UNIWERSYTET ZIELONOGÓRSKI

DYSKURS PRAWNICZY I ADMINISTRACYJNY 4/2022 ISSN 2657-926X

Antoni Napieralski
University of Vienna
ORCID 0000-0002-0576-0733
antoni.napieralski@univie.ac.at

EU Digital COVID Certificate and Data Protection. The Case of Poland and Austria

Keywords: EU Digital COVID Certificate, personal data, GDPR, Poland, Austria

Summary. The EU Digital COVID Certificate was introduced as a technological promise of a smooth exit from the pandemic. At the same time, due to the scope of the data processed, it interacts with the European system of personal data protection law. The EU Digital COVID Certificate is designed to function for two different purposes: to facilitate border crossings during a pandemic and for domestic purposes as defined by the Member States. Given the degree of discretion left to Member States in the implementation of the EU COVID Digital Certificates, a comparative analysis is necessary. The key issue that is visible in both Polish and Austrian implementation of the EU Digital COVID Certificate is the question of determining the controller of the processed personal data. The difficulty of both countries' authorities to determine the controller in decentralised infrastructures of personal data processing is clearly visible here. Specifically, it is problematic to identify the controller in relation to mobile applications that locally store a copy of the EU Digital COVID Certificate and display it on demand.

Unijne cyfrowe zaświadczenie COVID i ochrona danych. Przypadek Polski i Austrii

Słowa kluczowe: unijne cyfrowe zaświadczenie COVID, UCC, dane osobowe, RODO, Polska, Austria

Streszczenie. Unijne cyfrowe zaświadczenie COVID zostało wprowadzone jako technologiczna obietnica sprawnego wyjścia z pandemii. Jednocześnie, ze względu na zakres przetwarzanych danych, wchodzi ono w interakcję z europejskim systemem prawa ochrony danych osobowych. Unijne cyfrowe zaświadczenie COVID przewidziane jest do funkcjonowania w dwóch różnych celach: ułatwienia przekraczania granic w czasie pandemii oraz w celach wewnątrzkrajowych, zdefiniowanych przez państwa członkowskie. Biorąc pod uwagę zakres swobody decyzyjnej pozostawionej państwom członkowskim w implementacji unijnych cyfrowych zaświadczeń COVID, niezbędna jest analiza porównawcza. Kluczową kwestią, która została uwidoczniona w zarówno polskiej, jak i austriackiej implementacji unijnego cyfrowego zaświadczenia COVID, jest określenie administratora przetwarzanych danych osobowych. Wyraźnie widoczna jest tu trudność organów obu państw w określeniu administratora w zdecentralizowanych infrastrukturach przetwarzania danych osobowych. Szczególnie problematyczne jest określenie administratora w odniesieniu do aplikacji mobilnych umożliwiających lokalne przechowywanie kopii unijnego cyfrowego zaświadczenia COVID i jej wyświetlanie na żądanie.

1. Introduction

The European Commission in its report on the application of Regulation 2021/953 (hereinafter: EDCC Regulation)[1] states that the EU digital COVID certificate is an example of „guaranteeing data protection and security, maintaining the core value of human-centricity during the digital transition, and remaining open to the world"[2]. Drawing from this assessment, the purpose of the following paper is to analyse the data protection implications of the European Digital COVID Certificate (hereinafter EDCC). In particular, the national implementations of the EDCC in Poland and Austria are analysed.

The comparison of Polish and Austrian implementation is dictated, among other things, by the desire to test the practical aspects of implementing EU legal and technological standards on domestic grounds. Moreover, an interesting aspect of the comparison seems to be the different degree of use of EDCC certificates for domestic purposes (e.g. access control to cultural institutions, catering, service premises, etc.). While Poland has still not decided to impose the domestic use of EDCC certificates, Austria has been using them for a long time, in various configurations (3G, 2.5G, 2G, 2G+)[3].

The analysis of national implementations of the EDCC highlights the complex issue of delineating the material scopes of the EDCC Regulation and national legal orders allowing the use of the EDCC for purposes other than crossing borders. Accordingly, the following article distinguishes between cross-border and domestic fields of application of the EDCC (cf. Parts 2 and 3 and 4).

2. EU Digital COVID Certificate (EDCC)

EDCCs are defined as „interoperable certificates containing information about the vaccination, test result or recovery of the holder issued in the context of the

[1] 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, OJ L 211/1, 2021 (hereinafter: Regulation 2021/953).

[2] Commission, *Report from the Commission to the European Parliament and the Council pursuant to Article 16(1) of Regulation (EU) 2021/953 of the European Parliament and of the Council 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*, 18.10.2021, p. 5.

[3] See Stadt Wien, *Derzeit gültige Corona-Regeln*, https://coronavirus.wien.gv.at/oeffentliches-leben/ [access: 30.11.2021].

COVID-19 pandemic"[4]. Due to its personal scope, the EDCC was introduced via two legal acts, as to distinguish between the EU citizens and third-country nationals residing legally in the EU[5]. However, irregular migrants in the EU are excluded from the personal scope of the EDCC.

The EDCC is available in three versions, i.e. as a vaccination, a test result or a recovery certificate[6]. The certificate is available in both paper and electronic versions[7]. The data fields on an EDCC are standardised and can be divided into the following three categories: (i) data on EDCC's holder's identity, (ii) data on vaccination / test / SARS-CoV-2 infection and (iii) EDCC's metadata (np. issuing authority, unique identifier[8]. Using the vaccination certificate as an example, these are:

a) name: surname(s) and forename(s), in that order;
b) date of birth;
c) disease or agent targeted: COVID-19 (SARS-CoV-2 or one of its variants);
d) COVID-19 vaccine or prophylaxis;
e) COVID-19 vaccine product name;
f) COVID-19 vaccine marketing authorisation holder or manufacturer;
g) number in a series of doses as well as the overall number of doses in the series;
h) date of vaccination, indicating the date of the latest dose received;
i) Member State or third country in which the vaccine was administered;
j) certificate issuer;
k) unique certificate identifier[9].

This data is stored in the QR code included in each EDCC certificate. Sample QR codes for each country are available on the GitHub platform together with the corresponding schemes in .json format[10]. Analysing the structure of QR codes, one can see the difference between the range of data displayed during the verification of the EDCC certificate and the actual range of data stored in the QR code.

From the perspective of data protection legislation, it should be noted that in the case of EDCC certificates, a special category of personal data is involved, i.e. data

---

4 Art. 2(2) Regulation 2021/953.

5 Regulation 2021/953; Regulation (EU) 2021/954 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) with regard to third-country nationals legally staying or residing in the territories of Member States during the COVID-19 pandemic, OJ L 211/24, 2021.

6 Art. 3(1) Regulation 2021/953.

7 Art. 3(2) Regulation 2021/953.

8 Art. 5(2), art. 6(2), art. 7(2) Regulation 2021/953.

9 Annex to the Regulation 2021/953.

10 https://github.com/eu-digital-green-certificates/dgc-testdata [access: 30.11.2021].

concerning health[11]. This implies additional obligations on the controller, such as the need to indicate the legal basis for the processing also from Article 9(2) of the GDPR or the high likelihood of the need for a data protection impact assessment[12].

For personal data processed under the EDCC Regulation and within the scope of its Article 1, a single legal basis for processing within the meaning of the GDPR is defined. Article 1 and Recital 48 of the EDCC Regulation establish the EDCC Regulation itself as the legal basis for processing within the meaning of Article 6(1)(c) and Article 9(2)(g) of the GDPR. Following a literal interpretation of Article 1 and Recital 48 of the EDCC Regulation, it should be assumed that the issue of a legal ground for processing is comprehensively regulated here, covering all stages of the EDCC life cycle and therefore does not require additional legal grounds at national level. According to Article 10(6) of the EDCC Regulation, authorities issuing the EDCC are also the controllers of data processed within the material scope of the EDCC Regulation[13]. The national issuing authorities are responsible for the whole life-cycle of the EDCCs that they issued[14]. This includes issuing, verifying, recognising and erasure of the EDCCs.

The EDCC is a time-limited instrument. According to Article 17 of the EDCC Regulation, it shall apply from 1.07.2021 to 30.06.2022. However, it should be underlined that, in accordance with Article 16, the Commission may propose an extension of this period depending on the future epidemiological situation[15]. This is an interesting example of linking the scope of a legal act to the current state of scientific knowledge. It is not clear what the procedures are for extinguishing infrastructures created under the EDCC Regulation. According to Article 10(4) of the EDCC Regulation, personal data collected will have to be deleted, but the question of the infrastructure itself remains open[16].

An important element of the EDCC is its interoperability at Union level, allowing cross-border verification of certificates[17]. The cross-border use of EDCC, i.e. the

[11] See European Data Protection Board-European Data Protection Supervisor, *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)*, 31.03.2021, para 34; O.J. Gstrein, *The EU Digital COVID Certificate: A preliminary data protection impact assessment*, "European Journal of Risk Regulation" 2021, vol. 12, iss. 2, p. 10.

[12] Art. 35(3)(b) GDPR.

[13] Art. 10(6) Regulation 2021/953.

[14] Recital 54 Regulation 2021/953.

[15] Art. 16 Regulation 2021/953.

[16] See O.J. Gstrein, *op. cit.*, p. 9.

[17] See art. 2(7) Regulation 2021/953: "interoperability" means the capability of verifying systems in a Member State to use data encoded by another Member State.

effective verification of EDCC from country A in country B is the main purpose for which EDCC was introduced. In the case of cross-border use of EDCC, the electronic seal authenticating the EDCC in question shall be verified[18]. Verification is in two steps, first against the provided public key[19]. Then it is checked if the indicated public key is present in the repository of trusted public keys[20]. Only after verification in this way can the application (locally) read the data contained in the QR code of a specific certificate[21].

The EDCC infrastructure is developed on the basis of existing EU-level mechanisms of the so-called eHealth network. The eHealth Network was established by Article 14 of Directive 2011/24/EU on the application of patients' rights in cross-border healthcare[22]. The aim of the eHealth Network is to support technological progress in cross-border healthcare and cross-border research[23]. The eHealth Network provides technical support for the EDCC, in particular regarding mutual recognition mechanisms and interoperability of certificates at EU level. The experts of the eHealth Network have developed technical documentation specifying how the EDCC will operate, implicitly also defining the scope and the way in which personal data will be processed[24]. The following graphic illustrates the cross-border functioning of EDCC certificates:

---

[18] Art. 2(9) Regulation 2021/953: 'electronic seal' means electronic seal as defined in point (25) of Article 3 of Regulation (EU) No 910/2014.

[19] eHealth Network, *Interoperability of health certificates. Trust framework, V.1.0*, 3.12.2021 r., p. 15.

[20] *Ibidem*.

[21] *Ibidem*.

[22] 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 L88, 2011.

[23] Art. 14(2) Directive 2011/24/EU.

[24] eHealth Network, *Guidelines on Technical Specifications for Digital Green Certificates. Volume 1, V1.0.5*, 21.04.2021 r.; eHealth Network, *Guidelines on Technical Specifications for Digital Green Certificates. Volume 2 European Digital Green Certificate Gateway, V1.3*, 21.04.2021 r.; eHealth Network, *Guidelines on Technical Specifications for Digital Green Certificates. Volume 3 Interoperable 2D Code, V1.3*, 21.04.2021 r.; eHealth Network, *Guidelines on Technical Specifications for Digital Green Certificates. Volume 4 European Digital Green Certificate Applications, V1.3*, 21.04.2021 r.; eHealth Network, *DCC Anomaly Capture Process for COVID Certificate Data. Best current practice, V1.01*, 15.09.2021 r.; eHealth Network, *Guidelines on Value Sets for EU Digital COVID Certificates, V1.4*, 13.10.2021 r.; eHealth Network, *Interoperability of health certificates. Trust framework, V.1.0*...; eHealth Network, *Guidelines on Technical Specifications for Digital Green Certificates. Volume 5 Public Key Certificate Governance, V1.02*, 5.12.2021.

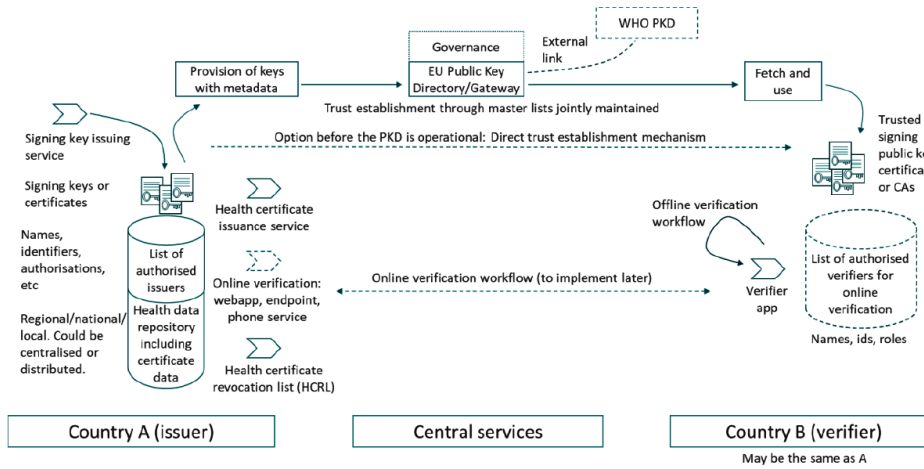

Figure 1. Overall architecture of the system
— first version of the trust framework specifications
--- future version of the trust framework specifications
Source: eHealth Network, Interoperability of health certificates. Trust framework, V.1.0.[25]

As can be seen in the graphic above, the only element of the EDCC certificate that is subject to international exchange is the public key. This is done via a central gateway operating under the auspices of the European Commission (EU Public Key Directory/Gateway). Personal data contained in the EDCC certificate are not exchanged between countries[26]. Therefore, the issues of the legal basis for the processing of personal data or of the controller defined in the EDCC Regulation only apply when the EDCC is used for the purpose specified in Article 1 of the EDCC Regulation. The first, defined by the EDCC Regulation and at the same time setting its limits, is to facilitate the exercise of the right to free movement within the EU during the COVID-19 pandemic[27]. For applications outside this material scope, the question of the legal basis of the processing and the liability for the data processed remains open.

A second field of application of the EDCC, outside the material scope of the EDCC Regulation, is national applications not related to the right of free move-

[25] eHealth Network, *Interoperability of health certificates. Trust framework, V.1.0...*, p. 8.
[26] Art. 1 Regulation 2021/953.
[27] *Ibidem*: This Regulation lays down a framework for the issuance, verification and acceptance of interoperable COVID-19 vaccination, test and recovery certificates (EU Digital COVID Certificate) for the purpose of facilitating the holders' exercise of their right to free movement during the COVID-19 pandemic. This Regulation shall also contribute to facilitating the gradual lifting of restrictions to free movement put in place by the Member States, in accordance with Union law, to limit the spread of SARS-CoV-2, in a coordinated manner.

ment[28]. These include, for example, national restrictions on admission to cultural institutions and on the use of service and catering outlets. The determination of the objectives for the national application of the EDCC remains solely within the competence of the Member States[29].

Neither Poland nor Austria have chosen to set up separate infrastructures for the two possible fields of application of EDCCs, i.e. cross-border use and domestic use. Such a decision would contradict Recital 49 of the EDCC Regulation, which requires that where a domestic system is established, the foreign EDCCs should be recognised without the need for a parallel domestic EDCC[30].

This is an example of an interesting method of regulation, i.e. regulation outside the material scope by means of a forced shape of the data processing infrastructure[31]. This method can be briefly described as follows. EU legislation sets up infrastructures to handle tasks that fall within its scope. In the case of the EDCC, this is the cross-border aspect of the EDCC enabling the freedom of movement of persons in the era of the COVID-19 pandemic[32]. At the same time, so-called domestic opening-clauses allow Member States to use the same infrastructure for national purposes outside the material scope of the EDCC Regulation and even beyond the scope of EU law. The final step of this regulatory method is the requirement in the EDCC Regulation that national infrastructure must be capable of handling foreign EDCCs, without the need for parallel national certificates.

In this way, the shape of the key elements of the national infrastructure serving national EDCC application fields is determined by EU legislation. We are mainly talking about the shape of the certificate itself, the categories of data processed, the verification method and the data storage model. Furthermore, the EDCC Regulation defines the qualitative requirements that national legislation has to meet. According to Recital 48 of the EDCC Regulation, national legislation must: (i) comply with EU data protection law, (ii) comply with the principles of effectiveness, necessity and proportionality, (iii) clearly define the scope of the processing, the specific purpose and the categories of entities that can verify the certificate, (iv) include adequate safeguards against abuse and discrimination,

---

28 Recital 48 Regulation 2021/953.

29 *Ibidem*.

30 Recital 49 Regulation 2021/953: Where a Member State has adopted or adopts, on the basis of national law, a system of COVID-19 certificates for domestic purposes, it should ensure for the period of application of this Regulation that certificates making up the EU Digital COVID Certificate can also be used and are also accepted for domestic purposes, in order to avoid that persons travelling to another Member State and using the EU Digital COVID Certificate are obliged to obtain an additional national COVID-19 certificate.

31 See T. Streinz, *The Evolution of European Data Law*, [in:] P. Craig, G. de Búrca (eds.), *The Evolution of EU Law*, OUP 2021, p. 48.

32 Art. 1 Regulation 2021/953.

(v) if the EDCC applies to non-medical purposes then personal data processed during the verification of the certificate must not be retained[33].

When analysing national implementations of EDCC, the following elements of the national infrastructure can be distinguished:

– a national ICT system that issues EDCCs based on national registers of vaccinations, tests or recoveries (Polish P1 or Austrian EPI-Service)[34],
– national applications that store a copy of the EDCC and display it on request (e.g. the Polish IKP, mojeIKP, mObywatel or the Austrian Grüner Pass App)[35],
– national mobile applications for EDCC verification (Polish Skaner Certyfikatów COVID or Austrian GreenCheck)[36].

In addition, the role of national systems acting as a source of data on the basis of which the EDCC is issued should be emphasized, e.g. national vaccination registers.

The following analysis of the Austrian and Polish implementation is carried out taking into account the division into the above mentioned elements.

3. Austrian implementation of the EDCC

The Austrian implementation of EDCC, like the Polish one (cf. section 4 below), consists of three main components: the EPI-Service platform acting as issuer of EDCC certificates, the Grüner Pass mobile application storing and displaying a local copy of EDCC on demand, and the GreenCheck mobile application for verification of EDCC certificates.

National data sources are laboratories (for tests), the EMS system supported by a national patient index (for recoveries)[37] and the Impfregister (for vaccinations)[38]. All this information flows into the EPI-Service platform, which generates the EDCC certificates in accordance with the requirements defined in the EDCC Regulation[39]. The certificates are then available both electronically via the elec-

[33] Recital 48 Regulation 2021/953.

[34] Art. 7(1) ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2011 r., Nr 113, poz. 657); §4b (3) Epidemiegesetz 1950 (EpiG) StF: BGBl. Nr. 186/1950.

[35] https://pacjent.gov.pl; https://www.gov.pl/web/mobywatel; https://gruenerpass.gv.at/ [access: 30.11.2021].

[36] https://pacjent.gov.pl/aktualnosc/sprawdz-unijny-certyfikat-covid; https://greencheck.gv.at/ [access: 30.11.2021].

[37] The EMS (Epidemiologische Meldesystem) is a register of notifiable communicable diseases shared by district administrative authorities (Bezirksverwaltungsbehörden), regional health directorates (Landessanitätsdirektionen), the Federal Minister of Health and the Austrian Agency for Health and Food Safety (AGES); see § 4 EpiG.

[38] https://www.gesundheit.gv.at/service/gruener-pass/datenschutzinformation [access: 30.11.2021].

[39] § 4b EpiG; https://www.gesundheit.gv.at/service/gruener-pass/datenschutzinformation [access: 30.11.2021].

tronic vaccination register (e-Impfpass, available via ELGA)[40], as well as in paper format. The electronic version of the EDCC certificate is available for download on the Grüner Pass mobile app.

An element of the Austrian implementation of the EDCC that should be assessed critically is the definition of roles in the sense of the GDPR, i.e. in particular the designation of controllers for the individual components of the implementation. The effect achieved is at least unclear for data subjects. Suffice it to say that the data protection impact assessment conducted for the Austrian implementation does not identify any controller[41].

The controller of the data processed for the issuance and provision of EDCC certificates within the EPI-Service is the Federal Minister of Health[42]. As far as the transmission of test results and information on vaccinations administered to the EPI-Service platform (national data sources) is concerned, there is a co-administration relationship between the Federal Minister of Health and (respectively) laboratories or vaccination centres[43].

National legislation has identified a number of entities that are authorised to download EDCC certificates from the EPI-Service platform in order to make them directly available to EDCC holders[44]. Importantly, all of these entities have been identified as parallel controllers (not joint controllers) to the extent that they have access to download data from the EPI-Service. These are the provincial premiers (Landeshauptleute), municipalities (Gemeinden), district administrative bodies (Bezirksverwaltungsbehörden), the ombudsman offices of the ELGA system (ELGA-Ombudsstelle), the customer service centres of the Austrian health insurance fund (Kundenservicestellen der Österreichischen Gesundheitskasse) and doctors and physicians in private practice (niedergelassene Ärztinnen und Ärzte)[45]. Considering the number of entities involved as controllers, one can see the absurdity of such a model of responsibility for the processed data. There is a tendency to label every user of the system as controller.

With regard to the Grüner Pass mobile app, no controller is indicated, either in the legislation or in the privacy policy of the app itself. The provider of the app is the Federal Ministry of Health and the Federal Centre for Computing

[40] https://www.elga.gv.at/e-impfpass/e-impfpass/ [access: 30.11.2021].

[41] *Datenschutz-Folgenabschätzung zum Grünen Pass und zum EPI-Service*, https://www.gesundheit.gv.at/service/gruener-pass/datenschutz-folgenabschaetzung [access: 30.11.2021].

[42] § 4b(3) EpiG.

[43] § 4c(3) EpiG; § 24c(3a) Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verarbeitung elektronischer Gesundheitsdaten und genetischer Daten (Gesundheitstelematikgesetz 2012 – GTelG 2012) StF: BGBl. I Nr. 111/2012.

[44] § 4b EpiG.

[45] *Ibidem*.

(Bundesrechenzentrum, BRZ)[46]. Despite this, the privacy policy, dispensing with the identity of the controller in silence, indicates instead that both the Minister and BRZ are not data controllers (sic!)[47]. The designation of non-controllers is not a practice prescribed by law and should be criticised.

According to the documentation, the argument for refusing to name the controller of the Grüner Pass mobile app is that, as personal data is stored locally on the EDCC holder's smartphone, neither BRZ nor the Federal Minister of Health processes personal data[48]. This argument is not convincing under the definition of controller in the GDPR. According to Article 4(7) GDPR, the controller's role may derive either from a provision of law (EU or national) or from a de facto power to define the purposes and means of the processing of specific personal data[49]. This definition leads to two conclusions relevant to the Grüner Pass application.

First, the GDPR provisions do not provide for the possibility to negatively define a controller, i.e. to determine who is not a controller. This type of definition cannot have legal effects and remains unaffected by the actual assignment of the controller role. Second, in the absence of a statutory attribution of the role of controller, the only rule that remains available is the rule on the power to define the purposes and means of processing certain personal data[50].

Following this line of reasoning, it can be seen that although the data are stored locally on the EDCC holder's device, both the purpose of their processing (verification of EDCC status and verification of the authenticity of the EDCC certificate) and the means of their processing (specification and functionalities of the mobile application) remain under the control of state authorities. The tendency, evident in the privacy policy of the Grüner Pass application, to place the sole responsibility for the processing of personal data on the data subject, i.e. the EDCC holder, is close to the concept of circumvention of the law[51]. This is particularly evident in the case of liability for data breaches resulting from security gaps in the application and/or lack of adequate security updates. The design of application security features remains under the direct control of application developers and providers and beyond the control of the average user. In this situation, it is impossible to

[46] Para 5.1, https://gruenerpass.gv.at/app/datenschutz/ [access: 30.11.2021].

[47] Para 8, https://gruenerpass.gv.at/app/datenschutz/ [access: 30.11.2021].

[48] Para 8, https://gruenerpass.gv.at/app/datenschutz/ [access: 30.11.2021].

[49] Art. 4(7) GDPR: 'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

[50] Art. 4(7) GDPR.

[51] Para 8, https://gruenerpass.gv.at/app/datenschutz/ [access: 30.11.2021]: Die Anbieter haben keinerlei Kontrolle darüber, für welche Zwecke der Nutzer seine eigenen, in der App gespeicherten Daten verwenden wird.

exclude the application provider's liability under the GDPR solely based on the argument of a decentralised data storage model.

As a side note, one should ask why, despite disavowing the role of a controller, the federal minister responsible for health felt obliged to prepare a privacy policy for the Grüner App, thus fulfilling the controller's obligation under Article 13/14 GDPR.

Two categories of personal data have been defined for the GreenCheck application for the verification of EDCC certificates, for which two groups of different controllers have been assigned. First, data read from the QR code contained in the EDCC certificate to verify its authenticity and the identity of the holder[52]. The privacy policy is limited to indicating the data displayed on the screen of the verifying device, i.e. the name, surname and date of birth of the EDCC holder and feedback on the validity of the EDCC certificate itself (valid/invalid/verification error). Other data contained in the QR code of the EDCC certificate that can be read at the same time are omitted.

The provider of the GreenCheck application, IT-Services der Sozialversicherung GmbH (ITSV, IT subcontractor of the public social security sector), has prepared a blank privacy policy allowing each person verifying EDCC with the GreenCheck application to be entered as the controller of the data processed[53]. As in the case of the Grüner Pass app, there is a clear trend to exclude the liability of public institutions (app providers) under the GDPR. This is a contradictory constellation, according to which the controller is each user of the GreenCheck application (verifier, e.g. restaurant, cinema, theatre), at the same time processing personal data on the basis of the legal basis imposed by the application provider (Article 6(1)(c) and Article 9(2)(i) GDPR) and with the help of tools on the shape of which it has no influence.

As an aside, it is important to emphasise the rather broad spectrum of possible complications associated with the use of private devices by employees of restaurants, cinemas or theatres to verify EDCC certificates using GreenCheck. In such a situation, the possible distribution of liability under THE GDPR becomes even more complicated.

Secondly, telemetry data generated during the update of the list of trusted public keys – the GreenCheck application requires an update at least every 48 hours in order to function properly[54]. Due to the verification method (offline, the list of trusted public keys is stored on the verification device) a regular update of the list

[52] https://www.itsv.at/cdscontent/load?contentid=10008.748781&version=1623920316 [access: 30.11.2021].

[53] *Ibidem*.

[54] https://www.itsv.at/cdscontent/load?contentid=10008.751477 [access: 30.11.2021].

of trusted public keys is necessary. The telemetry data indicated above includes: the IP address of the device sending the request to update the list of keys, the time of the update, and the data of the device (including the operating system and its version)[55]. With regard to the processing of this category of data, the designated controller is the Federal Minister responsible for health[56]. Article 6(1)(f) of the GDPR was indicated as the legal basis for the processing[57].

Unlike Poland, Austria decided to carry out a data protection impact assessment for the national implementation of the EDCC as required by the GDPR[58]. Such an obligation arises from Article 35(3)(b) of the GDPR. However, the GreenCheck application was excluded from the Austrian assessment. The assessment identified three categories of risks:

– intangible damage, breach of professional secrecy, discrimination through knowledge or other unauthorised processing of personal data by third parties (risk 1),
– identity theft (risk 2),
– unauthorised undermining of pseudonymisation (risk 3)[59].

These risks were assessed as low (risk 2) and medium (risks 1 and 3)[60].

4. Polish implementation of the EDCC

In Poland, EDCCs are issued in a centralized manner using the Electronic Platform for Collection, Analysis and Sharing of Digital Medical Records (e-health system, P1)[61]. One of the modules of the P1 system is used for centralised issuing of EDCC certificates in Poland, both in the form of certificates of vaccination and certificates of negative test and recovery[62]. In the context of the Polish implementation of EDCC, the P1 system has a dual function. In addition to issuing EDCC certificates, the P1 system is also a national data source for vaccination certificates.

For the purposes of test and recovery certification, the EWP (Entry to Poland Record) system is the national data source. The EWP functions on the basis of ref-

[55] *Ibidem*.
[56] *Ibidem*.
[57] *Ibidem*.
[58] *Datenschutz-Folgenabschätzung zum Grünen Pass und zum EPI-Service*, https://www.gesundheit.gv.at/service/gruener-pass/datenschutz-folgenabschaetzung [access: 30.11.2021].
[59] *Ibidem*, p. 24.
[60] *Ibidem*, p. 25.
[61] See art. 7(1) ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2011 r., Nr 113, poz. 657).
[62] See https://www.gov.pl/web/mobywatel/unijny-certyfikat-covid [access: 30.11.2021].

erences in sub-legislative acts[63]. The role of the EWP is (inter alia) to process data on imposed quarantine, isolation, testing for SARS-CoV-2, and persons infected with SARS-CoV-2, including those who died due to infection[64]. According to the Chief Sanitary Inspector, recovery status is generated from the EWP for any person who "has a positive PCR test result entered in the EWP for which 11 days have already passed since the result was obtained, but 180 days have not passed"[65].

Electronic access to issued EDCC certificates is possible via the IKP application as a module of the P1 system[66]. Via the IKP web application the EDCC certificate can be downloaded to the phone and displayed on demand in the mojeIKP application or in the mObywatel application[67]. Verification of the authenticity of the EDCC is carried out using a dedicated application Skaner Certyfikatów COVID[68].

The Polish implementation of the EDCC does not distinguish between data processing resulting directly from the EDCC Regulation (cross-border applications) and from national provisions (domestic applications). In particular, there is no such distinction in the privacy policies of the individual components of the Polish implementation. Therefore, it should be assumed that the indicated legal basis of processing, the scope of processed data and data controllers refer to domestic, not cross-border applications.

For all components of the Polish implementation of the EDCC, a single controller was identified, i.e. the Minister of Health[69]. This solution is consistent with the letter of the EDCC Regulation, which places the role of controller on the authorities and bodies responsible for issuing EDCC certificates[70].

Unlike Austria, Poland has chosen to treat the mobile application as an "extension" of the national system issuing EDCC certificates. At the level of privacy policies, there is no distinction between the components of the P1 system responsible for issuing EDCCs and the mojeIKP mobile application used to store a local copy

---

[63] § 2(3)(1) Rozporządzenia Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii, [in:] Dz.U. z 2020 r. poz. 491; § 2 ust. 4 pkt 1 Rozporządzenia Rady Ministrów z dnia 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, [in:] Dz.U. z 2021 r. poz. 861.

[64] § 2(5) Rozporządzenia Rady Ministrów z dnia 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii.

[65] https://www.gov.pl/web/psse-lodz/informacje-o-generowaniu-certyfikatu-ucc [access: 30.11.2021].

[66] Art. 7a ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2011 r., Nr 113, poz. 657); see https://pacjent.gov.pl/polityka-prywatnosci [access: 30.11.2021].

[67] https://pacjent.gov.pl/; https://play.google.com/store/apps/details?id=pl.gov.cez.mojeikp; https://play.google.com/store/apps/details?id=pl.nask.mobywatel&hl=pl&gl=US [access: 30.11.2021].

[68] https://play.google.com/store/apps/details?id=pl.gov.cez.sws&hl=pl&gl=US&showAllReviews=true [access: 30.11.2021].

[69] https://pacjent.gov.pl/polityka-prywatnosci; https://ezdrowie.gov.pl/portal/home/polityka-prywatnosci-ucc; brak jednoznacznego wskazania w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2011 r., Nr 113, poz. 657) [access: 30.11.2021].

[70] Art. 10 ust. 6 Regulation 2021/953.

of the EDCC on the EDCC holder's device[71]. Similarly, there is no distinction in terms of controllers and legal basis of processing between the P1 system and the mojeIKP mobile application. In both cases, the controller is the Minister of Health and the legal basis for processing is Article 9(2)(h) GDPR in conjunction with the act of 28 April 2011 on the healthcare information system[72].

Analysing the mojeIKP application, it can be seen that, in contrast to Austrian institutions (cf. part 3. above), the Minister of Health was not afraid to take responsibility for data processed in a decentralised model, i.e. on EDCC holders' devices. This decision should be viewed positively as being in line with the definition of controller set out in Article 4(7) of the GDPR, i.e. an entity with the authority to determine the purposes and means of processing certain personal data.

The solution of the controller problem in the case of the mObywatel application, which also enables local storage of the EDCC certificate, should be assessed critically. In principle, the controller of the data processed in the mObywatel application is the minister competent for digitisation[73]. However, the privacy policy of the mObywatel application indicates that the controller of the data downloaded from the P1 system for the purpose of operating the EDCC and processed in the mObywatel application is (still) the Minister of Health[74].

The demarcation of responsibilities between the minister responsible for digitalisation and the Minister of Health is unclear in this case. Considering the exclusive control exercised by the minister responsible for digitisation over the infrastructure (the shape of the mObywatel application, IT security mechanisms used), it is reasonable to ask whether this is not an example of data co-management[75]. The relationship of co-management may occur in this case between the Minister responsible for digitization who determines the way of data processing (i.e. the shape and parameters of the mObywatel application) and the Minister of Health (the EDCC data provider). Otherwise, in the case of e.g. a data protection breach, the demarcation of responsibility will remain unclear, to say the least.

In accordance with the privacy policy of the P1 system, the legal basis for the processing of personal data for EDCC purposes is the act of 28 April 2011 on the healthcare information system, in conjunction with Article 9(2)(h) of the GDPR[76].

---

[71] https://pacjent.gov.pl/polityka-prywatnosci [access: 30.11.2021].

[72] *Ibidem*; ustawa z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia (Dz.U. z 2011 r., Nr 113, poz. 657).

[73] https://www.gov.pl/web/mobywatel/polityka-prywatnosci-aplikacji-mobywatel [access: 30.11.2021].

[74] *Ibidem*.

[75] See art. 26 GDPR.

[76] https://pacjent.gov.pl/polityka-prywatnosci [access: 30.11.2021]; art. 9(2)(h) GDPR: processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or

Although the legal prerequisite for the processing of data set out therein applies to 'management of healthcare systems and services', it also requires that such processing be carried out solely by or under the responsibility of an employee bound by professional secrecy[77]. It is an open question to what extent this requirement can be fulfilled in the conditions of large-scale and centralised processing of personal data under the custody of the Ministry of Health.

In the case of the Skaner Certyfikatów COVID application, which is used to verify EDCC certificates, the attribution of the controller's role is diametrically opposed to the Austrian solution. In the case of the Polish implementation, the controller is the Ministry of Health and not each user of the application[78]. Similarly to the mojeIKP application, the Polish implementation, following the spirit of the definition of controller in Article 4(7) of the GDPR, did not limit the scope of responsibility by hiding behind a decentralised model of personal data processing.

The scope of personal data processed in the Skaner Certyfikatów COVID application is defined in the privacy policy in a vague manner. The policy notes that no personal data is "held" in the Skaner Certyfikatów COVID application[79]. This is most likely due to the last sentence of recital 48 of the EDCC Regulation, which states that: "Where the certificate is used for non-medical purposes, personal data accessed during the verification process are not to be retained, as provided for in this Regulation"[80]. Based on the quoted passage, it must be presumed that the Skaner Certyfikatów COVID application does not store personal data read from the QR codes of verified EDCC certificates.

The reference in the Skaner Certyfikatów COVID privacy policy to the use of Google Analytics is disturbing[81]. The exact use of Google Analytics and the scope of the data processed in this way is not specified.

Particularly controversial is the legal basis indicated in the privacy policy for the processing of personal data in the Skaner Certyfikatów COVID application. First, there is no distinction between the data of verified EDCC holders and the telemetric data of the owners of the terminal equipment used for verification. Second, the indicated legal basis for the processing of EDCC holders' personal data here

treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

77 Art. 9(3) GDPR: Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.

78 https://ezdrowie.gov.pl/portal/home/polityka-prywatnosci-ucc [access: 30.11.2021].

79 *Ibidem*.

80 Recital 48 Regulation 2021/953.

81 https://ezdrowie.gov.pl/portal/home/polityka-prywatnosci-ucc [access: 30.11.2021].

is the implied (sic!) consent[82]. This consent shall be presumed from the act of submission of the EDCC certificate for control by placing it under the scanner[83].

According to the provisions of the GDPR, in order to be valid, consent must be given unambiguously, explicitly and in a manner that allows the controller to document receipt of consent[84]. None of these conditions are met in the case of consent implied from a hand movement. Moreover, it is unclear how the withdrawal of such consent would take place; the ease of withdrawal required by the GDPR equal to the ease of submission would in this case have to imply a gesture of withdrawal of the hand holding the EDCC[85].

EU Regulations 2021/953 (EDCC Regulation) and 2021/954 (extending the personal scope of the EDCC Regulation to third-country nationals lawfully residing in the EU) are indicated as additional legal bases for the processing. Given the material scope of the EDCC Regulation discussed above and the scope of national implementations of the EDCC, it should be considered that they only relate to cross-border applications of the EDCC, i.e. the verification of foreign EDCC certificates in Poland.

Finally, it should be noted that the entire Polish implementation of the EDCC available to a wider range of users, i.e. IKP, mojeIKP, mObywatel and Skaner Certyfikatów COVID, is only available in the Polish language version. Considering the constantly growing number of foreigners residing in Poland, such an exclusionary solution should be viewed critically. It is incomprehensible why (similarly to the Austrian implementation) an English language version was not introduced.

5. Conclusions

The analysis conducted above leads to the following conclusions. Controversies and unclear solutions related to the role of the controller in decentralised infrastructures of personal data processing are visible. On the example of the Polish and Austrian implementation of EDCC, two extreme solutions can be seen here, at opposite ends of the spectrum.

On the one hand, in the Austrian model part of the implementation (Grüner Pass application) is left without any controller, presuming the responsibility of the data subject for the data processed in a decentralised structure. Such a solution deserves criticism, especially considering the possible liability (or rather lack

[82] *Ibidem*.
[83] *Ibidem*.
[84] Art. 6(1)(a), art. 7, art. 9(2)(a), and recital 32 GDPR.
[85] Art. 7(3) GDPR.

thereof) for data breaches caused by faulty app design or lack of regular security updates in the mobile application.

On the other hand, in the Polish model, the Minister of Health, as a controller, takes responsibility not only for those aspects of the functioning of the national implementation of the EDCC which they actually has an influence on, but also for those which they do not. The EDCC holder has the ability to make their certificate available to a potentially unlimited audience, either by displaying it in a mobile app or by exporting a pdf file.

It follows that the current non-negotiable model of the triad of roles from THE GDPR (controller, processor, data subject) is insufficient to describe decentralised processing infrastructures, in particular distributed infrastructures at the end-user and mobile device level.

References

Bundesgesetz betreffend Datensicherheitsmaßnahmen bei der Verarbeitung elektronischer Gesundheitsdaten und genetischer Daten (Gesundheitstelematikgesetz 2012 – GTelG 2012) StF: BGBl. I Nr. 111/2012.

Commission, Report from the Commission to the European Parliament and the Council pursuant to Article 16(1) of Regulation (EU) 2021/953 of the European Parliament and of the Council 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, 18.10.2021.

Datenschutz-Folgenabschätzung zum Grünen Pass und zum EPI-Service, https://www.gesundheit.gv.at/service/gruener-pass/datenschutz-folgenabschaetzung.

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 L88/45, 2011.

Epidemiegesetz 1950 (EpiG). StF: BGBl. Nr. 186/1950.

European Data Protection Board-European Data Protection Supervisor, 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), 31.03.2021.

eHealth Network, *Guidelines on Technical Specifications for Digital Green Certificates. Volume 5 Public Key Certificate Governance*, V1.02, 5.12.2021.

eHealth Network, *Interoperability of health certificates. Trust framework*, V.1.0, 3.12.2021.

eHealth Network, *Guidelines on Value Sets for EU Digital COVID Certificates*, V1.4, 13.10.2021.

eHealth Network, *DCC Anomaly Capture Process for COVID Certificate Data. Best current practice*, V1.01, 15.09.2021.

eHealth Network, *Guidelines on Technical Specifications for Digital Green Certificates. Volume 1*, V1.0.5, 21.04.2021.

eHealth Network, *Guidelines on Technical Specifications for Digital Green Certificates. Volume 2 European Digital Green Certificate Gateway,* V1.3, 21.04.2021.

eHealth Network, *Guidelines on Technical Specifications for Digital Green Certificates. Volume 3 Interoperable 2D Code*, V1.3, 21.04.2021.

eHealth Network, *Guidelines on Technical Specifications for Digital Green Certificates. Volume 4 European Digital Green Certificate Applications*, V1.3, 21.04.2021.

Gstrein O.J., *The EU Digital COVID Certificate: A preliminary data protection impact assessment*. "European Journal of Risk Regulation" 2021, vol. 12, iss. 2.

Rozporządzenie Ministra Zdrowia z dnia 20 marca 2020 r. w sprawie ogłoszenia na obszarze Rzeczypospolitej Polskiej stanu epidemii, Dz.U. z 2020 r. poz. 491.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/953 z dnia 14 czerwca 2021 r. w sprawie ram wydawania, weryfikowania i uznawania interoperacyjnych zaświadczeń o szczepieniu, o wyniku testu i o powrocie do zdrowia w związku z COVID-19 (unijne cyfrowe zaświadczenie COVID) w celu ułatwienia swobodnego przemieszczania się w czasie pandemii COVID-19 (Tekst mający znaczenie dla EOG), OJ L 211/1, 2021.

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/954 z dnia 14 czerwca 2021 r. w sprawie ram wydawania obywatelom państw trzecich legalnie przebywającym lub zamieszkującym na terytoriach państw członkowskich w czasie pandemii COVID-19 interoperacyjnych zaświadczeń o szczepieniu, o wyniku testu i o powrocie do zdrowia w związku z COVID-19 (unijne cyfrowe zaświadczenie COVID), oraz weryfikowania i uznawania takich zaświadczeń (Tekst mający znaczenie dla EOG), OJ L 211/24, 2021.

Rozporządzenie Rady Ministrów z dnia 6 maja 2021 r. w sprawie ustanowienia określonych ograniczeń, nakazów i zakazów w związku z wystąpieniem stanu epidemii, Dz.U. z 2021 r. poz. 861.

Streinz T., *The Evolution of European Data Law*, [in:] *The Evolution of EU Law*, eds. P. Craig, G. de Búrca, OUP 2021.