Opinion of the CPDP on the processing of data on vaccination status OPINION OF THE PERSONAL DATA PROTECTION COMMISSION reg. Sofia, 06.10.2021 SUBJECT: Processing of data on the vaccination status The Commission for Personal Data Protection (CPDP) composed of - Chairman: Ventsislav Karadzhov and members: Tsanko Tsolov, Maria Mateva and Veselin Tselkov, at a meeting, held on 29.09.2021, considered a number of letters from organizations and citizens regarding the lawful processing of data on vaccination status. An analysis of the above letters shows that both citizens and businesses need clarification and guidance on the admissibility of processing vaccination status data. This opinion aims to respond to the requests, taking into account the guidelines and positions of the European Data Protection Board (EDPS) and the European Data Protection Supervisor (EDPS) expressed on the same issues. Legal analysis: At EU level, European co-legislators have adopted the EU Digital COVID Certificate Regulation1, which is directly applicable in all Member States from 1 July 2021 (it is set to apply until 30 June 2022). Its aim is to facilitate and make safe the free movement of citizens within the EU during the COVID-19 pandemic. The certificate has an interoperable and machine-readable QR code, available on paper or digital. It certifies that a person has been: · vaccinated against COVID-19; · Received a negative test result; or · has had an infection. The provision of Art. 10, para. 1 in conjunction with rec. Article 48 of the Regulation on the EU's COVID Digital Certificate clearly defines that Regulation (EU) 2016/679 (ORD) applies to the processing of personal data carried out during its implementation. According to Art. 10, para. 2 of Regulation (EU) 2021/953 (which is a lex specialis with regard to ORD), personal data contained in certificates are processed only for the purpose of accessing and verifying the information contained therein in order to facilitate the exercise of the right to free movement within the Union during the COVID-19 pandemic and only within the time limit set by the Regulation, after which no further processing should take place. An additional legally binding argument in favor of the approach set out in Regulation (EU) 2021/953 is recital (54) of Regulation (EU) 2016/679, which states: (54) The processing of special categories of personal data may be necessary for reasons of public interest in the field of public health without the consent of the data subject. Such treatment should be subject to appropriate and specific measures to protect the rights and freedoms of individuals. In this context, the term "public health" should be interpreted within the meaning of Regulation (EC) № 1338/2008 of the European Parliament and of the Council and means all elements related to health, namely health, including morbidity and disability, decisive factors. which affect this state of health, health care needs, resources allocated to health care, provision of and universal access to health care, health care costs and funding, and causes

of death. Such processing of health data for reasons of public interest should not lead to the processing of personal data for other purposes by third parties such as employers or insurance companies and banks. However, for any other purpose, national law must explicitly provide a legal basis for the processing of certificate data2. In this sense, the ORD is fully applicable to the processing of personal data for any purpose other than the purpose of the EU Digital COVID Regulation. In this spirit is the Joint Opinion 04/20213 of the European Data Protection Board (EDPS) and the European Data Protection Supervisor (EDPS) on the proposal for a Regulation of the European Parliament and of the Council on the framework for issuing, verifying and adopting interoperable vaccination certificates, tests and illnesses to facilitate free movement during the COVID-19 pandemic (Digital Green Certificate). Whether and how the certificates fall within the scope of the ORD will depend on how the administrators intend to use them. In this regard, the following hypotheses can be outlined: 1) The administrator intends to systematically record the certificates or the information they contain as part of a register of personal data; 2) The administrator intends to introduce digital verification of certificates, including scanning of their QR code (with or without recording the data they contain); 3) The administrator intends to introduce manual verification of certificates, including verification of printed paper copies or manual verification of the digital certificate (only by visualizing the certificate, without scanning the QR code and / or without recording / documenting the information contained in him). Hypotheses (1) and (2) are activities for processing personal data that fall within the material scope of the ORD (Article 2, paragraph 1 of the ORD) and in this sense must meet the conditions for legality provided therein. Hypothesis (3) does not fall within the scope of the ORD, but nevertheless, the requirement to share sensitive medical information constitutes an interference with the fundamental right to privacy, which is protected by Art. 7 of the EU Charter of Fundamental Rights (Charter). Such interference may affect other human rights than his or her inviolability, such as the right to non-discrimination, the right to work, the right to education, the rights of the child4, etc. Therefore, such a measure must be subject to the conditions of legality, necessity and proportionality provided for in Art. 52, para. 1 of the Charter and the administrator must make a careful assessment of whether such interference can be legally justified. It is indisputable that the certificates contain sensitive health information, which is a special category of data and its processing must meet the higher threshold of legality set in Art. 9 of the ORD. As a measure designed to protect the health and safety of staff (employees) Art. 9, para. 2, p. "B" of the ORZD can provide an appropriate basis for lawful processing of data from digital certificates. The conditions for legality under Art. 9, para. 2, p. "G" or Art. 9, para. 2, p. "I" ORZD, if national law requires wider use of certificates. It should be noted that some of the practical applications of the

certificates can be qualified as activities for automated individual decision-making and profiling, which in turn are regulated by Art. 22 of the ORZD. This may be the case, for example, when digital certificate verification (by scanning a QR code) is used for the purpose of automated access to premises. This activity would be automated individual decision-making, which has adverse consequences for the data subject, incl. legal ones. At present, neither EU law nor our national law allows (as required by Article 22, paragraph 2, item "b" of the ORD) verification of certificates based solely on automated processing for the purpose of granting or refusing access to premises based on health safety considerations. In practice, this means that the use of certificates for such purposes cannot be based solely on automated processing that does not involve adequate human participation in the verification process. Where the processing of data from certificates meets the requirements of legality, necessity and proportionality, appropriate technical and organizational measures for their security must be applied. The controller should assess the need to perform an assessment of the impact on data protection under Art. 35 of the ORD in order to identify the risks and their mitigation at all stages of processing. When certificates are used as a condition and means of gaining access to premises, such an assessment will almost always be necessary, as it involves large-scale processing of special categories of personal data. Methods of data protection at the "design" and "default" stages must also be taken into account by the controller, ensuring that only a minimum amount of data is processed and confidentiality technologies are used. In this regard, verification procedures should be provided to avoid the recording and retention of personal data in accordance with the principle of data minimization and in implementation of the EU Digital COVID Certificate Regulation, which aims at decentralized verification. of the certificates without processing additional data for this. In accordance with the principle of transparency, data subjects (employees, visitors, etc.) must be informed in advance of the measures imposed by the controller when checking certificates, such as how it will be done, what data will be processed, who will have access to it and to whom requests or objections related to the processing of this data may be addressed. The protection of personal data is only one aspect of the introduction and implementation of measures to limit the spread of the epidemic. To date, a number of EU countries (Germany5, France6, Italy7, the Netherlands, Austria8, Greece, Denmark9, Cyprus10, etc.) have made or are in the process of making legislative changes that respond to both the unprecedented public relations and and the existing legal order guaranteeing the fundamental rights and freedoms of citizens. Switzerland, although not an EU member state, adopted in early September this year. legislation introducing mandatory use of certificates for the purpose of visiting restaurants and other public places. As the topic goes beyond the competence of a data protection supervisory authority, we believe that it should be

strategically discussed in the widest possible range of other public authorities, citizens and organizations. the necessary legally binding acts at national level. In the State Gazette no. 44 of 13.05.2020, the Law for amendment and supplement of the Health Act was promulgated, which regulates the legal instruments for limiting the spread of the epidemic and overcoming its consequences, which are applied on the territory of the country after the abolition of the state of emergency. .e. after 13 May 2020. Both completely new, different in nature measures and changes in the already introduced ones are regulated. The law entitles the Council of Ministers, at the suggestion of the Minister of Health, to declare an emergency epidemic situation in the country in imminent danger to life and health of citizens from the spread of a contagious disease such as COVID-19. The conditions that must be met in order for such a situation to be introduced are also regulated. In this regard, with its Decision № 325 of 14.05.2020, the Council of Ministers declared an emergency epidemic situation on the territory of the country, which continues to this day. Anti-epidemic measures are introduced by order of the Minister of Health or another competent body (eg director of the relevant RHI). In addition, the Law on Measures and Actions during the State of Emergency, declared by a decision of the National Assembly of March 13, 2020 and on overcoming the consequences of 14.05.2020) provides that the Minister of Health may, in addition to the Health Act, introduce other temporary measures and restrictions specified in law. Before introducing intrusive measures such as tests (antigen / PCR) or processing data on the vaccination status of individuals, administrators may consider using aggregated (aggregated) health data. Aggregate data that do not allow the association of health information with individuals can be considered anonymous11, ie. do not fall within the scope of the ORD. Examples of such aggregated health data include: · Percentage of employees who have been vaccinated against COVID-19 over a period of time; · Percentage of employees without vaccination against COVID-19 or those with unknown vaccination status. Occupational health services that have the vaccination status of individuals may be tasked with producing such aggregated data. However, in order to ensure that aggregated data are anonymous, they should always refer to groups of individuals that are large enough to exclude the possibility of identifying a specific person. In principle, the occupational health service may not have this information (either inaccurate or out of date). In these cases, in order to obtain aggregated data, administrators may encourage their staff to inform the occupational health service of their vaccination status, provided that this is voluntary and carried out only by a medical professional. Administrators may also consider using surveys to get an idea of the percentage of vaccinated and unvaccinated employees. These surveys should be voluntary and anonymous. If an electronic tool is used to conduct it, it must be ensured that it ensures the anonymity of the participants (even if such a tool

does not collect names or email addresses, it can collect IP addresses). Asking open-ended questions in these surveys should be avoided, as their answers can identify a specific person. At EU level, the requirements of the EU Digital COVID Regulation exclude from the outset the applicability of consent to the processing of data contained in certificates. As mentioned above, the processing of data for other purposes can only take place if the legal basis for this is established in national law, ie. it must have the character of a legal obligation. Consent, as a ground provided for in EU law (ORZD), cannot be applied to the processing of personal data from the EU Digital COVID certificate. Recital (48) of Regulation (EU) 2021/953 explicitly provides that Member States may introduce into their national law the possibility of processing data for other purposes, provided that a clearly defined legal basis is provided for that which corresponds to EU data protection law and the principles of efficiency, necessity and proportionality, and should include provisions that clearly state the scope and extent of processing, the specific purpose, the categories of entities that can verify the certificate and the relevant guarantees to prevent discrimination and abuse, taking into account the risks to the rights and freedoms of data subjects. Regulation (EU) 2021/953 explicitly prohibits the storage of certificate data when the processing is for non-medical purposes. As far as the open letter submitted to the CPDP raises issues related to the vaccination status of the parents of children from kindergartens, the above arguments remain fully applicable. However, it should be borne in mind that the exclusion of children from unvaccinated parents in kindergarten can lead to violations of specific rights and interests of children. Guided by the principle of ensuring the best interests of the child (Article 3, item 3 of the Child Protection Act), he should not suffer adverse legal consequences and restrictions on his rights or privileges as a result of actions or inactions of the child. his parents (argument from art. 10, para. 3 of the Child Protection Act). For the sake of completeness, it should be borne in mind that the Ministry of Health has developed and launched an application for verification of the EU Digital COVID certificate - the so-called. Covid Check BG. For these reasons and on the grounds of Art. 58, para. 3, p. "B" of Regulation (EU) 2016/679 in conjunction with Art. 10a, para. 1 of the Personal Data Protection Act, the Commission for Personal Data Protection expresses the following OPINION: At present, our national legislation does not regulate the extended use of personal data from the EU Digital COVID certificate for purposes other than facilitating the right to free movement in Union during the COVID-19 pandemic and only within the time limit set by Regulation (EU) 2021/953. However, and in view of the need to comply with the orders of the Minister of Health introducing anti-epidemic measures, data controllers may process aggregated (summary) data on the vaccination status of individuals to assist them in carrying out risk assessment. in ensuring healthy and safe working conditions. The only legal possibility for

administrators, other than those referred to in paragraph 2, to ensure a balance in the implementation of both the orders of the Minister of Health and the data protection legislation is to verify the EU Digital COVID certificate without storing The results of it. These actions can be performed only with the voluntary presentation of the certificate, and the lack of such presentation can not be used to restrict the rights and freedoms of individuals. PRESIDENT: MEMBERS: Ventsislav Karadjov / tsanko Tsolov / p / Maria Mateva / p / Veselin Tselkov / p / 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 the adoption of interoperable vaccination certificates against, a study on and recovery of COVID-19 (EU Digital COVID Certificate) in order to facilitate free movement during the COVID-19 pandemic 2 Recital 48 of Regulation (EU) 2021/953 3 https://edpb.europa.eu/system/files/2021-07/edpb_edps_joint_opinion_dgc_bg.pdf 4 In cases where his socially guaranteed rights are denied, such as attending kindergarten or crèche, when his parents do not prove their status as vaccinated, ill or tested for COVID-19 5 On 22 April 2021, a law was promulgated granting privileges to vaccinated persons. 6 On 26 July 2021, the French Parliament passed a law extending the use of certificates, which subsequently passed constitutional scrutiny. 7 The legal act extending the use of certificates was published on 6 August 2021 in the Official Journal of Italy: https://www.gazzettaufficiale.it/eli/id/2021/08/06/21G00125/sg 8 On On May 26, 2021, the Austrian parliament approved a bill introducing the so-called "green pass", which gives its owners access to restaurants, hotels and cultural institutions if they can prove that they have been vaccinated, COVID-19 or negative. virus test. 9 Denmark was one of the first countries to introduce legislation in this area as early as April 2021. 10 In Cyprus, such legislation has been in force since 9 July 2021. 11 Cf. Opinion 05/2014 of the Working Group under Art. 29 on technical anonymization methods, adopted on 10 April 2014. Downloads Download CPDP opinion on data processing for vaccination status print