The EU Digital COVID Certificate: A Preliminary Data Protection Impact Assessment

Oskar Josef GSTREIN*

On 20 May 2021, the European Commission, Council and Parliament announced a breakthrough in the trialogue negotiations to establish the European Union (EU) Digital COVID Certificate. Originally, this standardisation effort was labelled as "Digital Green Certificate" and – "[i]n view of the urgency" – presented without a data protection impact assessment. It should allow citizens and residents of Member States to prove that they are either vaccinated against COVID-19, have recently tested negative or are currently immune against the virus. This article considers the proposal from a privacy perspective, taking into account the opinion of EU data protection authorities, ongoing negotiations in the EU institutions and relevant developments on the national and international level. While the European Parliament and others tried to improve the original Commission proposal, questions around the appropriateness and effectiveness of the framework remain. The technological and organisational implementation is essentially left to Member States, who already have started to develop their own tracing and identification systems.

I. Introduction

On 17 March 2021, the Commission of the European Union (EU) published a "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" (Draft Regulation).[1] Together with the corresponding proposal applicable to third-country nationals legally staying or residing in the EU,[2] it provided the basis for the ongoing

* University of Groningen, Campus Fryslân, Data Research Centre, Groningen, The Netherlands; email: o.j.gstrein@rug.nl.

[1] European Commission, "Proposal for 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)" (2021) COM(2021) 130 final 2021/0068(COD) <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021PC0130> (last accessed 22 May 2021).

[2] European Commission, "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 Third-Country Nationals Legally Staying or Legally Residing in the Territories of Member States during the COVID-19 Pandemic (Digital Green Certificate)" (2021) COM(2021) 140 final 2021/0071 (COD) <https://ec.europa.eu/info/sites/info/files/en_green_certif_tcn_home_reg140final.pdf> (last accessed 22 May 2021).

European Journal of Risk Regulation, 12 (2021), pp. 370–381 doi:10.1017/err.2021.29

negotiations to establish a "Digital Green Certificate".[3] After several rounds in the "trialogue" format adopted to speed up the process, the European Parliament, the Council of the EU and the Commission announced a breakthrough on 20 May 2021. It seems that the final compromise is scheduled for adoption by the European Parliament in the session from 7 to 10 June 2021.[4] During the negotiation process the name was changed to "EU Digital COVID Certificate" (EUDCC), which could be interpreted as an attempt to leave the mixed reception of the original Commission proposal behind. Officially, the main purpose of this certificate is to guarantee the right to move and reside freely within the territory of the Member States in accordance with Article 21 paragraph 2 of the Treaty on the Functioning of the European Union (TFEU). The Draft Regulation should fully harmonise efforts of Member States to facilitate cross-border movement within the Union without discrimination, while not in itself becoming a mandatory requirement to do so. As acknowledged in recital 8 of the original proposal, the publication of the Draft Regulation might even seem urgent from the Commission's perspective, since many Member States have or are planning to launch national initiatives to issue certificates.[5] These are a priority for those countries with large tourism and transport sectors, who fear losing a significant portion of their economic activity for the second year in a row since the World Health Organization (WHO) declared the COVID-19 pandemic on 11 March 2020.[6] At the time of writing, Austria, Bulgaria, Croatia, Cyprus, Denmark, France, Germany, Greece, Italy, Malta, Portugal, Slovenia and Spain seem to actively promote the EUDCC. The technological implementation of programmes in Member States varies, with proposed solutions spanning from classical paper-based documentation to advanced identity management systems using blockchain.[7] The EUDCC should become a reality before the end of June 2021, according to EU Commissioner Didier Reynders.[8]

The Commission proposals marked an important milestone in a discussion that has been running for much longer.[9] On 25 February 2021, the European Council called

[3] European Commission, "COVID-19: Digital Green Certificates" (17 March 2021) <https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/covid-19-digital-green-certificates_en> (last accessed 22 May 2021).

[4] European Parliament, "EU Digital Covid Certificate: Provisional Deal between Parliament and Council | News | European Parliament" (20 May 2021) <https://www.europarl.europa.eu/news/en/press-room/20210517IPR04111/eu-digital-covid-certificate-provisional-deal-between-parliament-and-council> (last accessed 22 May 2021).

[5] European Commission, "Proposal for 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)", supra, note 1.

[6] D Cucinotta and M Vanelli, "WHO declares COVID-19 a pandemic" (2020) 91 Acta Bio Medica: Atenei Parmensis 157.

[7] S Krempl, "Digitaler EU-Impfnachweis soll in die Corona-Warn-App integriert werden" (*heise online*, 15 April 2021) <https://www.heise.de/news/Digitaler-EU-Impfnachweis-soll-in-die-Corona-Warn-App-integriert-werden-6017119.html> (last accessed 22 May 2021).

[8] ES Nicholás, "MEPs raise concerns on vaccine 'travel certificates'" (*EUobserver*, 14 April 2021) <https://euobserver.com/coronavirus/151529> (last accessed 22 May 2021).

[9] A Alemanno and L Bialasiewicz, "Covid-19 : « Le passeport vaccinal européen, une idée au mieux prématurée, au pire irréfléchie »" (*Le Monde.fr*, 26 January 2021) <https://www.lemonde.fr/idees/article/2021/01/26/covid-19-le-passeport-vaccinal-europeen-une-idee-au-mieux-prematuree-au-pire-irreflechie_6067602_3232.html> (last accessed 22 May 2021).

for a common approach to vaccination certificates.[10] As the EU struggles to ramp up its inoculation effort due to countless medical (eg inefficacy of vaccines, unforeseen side effects, virus mutations), organisational (eg manufacturing and logistics, setting up large-scale vaccination campaigns) and political hurdles (eg stockpiling of resources and vaccines in the name of "vaccine nationalism", "vaccine diplomacy" that transforms more or less effective vaccines into political bargaining chips), which it needs to tackle simultaneously, the EUDCC is proposed as an alternative for reopening societies and boosting economic activity.

Internationally, similar efforts are being discussed under the label "vaccine passports". All of these initiatives come with the promise that a quick return to "normal life" is possible once effective vaccines are available – at least to some. In the race to implement such programmes, Israel took pole position, with its digital "Green Pass" becoming operational nationwide on 21 February 2021, while the UK is in the runner-up position: its first pilot schemes took place from 16 April 2021 and the nationwide rollout started on 17 May 2021.[11] Many other countries such as Australia, China and some US states are in the process of developing and rolling out their own programmes.[12] The idea has failed to gain traction at the federal level in the USA so far, but it remains to be seen what will happen if the inoculation rate remains too low to achieve "herd immunity", which is required for an effective vaccine-based deterrence of SARS-CoV-2 and its variants.[13] In addition, there are corporate initiatives such as IBM's "Digital Health Pass", as well as sector-specific initiatives such as that of the International Air Transport Association (IATA).[14] While there is much to write about the ethical, social, political and legal aspects associated with the idea behind the EUDCC,[15] this article analyses the original Draft Regulation and the current discussion through the lens of European privacy and data protection law. This

[10] European Council, "Statement of the Members of the European Council on COVID-19 and Health, 25 February 2021" (25 February 2021) <https://www.consilium.europa.eu/en/press/press-releases/2021/02/25/statement-of-the-members-of-the-european-council-on-covid-19-and-health-25-february-2021/> (last accessed 22 May 2021).

[11] O Holmes and Q Kierszenbaum, "Covid: vaccinated Israelis to enjoy bars and hotels with 'Green Pass'" (*The Guardian*, 19 February 2021) <http://www.theguardian.com/world/2021/feb/19/covid-vaccinated-israelis-to-enjoy-bars-and-hotels-with-green-pass> (last accessed 22 May 2021); J Parker, "Covid: trials to begin for return of England mass events" (*BBC News*, 4 April 2021) <https://www.bbc.com/news/uk-56625307> (last accessed 22 May 2021); L Muscato, "What England's new vaccine passport could mean for Covid tech's next act | MIT Technology Review" (19 May 2021) <https://www.technologyreview.com/2021/05/19/1025041/england-nhs-vaccine-passports-worldwide/> (last accessed 22 May 2021).

[12] J Massola, "Morrison government readies rollout of vaccine certificates" (*The Sydney Morning Herald*, 6 February 2021) <https://www.smh.com.au/politics/federal/jab-and-go-morrison-government-readies-rollout-of-vaccine-certificates-20210205-p56zv7.html> (last accessed 22 May 2021); S Popescu and A Phelan, "Opinion | Vaccine passports won't get us out of the pandemic" (*The New York Times*, 22 March 2021) <https://www.nytimes.com/2021/03/22/opinion/covid-vaccine-passport-problem.html> (last accessed 14 April 2021); M Peel and A Hancock, "EU plans digital vaccine passports to boost travel" (1 March 2021) <http://www.ft.com/content/b038316f-4c58-4667-810d-efe48f54a927> (last accessed 2 March 2021); D Walsh, "Do we need 'vaccine passports' to get Europe moving again?" (*euronews*, 11 December 2020) <https://www.euronews.com/travel/2020/12/11/do-we-need-coronavirus-vaccine-passports-to-get-the-world-moving-again-euronews-asks-the-e> (last accessed 22 May 2021).

[13] A Mandavilli, "Reaching 'herd immunity' is unlikely in the U.S., experts now believe" (*The New York Times*, 11 May 2021) <https://www.nytimes.com/2021/05/03/health/covid-herd-immunity-vaccine.html> (last accessed 22 May 2021).

[14] JL Parker, "The case for one Covid passport" (*Forbes*, 22 December 2020) <https://www.forbes.com/sites/jenniferleighparker/2020/12/22/the-case-for-one-covid-passport/> (last accessed 22 May 2021).

[15] See the other contributions to this special issue and OJ Gstrein, DV Kochenov and A Zwitter, "A terrible great idea? COVID-19 'vaccination passports' in the spotlight" (2021) Centre on Migration, Policy and Society Working Papers 28.

seems particularly necessary since "[i]n view of the urgency, the Commission did not carry out an impact assessment".[16]

II. Context and focus

Before turning to the analysis and discussion of central elements of the proposed EUDCC, it is necessary to briefly elaborate on the context and focus of the remarks and claims in this article. Since the development of the legislative framework is ongoing during the time of writing, the assessment is essentially based on the original Commission proposal. However, it takes into account a Joint Opinion published by the European Data Protection Board (EDPB) and the European Data Protection Supervisor (EDPS),[17] as well as a version of the amended draft shared by the Presidency of the EU Council on 21 May 2021, after the end of the trialogue negotiations. This can be considered as a compromise between the legislators, as well as a reaction to remarks from civil society and other European institutions ("updated draft" from here on).[18] The updated draft is particularly relevant since it contains recitals 37–40c, which clarify that Regulation (EU) 2016/679 – better known as the General Data Protection Regulation or GDPR – is applicable as further elaborated below. Additionally, the update contains with Article 9 a provision that is dedicated to the protection of personal data.

Nevertheless, the national frameworks, including the national data protection authorities (DPAs), play an essential role in guiding the implementation of the EUDCC. The EU Regulation is merely standardising the necessary data, as well as the exchange of information between Member States. Therefore, enhanced scrutiny of the national systems implementing the EUDCC in practice is crucial. This has already been acknowledged through critical statements by the Austrian, French and Italian DPAs.[19] It goes beyond the scope of this article to assess all of these national systems in detail. The focus is on the assessment of the central provisions of the proposed and updated draft for a EUDCC Regulation, as they seem particularly relevant in the context of European data protection law and associated privacy-preserving principles.

[16] European Commission, "Proposal for 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)", supra, note 1, 5.

[17] European Data Protection Board and European Data Protection Supervisor, "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)" (2021) Version 1.1 6 <https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_edps_joint_opinion_dgc_en.pdf> (last accessed 22 May 2021).

[18] Presidency of the Council of the European Union, "Note from the Presidency to the Permanent Representatives Committee" (2021) Note 8719/21.

[19] Österreichische Datenschutzbehörde, "1575/SN-122/ME (XXVII. GP) – Epidemiegesetz 1950, COVID-19-Maßnahmengesetz, Änderung" (17 May 2021) <https://www.parlament.gv.at/PAKT/VHG/XXVII/SNME/SNME_94293/index.shtml> (last accessed 22 May 2021); Commission nationale de l'informatique et des libertés, "La CNIL Précise Les Garanties Que Doit Respecter La Fonctionnalité TousAntiCovid-Carnet | CNIL" (22 April 2021) <https://www.cnil.fr/fr/la-cnil-precise-les-garanties-que-doit-respecter-la-fonctionnalite-tousanticovid-carnet> (last accessed 22 May 2021); Garante per la protezione dei dati personali, "Covid: Garante privacy, no a 'pass vaccinali' per accedere a locali o fruire di servizi senza una legge nazionale" (1 March 2021) <https://www.garanteprivacy.it:443/home/docweb/-/docweb-display/docweb/9550331> (last accessed 22 May 2021).

III. Preliminary data protection impact assessment

1. Necessity and benefits

Over recent decades, the EU has positioned itself prominently as a stronghold for privacy and data protection.[20] The establishment of the GDPR was fuelled by the ambition to establish a "digital gold standard".[21] One important addition to this state-of-the-art framework is the requirement to carry out a Data Protection Impact Assessment (DPIA) as enshrined in Article 35 GDPR. "Although GDPR does not precisely specify the types of processing activities for which a DPIA would be necessary, through the guidelines that it provides, it is clear that the organization should conduct a DPIA if there is large scale processing of health (sensitive) data".[22] While Article 35 GDPR leaves the concrete implementation of a DPIA open, the benefits are obvious in the context of the EUDCC. DPIAs minimise risks to privacy, security and reputation, ensure compliance as well as the rule of law and enhance trust amongst data subjects and stakeholders.[23] There are several authoritative and practicable implementation models available, such as the "Standard Data Protection Model" provided by the German Conference of the Independent Data Protection Supervisory Authorities,[24] or the guidelines and corresponding methodology developed by the French Commission Nationale de l'Informatique et des Libertés (CNIL).[25] Regardless, the Commission chose to forego a DPIA, which disregards not only Article 35 GDPR, but also the substantively similar provision in Article 39 of Regulation (EU) 2018/1725 that is applicable to EU institutions themselves, as well as the associated principles of European data protection law.

However, according to Article 42 paragraph 2 of Regulation 2018/1725, the Commission has requested that the EDPB – a body that associates all DPIAs of Member States – and the EDPS provide an opinion on the proposal. These EU DPAs published a joint opinion on 31 March 2021.[26] This non-legally binding statement of fourteen pages is divided into sections with general comments, as well as more detailed remarks relating to: necessary categories of personal data, technical and organisational privacy and security measures, identification of controllers and processors, transparency and individual rights, data storage (retention) and, lastly, international data transfers. From the outset, the EDPB and EDPS make clear that

[20] G González Fuster, "The right to the protection of personal data and EU law" in G González Fuster (ed.), *The Emergence of Personal Data Protection as a Fundamental Right of the EU* (Berlin, Springer International Publishing 2014).

[21] G Buttarelli, "The EU GDPR as a clarion call for a new global digital gold standard" (2016) 6 International Data Privacy Law 77.

[22] D Georgiou and C Lambrinoudakis, "Data Protection Impact Assessment (DPIA) for cloud-based health organizations" (2021) 13 Future Internet 66, 1.

[23] ibid, 2.

[24] AK Technik of the Independent Data Protection Supervisory Authorities of the Federation and the Länder, "The standard data protection model – a method for data protection advising and controlling on the basis of uniform protection goals" (2020) Version 2.0b <https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf> (last accessed 22 May 2021).

[25] Commission Nationale de l'Informatique et des Libertés, "Privacy Impact Assessment (PIA)" <https://www.cnil.fr/en/privacy-impact-assessment-pia> (last accessed 22 May 2021).

[26] European Data Protection Board and European Data Protection Supervisor, supra, note 17, 6.

data protection does not represent an obstacle to fighting the pandemic, since trust is essential when enacting restrictive measures with the objective of containing the pandemic.[27] The lack of trust and legitimacy has also undermined the efficacy of data-driven measures to mitigate the impact of COVID-19 in South American countries,[28] to name just one example.

2. Inappropriateness of the governance framework

Unsurprisingly, the DPAs highlight that further alignment of the original Draft Regulation with the EU data protection framework is necessary, especially with a view to avoiding legal uncertainty.[29] They stress the principles of effectiveness, necessity and proportionality, which indicates that there is much left to be desired: "In particular, the Proposal should achieve a fair balance between the objectives of general interest pursued by the Digital Green Certificate and the individual interest in self-determination, as well as the respect for her/his fundamental rights to privacy, data protection and non-discrimination, and other fundamental freedoms, such as freedom of movement and residence".[30]

Indeed, if one reads the original Draft Regulation from beginning to end, it becomes evident that detailed principles, rules and safeguards are largely absent. This is particularly surprising when considering that the Commission chose a regulation instead of a directive, arguing that it "is the sole legal instrument ensuring the direct, immediate and common implementation of EU law in all Member States".[31] However, the original draft lacks the necessary quality and detail to effectively achieve immediate implementation of a EUDCC,[32] and therefore it cannot be considered an appropriate governance framework. Rather, it seems carefully drafted to do both: putting the EU Commission in the driver's seat of the political discourse, while at the same time remaining vague on what is/are the exact purpose(s) of the certificate,[33] let alone answering how these objectives will be operationalised from a technical and organisational perspective.

3. Lack of detailed provisions and safeguards

From the outset, it has been unclear when the certificate will be created. Recital 14, Article 5 paragraph 1 and Article 6 paragraph 1 of the original Draft Regulation state that "... Member States should issue the certificates making up the Digital Green Certificate automatically or upon request ...". The EDPB and EDPS recommend

[27] ibid, 6–14.

[28] TF Blauth and OJ Gstrein, "Data-driven measures to mitigate the impact of COVID-19 in South America: how do regional programmes compare to best practice?" (2021) 11(1) International Data Privacy Law 18–31.

[29] European Data Protection Board and European Data Protection Supervisor, supra, note 17, 5.

[30] ibid, 8.

[31] European Commission, "Proposal for 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)", supra, note 1, 5.

[32] European Data Protection Board and European Data Protection Supervisor, supra, note 17, 9–10.

[33] Gstrein et al, surpa, note 15, 25–26.

clarification of whether the EUDCC will be created automatically, upon request of the data subject, or whether it will only be issued upon request.[34] The updated draft contains in Article 3 paragraph 2 a requirement to issue the EUDCC ("shall issue") for Member States or designated bodies acting on their behalf. Additionally, Article 3 paragraph 2a of the updated draft states that a separate certificate shall be issued for each vaccination, test or recovery, which shall not contain data from previous certificates apart from specified exceptions.[35] While this seems to be a measure to protect "privacy by design", it remains to be seen whether the national systems and databases used to process and collect the data from the EUDCC will not be able to create a more comprehensive picture of the life of an individual.

Another critical aspect concerns the criteria outlined in Article 8 of the original Draft Regulation with the title "Technical specifications". The original draft contains only headlines, such as "issue a valid, secure and interoperable barcode". In recital 14 of the Draft Regulation, the Commission states that "Member States should issue the certificates making up the Digital Green Certificate in a digital or paper-based format, or both".[36] One might defend such an approach by referring to the tradition of principle-based regulation of technologies in the EU.[37] However, in the case of the EUDCC, the detailed technical specifications should not be developed on the basis of a broad list of carefully debated principles (eg think of Article 5 GDPR), but rather laid down with "implementing acts" created by experts from Member States and the Commission, without the involvement of legislators in Brussels, Strasbourg or national parliaments. The updated draft seems to have taken this criticism on board with some amendments to clarify the purpose and aim of Article 8,[38] as well as stating in recital 24 that updated technical guidelines of the EU eHealth network should form the basis of the preferred code standards.[39] Nevertheless, it is clear that the development and consistent application of high data protection standards will be a challenge for Member States if there is so little time to design and test their systems.

Turning to more fundamental issues, the DPAs seemed to doubt whether the Commission substantiated the proportionality of the proposal sufficiently and whether the EUDCC contains only the minimum information necessary to achieve the facilitation of free movement. Specifically, they highlight that Annex I of the original Draft Regulation sets out categories and data fields of the personal data to be processed within the framework, but the justification of the need for such specific data fields is not clearly explained.[40]

[34] European Data Protection Board and European Data Protection Supervisor, supra, note 17, 11.

[35] Presidency of the Council of the European Union, supra, note 18, 31–32.

[36] European Commission, "Proposal for 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)", supra, note 1, 12.

[37] CJ Hoofnagle, B van der Sloot and F Zuiderveen Borgesius, "The European Union General Data Protection Regulation: what it is and what it means" (2019) 28 Information & Communications Technology Law 65, 67.

[38] Presidency of the Council of the European Union, supra, note 18, 41–42.

[39] European Union eHealth Network, "Guidelines on verifiable vaccination certificates – basic interoperability elements" (2021) Release 2 <https://ec.europa.eu/health/sites/default/files/ehealth/docs/vaccination-proof_interoperability-guidelines_en.pdf> (last accessed 22 May 2021).

[40] European Data Protection Board and European Data Protection Supervisor, supra, note 17, 12.

This is concerning since the EUDCC has at least three purposes that will require it to be integrated into the respective national systems: containing sensitive information relating to the vaccination status of individuals, storing COVID-19 test results and certifying recovery. While the original draft leaves much to be desired in terms of substantive detail and clarity, it increases the power of the Commission considerably. Article 5 paragraph 2, Article 6 paragraph 2 and Article 7 paragraphs 1 and 2 of the original Draft Regulation empower it to adopt delegated acts by adding, modifying or removing data fields on the categories of personal data of the three types of certificates proving the status of vaccination, testing and recovery. Any such modification might invalidate a DPIA and require re-evaluation. Hence, the EDPB and EDPS suggest that only more detailed sub-categories of already defined data categories should be added through delegated acts, and that the authorities should again be consulted if this is planned.[41] Some of these concerns seem to be addressed in Article 9 of the updated draft, which states in paragraph 1 that EUDCC data "shall be processed only for the purpose of accessing and verifying the information included in the certificate in order to facilitate the exercise of the right of free movement within the Union during the COVID-19 pandemic". Article 9 paragraph 2 clarifies that only the personal data that are strictly necessary shall be collected.[42]

The EDPB and EDPS further recommended that the final regulation comes with a list of all entities acting as controllers, processors and recipients of the data in each individual Member State and that this list should be public. This also requires clarification of the role of the Commission in safeguarding interoperability between the different national systems.[43] That such basic requirements and clarifications were missing at the presentation of the original Draft Regulation once more demonstrates the lack of quality and detail. While the updated draft does not address this demand in detail, Article 9 paragraph 4 clarifies the situation somewhat by requiring that "authorities or other designated bodies responsible for issuing the certificates referred to in Article 3 shall be considered as controllers referred to in Article 4(7) of Regulation (EU) 2016/679".[44]

The more data collected, the more risk posted to information security. To mitigate this risk, detailed technical and organisational safeguards in line with Article 32 GDPR are necessary yet still missing from the original proposal. They could substantiate the principles of "privacy by design and default", as well as data minimisation. These principles should also be considered in the context of expiry dates for the validity of credentials. The certification of recovery (immunity) currently only expires after 180 days, but the authorities also recommend introducing similar expiration dates for the certification of vaccination and testing.[45] In this context, it is also worth

41 ibid, 13.

42 Presidency of the Council of the European Union, supra, note 18, 42.

43 European Data Protection Board and European Data Protection Supervisor, supra, note 17, 13.

44 Presidency of the Council of the European Union, supra, note 18, 43.

45 European Data Protection Board and European Data Protection Supervisor, supra, note 17, 12–13.

highlighting that the EU law enforcement agency Europol identified a high risk of forgery and illicit sale of false COVID-19 test certificates in February 2021.[46] Finally, the necessity for carefully considered technical and organisational safeguards has already become apparent with a leak of eight million datasets relating to COVID-19 test results in the Netherlands, which became public at the end of January 2021.[47] Dutch Law enforcement agencies report a stark rise of identity theft-related crime since the beginning of the pandemic.[48]

The updated draft seems much more considered in this regard. It mentions the risk of forgery of certificates in recitals 13, 13a, 14 and 14a, as well as in Article 4 that outlines the establishment of an EUDCC trust framework.[49] More attention to the authenticity of the certificates seems absolutely necessary, as a recent media investigation in Germany demonstrates. It came to the conclusion that forged vaccination certificates are already circulating and present a considerable risk to undermining the inoculation campaign.[50] These false and usually paper-based vaccine passports might continue to be an issue for some time even if the EUDCC trust framework manages to upgrade information security going forwards. Already circulating forgeries might be difficult to identify and be used to gain authentic EUDCCs.

The DPAs also flag the issue of international data flows and the digital autonomy (sovereignty) of national EUDCC systems. Recital 39 as well as Article 4 paragraph 2 of the original Draft Regulation seemed to enable data flows beyond EU Member States based on a "trust framework". The EDPB and EDPS concluded that such transfers imply an additional risk for the processing of personal data, as third countries could use the data for secondary purposes.[51] When it comes to the rapid implementation of data-driven measures to mitigate the impact of the pandemic (eg digital contact tracing apps), this issue of technological and organisational dependence is already well documented and deserves attention.[52] The updated draft seems to address this issue in Article 9 paragraph 6, where it clarifies that data from the EUDCC must not be processed outside the EU.[53]

---

[46] Europol, "Early warning notification – the illicit sales of false negative COVID-19 test certificates" (*Europol*, 1 February 2021) <https://www.europol.europa.eu/early-warning-notification-illicit-sales-of-false-negative-covid-19-test-certificates> (last accessed 22 May 2021).

[47] M van de Klundert and J Schellevis, "Lek in GGD-systeem al driekwart jaar aanwezig" (28 January 2021) <https://nos.nl/l/2366341> (last accessed 22 May 2021); T Sterling, "Personal data stolen from Dutch Coronavirus track-and-trace programme" (*Reuters*, 29 January 2021) <https://www.reuters.com/article/us-health-coronavirus-netherlands-datapr-idUSKBN29Y1H3> (last accessed 22 May 2021).

[48] B de Waal and S Tukker, "Opvallende stijging aangiftes van online fraude tijdens coronacrisis: 'Vooral kwetsbaren en ouderen zijn slachtoffer'" (*EenVandaag*, 29 April 2020) <https://eenvandaag.avrotros.nl/item/opvallende-stijging-aangiftes-van-online-fraude-tijdens-coronacrisis-vooral-kwetsbaren-en-ouderen/> (last accessed 22 May 2021).

[49] Presidency of the Council of the European Union, supra, note 18, 10–13, 34.

[50] M Dursun and C Saathof, "Corona-Impfung: Gefälschte Impfpässe werden zum Problem" (*tagesschau.de*, 11 May 2021) <https://www.tagesschau.de/investigativ/report-mainz/gefaelschte-impfpaesse-101.html> (last accessed 22 May 2021).

[51] European Data Protection Board and European Data Protection Supervisor, supra, note 17, 14.

[52] M Veale, "Sovereignty, privacy and contact tracing protocols" in L Taylor et al (eds), *Data Justice and COVID-19: Global Perspectives* (Meatspace Press 2020); Blauth and Gstrein, supra, note 28, 1.

[53] Presidency of the Council of the European Union, supra, note 18, 43.

4. Unclear exit strategy

Since the EUDCC is a measure in response to the current pandemic, one would expect that it would cease to exist once the pandemic is over. However, Article 15 paragraph 2 of the original Draft Regulation states that it will only be suspended upon declaration of the Director-General of the WHO that the public health emergency has ended. Paragraph 3 goes on to state that if the Director-General again should declare an emergency relating to "SARS-CoV-2, a variant thereof, or similar infectious diseases with epidemic potential", the EUDCC could be re-enacted by a delegated act. It seemed that the Commission did not want to be "caught unprepared" the next time it faces a similar situation, but that such a measure could be taken in absence of European or national legislators seems debatable at least. The EDPB and EDPS suggest the removal of this passage in their Joint Opinion so long as the scope of the provision is not limited to SARS-CoV-2 only.[54] The updated draft enshrines a much more careful regime, which limits the applicability of the framework to twelve months after it becomes effective, according to Article 15 paragraph 3.[55] Additionally, according to Article 14a, the EU Commission needs to present an evaluation report to the European Parliament and Council four months after the inception of the framework, as well as at least three months before the end of the period.[56]

Another concern is related to data retention. While the DPAs acknowledge that the Commission does not plan to establish a central database,[57] questions have emerged about the oversight of data storage at the national level. In addition, even if the EUDCC is suspended at the EU level, it might be possible that nation states will continue to use their respective systems, which might also contain data originating from other Member States. The question not only relates to how such data could be updated, revised or deleted. Even more concerning is a scenario where nation states adopt dedicated national laws to keep the systems originally intended for the EUDCC running and start to use them for other purposes such as national security. The updated draft addresses this issue in Article 9 paragraphs 3 and 3a,[58] but there is no comprehensive guarantee that one or more Member State(s) will not use the data from the EUDCC in other contexts based on national laws.

To illustrate this concern with two examples, as of January 2021, the police of Singapore can access data from digital contact tracing apps despite earlier government promises that this would never happen,[59] while police in Germany have used registration lists that were mandatory at restaurants during the summer of 2020 for criminal investigations.[60] Additionally, in the context of the EUDCC, the Austrian

[54] European Data Protection Board and European Data Protection Supervisor, supra, note 17, 10.

[55] Presidency of the Council of the European Union, supra, note 18, 48.

[56] ibid, 47.

[57] European Data Protection Board and European Data Protection Supervisor, supra, note 17, 8.

[58] Presidency of the Council of the European Union, supra, note 18, 43.

[59] M Sato, "Singapore's police now have access to contact tracing data | MIT Technology Review" (5 January 2021) <https://www.technologyreview.com/2021/01/05/1015734/singapore-contact-tracing-police-data-covid/> (last accessed 22 May 2021).

[60] F Keilani, B Reuter and F Abbas, "Polizei nutzt Kontaktdaten aus Restaurants auch zur Strafverfolgung" (31 July 2020) <https://www.tagesspiegel.de/politik/faelle-aus-fuenf-bundeslaendern-bekannt-polizei-nutzt-kontaktdaten-aus-restaurants-auch-zur-strafverfolgung/26056130.html> (last accessed 22 May 2021).

government has recently presented draft legislation that embeds the data of the certificate in a comprehensive database. This would link COVID-19-related health data to statistical data such as employment history and income, recent sick leave and education. The proposal for the creation of this database was heavily criticised by public institutions and civil society. The law is still under consideration.[61] Regardless of the outcome of this case, it clearly highlights that not only are the data that the certificate contains relevant, but also the infrastructures that will be used to process, store and analyse these data in the long term.

IV. Emergencies and infrastructures

From a data protection perspective, even the basic idea behind the establishment of a EUDCC is problematic, since it is based on an attempt to repurpose highly sensitive health data. As the Commission outlines at the beginning of the Explanatory Memorandum of the original Draft Regulation, the origin of the EUDCC lies in the attempts of Member States to keep vaccination certificates interoperable and standardised.[62] Certainly, some form of administrative registration on who has been vaccinated, when and how is necessary to coordinate the inoculation effort. However, when the repurposing of highly sensitive medical data is considered, severe privacy risks emerge.

The shortcomings outlined in the preceding section demonstrate that the original Draft Regulation is not an appropriate governance framework, being practically incapable of mitigating those severe risks. It is difficult to believe that the Commission was completely unaware of the shortcomings of the proposal, which require much more debate and consideration to fully address. Therefore, the suspicion emerges that the presentation of the draft was all about the "right timing". However, this bargain to gain control of the political process could come at significant cost, especially for the rights of EU citizens. This is why careful consideration of the intended purposes, identification of the data strictly necessary, effective remedies to protect rights and technical and organisational safeguards are so important. These aspects need to be considered from an early design stage, which is what DPIAs are meant to achieve. The fact that the WHO officially declared the pandemic more than a year ago renders arguments that "emergency reactions" are necessary to respond to the situation increasingly invalid.[63] Instead of focusing on preliminary measures, it is now time to strive for the establishment of best practices,[64] some of which the EU has developed itself in the area of data protection.

[61] Der Standard, "Sozialversicherungen, Elga und Gemeindebund gegen geplante Superdatenbank" (*DER STANDARD*, 20 May 2021) <https://www.derstandard.at/story/2000126791029/gruener-pass-sozialversicherungstraeger-lehnen-geplante-datensammlung-ab> (last accessed 22 May 2021).

[62] European Commission, "Proposal for 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)", supra, note 1, 2.

[63] Gstrein et al, supra, note 15, 15–16.

[64] For a detailed account of the global reaction to the COVID pandemic see, eg, J Grogan, "Introduction & list of country reports" (*Verfassungsblog*, 2020) <https://intr2dok.vifa-recht.de/receive/mir_mods_00008563> (last accessed 22 May 2021).

At the time of writing, it seems that the trialogue negotiations between the European Parliament, the Council and the Commission have addressed some of the most worrisome issues of the original proposal. Regardless, the Commission and the Member States seem to have decided to establish a general-purpose infrastructure, one that will evoke all kinds of undesirable societal side effects. The risks of enabling cybercrime (eg identity theft), enhanced social control and repurposing of health data for national security have already been described in the previous section, but another scenario is also imaginable: besides what each individual's EUDCC will actively state, highly sensitive personal information could be inferred when combining these certificates with information about the relatively slow progress of inoculation efforts in the coming months in different Member States, together with the priorities of vaccination campaigns. In cases where a (relatively young) person with proof of vaccination is able to spend a summer vacation in Austria, Greece or any other Member State, while others in the same (age) category are not entitled to do so, it is relatively easy to infer whether the visitor has a sensitive health condition.[65] Alternatively, others around this person might feel inspired to all kinds of speculation, such as whether they found a way to "jump the queue".

In conclusion, it is clear that the original Draft Regulation was presented with significant flaws not addressing many concerns related to data protection. Since the Commission does not "practice what it preaches", this undermines the credibility of those European standards that it has fought for over the last decade all over the world. At the same time, the EUDCC might transform into a general-purpose infrastructure that will keep privacy advocates busy for years to come, as policymakers will attempt to reuse it in all kinds of contexts.

[65] I Cofone, "Immunity passports and contact tracing surveillance" (2021) 24 Stanford Technology Law Review 31–34.