/

NATIONAL DATA PROTECTION COMMISSION

OPINION/2020/82

I. Order

The Secretary of State for the Presidency of the Council of Ministers asked the National Data Protection Commission (CNPD) to issue an opinion on the Draft Decree-Law that establishes the person responsible for data processing and regulates the intervention of the health professional in the system. STAYAWAY COVID.

The CNPD issues an opinion within the scope of its attributions and powers, as the national authority to control the processing of personal data, conferred by subparagraph c) of paragraph 1 of article 57 and paragraph 4 of article 36 of the Regulation (EU) 2016/679 of the Parliament and of the Council of 27 April 2016 (General Regulation on Data Protection - RGPD), in conjunction with the provisions of article 3, paragraph 2 of article 4 .° and in paragraph a) of paragraph 1 of article 6, all of Law n.° 58/2019, of 8 August.

As a preliminary note, one cannot fail to mention that the request to the CNPD was made on July 16, 2020, the date of approval, "in general", of the diploma in question (cf. it appears in point 1 of the Communiqué of the Council of Ministers of July 16, 2020), with a period of five days for issuing an opinion. Regardless of the special circumstances inherent to the pandemic situation and the recognized urgency in adopting legislative and other measures, it follows from a legal imperative, as indicated above, that consultation with the CNPD is prior and not subsequent to the approval of the diplomas, under penalty of the opinion issued. not be of effective use and the reason underlying this consultation will be undermined.

II. appreciation

The legislation in question1, as stated in its preamble, "aims to provide a legal framework for the data controller and regulate the intervention of the

1 This draft diploma takes the form of a decree-law, when, strictly speaking, the legal provision for the processing of personal data, as it reflects the conditioning or regulation of the exercise of rights, freedoms and guarantees, should have been preceded by authorization of the Assembly of the Republic (cf. subparagraph b) of paragraph 1 of article 165 of the Constitution of the Portuguese Republic). It is recognized, however, that the processing of personal data carried out by the

STAYAWAY COVID system is based, with regard to the restriction of the fundamental rights of the data subject (the user of the application), on the consent of the user, pursuant to paragraph

health professional in the STAYAWAY COVID system», following the recommendations made by the CNPD in this regard.

As for the preamble of the decree-law, two notes are noted: one relating precisely to the paragraph in which what was recommended by the CNPD is mentioned, in order to clarify that it was not the CNPD that carried out the impact assessment on data protection (AIPD), but that it appreciated the impact assessment, which was in fact carried out by the promoters of the system; the second note is to include in the preamble of the diploma the reference to the hearing of the National Commission for Data Protection.

As for the provisions of the draft diploma, it is worth highlighting, from the outset, positively, in paragraph 2 of article 1, the assumption of the STAYAWAY COVID system as “a complementary and voluntary instrument for responding to the epidemiological situation”. The voluntary nature of the application was defended by the CNPD as an essential requirement, from the point of view of guaranteeing the rights and freedoms of citizens, for the operation of this type of proximity contact applications, as follows from points 29-35 of Deliberation/20 20/2772, and whose reasoning is given here as reproduced.

It is also clear from paragraph 2 of article 1 that the purpose of data processing is to notify STAYAWAY COVID users of “individual exposure to contagion factors by SARS-CoV-2, resulting from contact with a user of the application to who has subsequently been diagnosed with the disease COVID-19», thus contributing to the identification and monitoring of contacts between citizens as a complementary means of interrupting the chains of transmission of the virus, as indicated in the preamble of the project.

a) of paragraph 2 of article 9 of the RGPD, and not in the present diploma. To that extent, and considering the current circumstances, the CNPD limits itself to pointing out this aspect.

2 Deliberation/2020/277, of June 29, 2020, regarding the impact assessment on data protection of the STAYAWAY COVID system, submitted by INESC TEC, as one of the project promoters, available at https://www

.cnpd.pt/home/decisoes/Delib/DEL_2020_277.pdf

Although not expressly identified as such, the purpose is considered to be specific, explicit and legitimate, in accordance with the requirement of Article 5(1)(b) of the GDPR.

The draft decree-law determines that "[the] Directorate-General for Health (DGS) is the health authority that manages the STAYAWAY COVID system, being, in terms of its legal powers, responsible for the treatment (...)" ■ In this capacity, the project generally refers to the DGS the definition of the functioning of the system, the various data processing operations, the articulation between all the actors in the system and the contracting with SPMS - Serviços Partilhados do Ministério da Saúde, E.P.E., of the services and technical means necessary for the proper functioning of the system (cf. article 3).

Given the purposes of the treatment and the fact that the pseudonymised data to be processed by the STAYAWAY COVID system constitute personal health data, within the meaning of paragraphs 1), 5) and 15) of article 4 of the GDPR, it can only be responsible for this treatment to those who have legal powers and powers in the area of health and adjusted to the specific purpose of the application. The CNPD has already commented on this matter in points 73-76 of Deliberation/2020/277, whose arguments are reproduced here.

Given that the Director-General of Health is the national health authority3, with specific powers in this context, namely in the field of epidemiological surveillance and systems for alerting and responding to public health emergencies, it seems that, if the diploma intends to assigning responsibility for processing to the 'health authority', it should refer to the Director-General for Health as responsible for processing. In any case, it is clear that, from a data protection perspective, taking into account the attributions of the DGS4, nothing prevents the DGS from assuming that capacity as a responsible person, provided that it is not qualified here as a health authority.

3 As can be read in paragraph 3 of article 3 of Decree-Law No. 82/2009, of 2 April: "The national health authority is the Director-General of Health".

4 Cf. subparagraph b) of no. 2 of article 2 of Regulatory Decree no. 14/2012, of 26 January - Organic Law of the DGS.

Article 4 of the draft decree-law under consideration here intends to regulate the intervention of the health professional, in

compliance with paragraph 1 of article 1, of the diploma, which has as its object, in addition to establishing the person responsible for the treatment , reguiáj] the intervention of the health professional in the ST AY A WA Y COViD system.

It is expected that the health professional obtains and communicates the legitimation code (CL) to the user of the application so that he can, if he so wishes, insert this code into the application with a view to later reporting his condition of positive diagnosis5.

However, it appears that very little is effectively regulated in this article. So, let's see.

Firstly, in paragraph 1 of article 4 it is mentioned that the health professional obtains and communicates to the user of the ST AYAWAY COViD application that he is diagnosed with the disease COViD-19 the legitimation code, without determining through of which application the doctor becomes aware of the diagnosis of the disease. Now, it seems that there may be two applications at stake - SINAVE and Trace COVID-19, appearing to be such an essential element for the functioning of STAYAWAY COVID, as is the source of information regarding the positive diagnosis of a user and from which if you can apply for the CL, it must be defined in this legal diploma.

Secondly, the qualification of the health professional with the capacity to validate the medical diagnosis is not even determined by the legislator. Indeed, it is considered that obtaining a diagnostic legitimation code, which represents a fundamental aspect of the reliability of the application, insofar as it certifies that a certain person is infected with the SARS-CoV-2 virus, can only be performed by a doctor and not by another health professional6. Consequently, it is not understood why this question does not remain

5 For a better understanding of the functioning of the system and its interactions between the legitimation of the diagnosis of a person infected with the virus and the sending of this information to the diagnosis publication server, see points 13-21 of Deliberation/2020/277, of the CNPD, mentioned above.

6 Cf. Article 7 of Regulation No. 689/2019, of 5 September.

defined in the law, from now on, instead of leaving open the possibility for the controller to decide otherwise.

Furthermore, it is not defined - as it should be at the legislative level - which is the universe of health professionals (doctors) who are expected to intervene in the system, whether only those from the public sector or also those from the private sector, which could result in a very different scope of the application, compromising its purpose and effectiveness from the outset.

Thirdly, since the STAYAWAY COVID system is expected to process, together with the legitimation code, the date of the first symptoms or the diagnostic test, for the purpose of selecting the number of TEK7 keys to be sent to the diagnostic publishing service, it must the legal diploma expressly provides for the secondary use of the information that was collected in the context of patient follow-up, for a different purpose.

This issue is completely absent from the text of the project, with the consequence that the information that can be transferred from a health information system to a server of the STAYAWAY COVID system is not delimited. If it is understood that some elements of the processing of personal data are defined by the DGS - already in line with the SPMS and after knowing all the technical means available in the short term -, namely those relating to the authentication of the health professional, it is up to the law to establish criteria and add safeguards, so as to have the predictability required of it, which is not the case in the present case. In this regard, it is recalled that Article 9(2)(i) of the GDPR allows processing of personal health data in the field of public health provided that national law provides for appropriate and specific measures that safeguard the rights and freedoms of the data subject.

With regard to the guarantees of rights, it is essential to ensure that the identifiable data of patients are not entered in the service of legitimation of diagnosis (SLD).

7 TEK - Temporary Exposure Key: pseudorandom identifiers generated daily on the user's device and stored there for 14 days.

Thus, in the terms in which it is written, article 4 of the project, by not determining, at least, which health professional is at stake, which personal data must be used by the doctor and in which application they reside, constitutes a blank rule, without sufficient density to provide the essential predictability to the processing of personal health data.

And to overcome this normative incompleteness, Article 2 is not enough, which, under the heading “Protection of personal data and cybersecurity”, refers to guidelines made at European level, in the context of applications and other technological resources to combat COVID. -19, for Guidelines No. 4/2020 of the European Data Protection Board8, for the cybersecurity

requirements of the European Cybersecurity Agency (ENISA)9 and for Commission Recommendation (EU) 2020/518, of 8 April10, prescribing that this set of non-binding instruments must be respected by the STAYAWAY COVID system.

Thus, it is considered that the legislator was excessively minimalist in the regulation regarding the operation of the STAYAWAY COVID system, referring all the specific aspects of the processing of personal data to a later definition to be made by the DGS, as responsible for the treatment, including in what concerns regarding interoperability with similar applications from other states.

Despite the fact that the application has already been structurally developed from a technical point of view, therefore, no significant changes are anticipated by the controller, and that the CNPD has already assessed, within the scope of the prior consultation on the IAPD, several aspects of the future data processing, it would always be for the legislator to introduce some

8

https://edpb.europa.eu/our-work-tools/our-documents/linee-guida/guidelines-042020-use-location-data-and-contact-tracing_en

9 https://www.enisa.europa.eu/topics/wfh-covid19

10 OJ L 114, 4.14.2020

safeguards regarding the processing of personal data, which, when involving digital technologies of proximity tracking, raises legitimate concerns, in an ethical and legal plan11.

Added to this framework is the fact that a substantial part of the data processing is not controlled by the controller, but by a partnership of two of the largest private technology companies (GAEN interface, created by Google and Apple).

Given the potential universe of application users and the objective of the STAYAWAY COVID system, the CNPD considers that it is up to the national legislator to outline the limits of its operation, providing for constant monitoring of the application's behavior and of changes that are introduced in the plan of the operating system of the mobile devices, also assuming the importance of the remote switch functionality that the system contains and under what conditions it should be used.

Finally, it is noted that the draft decree-law does not assume the exceptional and temporary nature of the STAYAWAY COVID system, and the processing of personal data that it implies, not setting any deadline or time period, even flexible with reference to verification. certain conditions (e.g., end of the pandemic/epidemic situation), for its termination.

However, in compliance with the principles set out in subparagraphs a), b), c) and e)6, paragraph 1 of article 5 of the RGPD, the CNPD understands that this is an essential issue, which should be included in the diploma.

11 On some of these concerns, see points 31, 87 and 89 of Deliberation/2020/277. See also Position of the National Council of Ethics for Life Sciences, of June 29, 2020, on Mobile digital applications to control the transmission of COVID-19 - relevant ethical aspects.

https://www.cnecv.pt/files/1593523643_62f80ed69c317b6cee76810d493bb77a_posic-a-o-cnecv-apps-mo-veis-controlo-covid 19-29-06-2020.pdf

III. Conclusion

Based on the observations and on the grounds set out above, the CNPD considers that:

1. The preamble of the diploma must be revised in the light of the two observations made, regarding the clarification on the IAPD and regarding the introduction of the reference on the hearing of the CNPD;

2. It must be made explicit in the diploma that the health professional with competence to validate a diagnosis of SARS-CoV-2 infection is a doctor, so the access profile to the diagnosis legitimation system must respect this rule;

3. The universe of covered doctors, the reuse of patients' clinical information and its limits must be effectively regulated, determining that identifiable patient data is not included in the diagnostic legitimation service (SLD).

4. Safeguards should be introduced regarding the processing of personal data, namely: limiting the use of data only for the purpose set forth herein; providing for the continuous monitoring of the application's behavior with regard to the GAEN interface and eventual changes; defining under which conditions the remote switch functionality can be activated to protect users;

5. A rule should be added that determines the transitory and exceptional nature of this data processing, providing for its termination, in a flexible way, by reference to the end of the pandemic/epidemic or when certain specified conditions are verified.

Approved at the meeting of July 21, 2020

Fílipa Calvão (President)