to be established system of the European Digital Identity.

Firstly, it would lead to the exclusion of some people from EU society, particularly those who have lower digital literacy or less access to digital devices. Such a group of people could be rather significant, as it would not only include elderly people and people with disabilities, but also those from socially disadvantaged groups. As it was pointed out in the comments to the legislative proposal by the European Economic and Social committee,[23] digitalization of this type would require a huge campaign and education as well as much work by the Member States in order not to face any cases of discrimination.

In addition, the rather doubtful aspect is the physical separation of the personal data, particularly once the personal data were uploaded to one mobile application. It is difficult to imagine a practical example of how such a physical and logical separation could be possibly reached. As a consequence, the role of the Data Protection Authorities would be very crucial in order to monitor this phenomenon closely.

Third, it seems that the scope of personal data held by the eWallet is very broad. As such, the lack of a data minimisation principle could very easily lead to misidentification and therefore discrimination against data subjects. How data subjects will be able to exercise their fundamental rights while knowing that such a large amount of their personal data might be transferred via mobile applications to countries which do not respect citizens' fundamental rights and have no redress equivalent to the protection of personal data within the territory of the EU can be obtained is a critical issue.

Concerning the legal basis, although the approximation of laws is somewhat relevant, intervention into processing personal data concerning health could require more attention. Although not completely necessary, as it is mentioned in Regulation (EU) 910/2014 to be amended, mentioning the competence of the European Union in the health sphere would be appropriate.

Last but not least, the question of processing personal data concerning health still stays open. For instance, processing the data from the Digital Green Certificates is conditional of the existence of a pandemic, hence derogation from the application of fundamental rights. However, if the eWallet will give the possibility to include the Digital Green certificates, these personal data would fall under a long-term processing rather than a derogation. It will be crucial to disable the digital tools of Mobile Tracing Applications and Digital Green Certificates and consequently delete the personal data from them. To close, the European Digital Identity should not include any personal data concerning health that goes beyond Directive 2011/24/EU concerning only cross-border health care.

[23] Point 1.2 of the Opinion of the European Economic and Social Committee on the proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, (COM(2021) 281 final 2021/0136 (COD)) (2022/C 105/12).

References

Bassot, É., & Wolfgang, H. (2018). *The Juncker Commission's ten priorities. State of play in autumn 2018.* European Parliamentary Research Service. https://doi.org/10.2861/50748

European Commission. (2020). *eHealth Network Guidelines to the EU Member States and the European Commission on Interoperability specifications for cross-border transmission chains between approved apps. Basic interoperability elements between COVID+ Keys driven solutions.* Online: https://bit.ly/3N0B8nd

European Commission. (2022). *Mobile contact tracing apps in EU Member States*. Online: https://bit.ly/3N3SAHs

European Data Protection Board (2021a). *EDPB-EDPS Joint Opinion 04/2021 on the Proposal for a Regulation of the European Parliament and of the Council on a framework for the issuance, verification and acceptance of interoperable certificates on vaccination, testing and recovery to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate)*. Online: https://bit.ly/3xrf1AI

European Data Protection Board (2021b). *Formal comments of the EDPS on the Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity*. Online: https://bit.ly/39wAJv7

European Data Protection Board. (2020). *Guidelines 04/2020 on the use of location data and contact tracing tools in the context of the COVID-19 outbreak.* Online: https://bit.ly/3mTLlY4

European Data Protection Supervisor. (2021). *Government access to data in third countries, Final Report, EDPS/2019/02-13.* Online: https://bit.ly/3xBqCxd

European Parliament. (2020, May 14). *COVID-19 tracing apps: MEPs stress the need to preserve citizens' privacy.* Online: https://bit.ly/3xBqNsn

Gawronski, M. (Ed.) (2019). *Guide to the GDPR.* Wolters Kluwer.

Krysztofek, M. (2021). *GDPR: personal data protection in the European Union.* Wolters Kluwer.

Tzanou, M. (Ed.) (2020). *Health Data Privacy under the GDPR: Big Data Challenges and Regulatory responses*. Routledge. https://doi.org/10.4324/9780429022241

Varga, B. M. (2020, April 23). *The differences between SARS-CoV-1 and SARS-CoV-2.* European Parliamentary Research Service. Online: https://bit.ly/3zNlBEn

Legal sources

Regulation (EC) No 45/2001 of the European Parliament and of the Council of 18 December 2000 on the protection of individuals with regard to the processing of personal data by the Community institutions and bodies and on the free movement of such data, OJ L 8, 12.1.2001, p. 1–22. Online: https://bit.ly/3xC7fnt

Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114. Online: https://bit.ly/3tCZQDm

Proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity, COM/2021/281 final

Opinion of the European Economic and Social Committee on the proposal for a Regulation of the European Parliament and of the Council amending Regulation (EU) No 910/2014 as

regards establishing a framework for a European Digital Identity (COM(2021) 281 final – 2021/0136 (COD)), EESC 2021/02756, OJ C 105, 4.3.2022, p. 81–86. Online: https://bit.ly/3mYpIWK

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) (Text with EEA relevance), OJ L 119, 4.5.2016, p. 1–88. Online: https://bit.ly/3tGK3DG

Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (Text with EEA relevance), PE/31/2018/REV/1, OJ L 295, 21.11.2018, p. 39–98. Online: https://bit.ly/3HylsGJ

Regulation (EU) 2021/953 of the European Parliament and of the Council of 14 June 2021 on a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) to facilitate free movement during the COVID-19 pandemic (Text with EEA relevance), OJ L 211, 15.6.2021, p. 1–22. Online: https://bit.ly/3tGAHYv

Directive 2011/24/EU of the European Parliament and of the Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88, 4.4.2011, p. 45-65. Online: https://bit.ly/3tE8ZvC

Commission Recommendation (EU) 2020/518 of 8 April 2020 on a common Union toolbox for the use of technology and data to combat and exit from the COVID-19 crisis, in particular concerning mobile applications and the use of anonymised mobility data, OJ L 114, 14.4.2020, p. 7–15. Online: https://bit.ly/39zWM4a

Council Recommendation (EU) 2020/1475 of 13 October 2020 on a coordinated approach to the restriction of free movement in response to the COVID-19 pandemic (Text with EEA relevance), OJ L 337, 14.10.2020, p. 3–9. Online: https://bit.ly/3y0e3gr

Decision No 1082/2013/EU of the European Parliament and of the Council of 22 October 2013 on serious cross-border threats to health and repealing Decision No 2119/98/EC (Text with EEA relevance), OJ L 293, 5.11.2013, p. 1–15. Online: https://bit.ly/3zZPxNV

Commission Implementing Decision 2019/1765 of 22 October 2019 providing the rules for the establishment, the management and the functioning of the network of national authorities responsible for eHealth, and repealing Implementing Decision 2011/890/EU (notified under document C(2019) 7460) (Text with EEA relevance), OJ L 270, 24.10.2019, p. 83–93. Online: https://bit.ly/3N3SSOy

Commission Implementing Decision (EU) 2020/1023 of 15 July 2020 amending Implementing Decision (EU) 2019/1765 as regards the cross-border exchange of data between national contact tracing and warning mobile applications with regard to combatting the COVID-19 pandemic (Text with EEA relevance), OJ L 227I, 16.7.2020, p. 1–9. Online: https://bit.ly/3zZPnWP

Case of Vavřička and others v. the Czech Republic, Applications nos. 47621/13 and 5 others. Online: https://bit.ly/39xErVe

Judgement of 16 July 2020, Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems, C-311/18, EU:C:2020:559.

The European Commission´s priorities for 2019-2024. Online: https://bit.ly/39uyOqU