

National Data Protection Commission

OPINION/2021/108

I. Order

1. The Office of the Minister of Health requested an opinion from the National Data Protection Commission (CNPD) on the request of the Coordinator of the Vaccination Task Force against Covid-19 for access to information contained in health databases, for the purpose of evaluating and monitoring procedures related to vaccination.

2. The CNPD issues an opinion pursuant to Article 58(3)(b) of Regulation (DE) 2016/679, of 27 April - General Data Protection Regulation (RGPD).

3. The Task Force Coordinator's request specifies that access to information is essential for planning and managing the vaccination plan, with an evident impact on public health in the context of the Covid-19 pandemic. The databases where the information resides are not identified, but the data to be accessed are indicated, which, in essence, are divided into four groups:

The. Identification data - SNS number and date of birth;

B. Vaccination data - gender, ARS of residence, municipality of residence, date, brand and batch of the 1st and 2nd inoculation;

ç. Positive Test Data - Date of positivity, test type, and SARS-CoV2 genetic variant;

d. Hospital admission data - Date of admission, date of entry into the ICU, date of hospital discharge, date of death.

4. According to the terms of the Task Force Coordinator's request, it is not intended to know data that directly identify the holders, but the number of the National Health Service (SNS) is essential as a link between the various databases, as well as the date of birth as the second identification data. That is, to correlate the information of the same person, even without the need to know their identity.

5. The possibility of, exceptionally and in specific circumstances, being able, within the scope of the tasks and powers of the Task Force, to have access to identified data was also considered.

Av.D. Carlos 1,134.1° 1200-651 Lisbon

T (+351) 213 928 400 F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

PAR/2021/90

1v.

II. Analysis

i. The processing of personal data and its legal basis

6. According to Order No. 11737/2020, of 26 November, amended by Order No. 3906/2021, of 19 April, both of the Ministers of National Defence, Internal Administration and Health, are attributions of the Task Force «[the] definition [...] of the vaccination strategy against COVID-19, namely with regard to the identification of priority target populations, the administration of the vaccine against COVID-19 and the identification of parameters for the appropriate clinical follow-up; [a] preparation [...] of the logistical plan for vaccination against COVID-19 [...]; [the] development [...] of the computer support process for vaccination against COVID-19, namely regarding the recording and monitoring of results and the identification of adverse reactions» -cf. subparagraphs a) to c) of no. 4 of the aforementioned order.

7. In the same order, in paragraphs a) to c) of no. 2.2., it is specified that the Task Force Coordinator's powers are "[to]articulate, monitor and evaluate the implementation process of the approved Vaccination Plan; [d]efine and adapt, within the framework of availabilities and needs at any given moment, the strategy for implementing the Vaccination Plan, in accordance with the technical guidelines of the competent authorities; [monitor and evaluate the efficiency of the implementation process and propose the adaptation, with the competent authorities of the Ministry of Health, of the established procedures, whenever deemed necessary and appropriate».

8. At issue is the processing of personal data, as it corresponds to operations that focus on information relating to identifiable natural persons (from the outset, by the SNS number), under the terms and for the purposes of paragraphs 1) and 2) of article 4 .° of the GDPR, under the responsibility of the Task Force, within the meaning of Article 4(7) of the GDPR.

9. The CNPD accepts that the processing of the personal data listed above is adequate and necessary for the purposes pursued by the Task Force, since the anonymized data does not allow the connection of vaccination information with subsequent infections, which is essential for the definition of the strategy vaccine against COVID-19, the evaluation of the

implementation process of the vaccination plan and its adaptation.

10. However, the Task Force does not have, for the purposes invoked and which fall within the attributions defined in the aforementioned Order, an effective need to know the identity of the data subjects, so, in accordance with the principle of proportionality and the principle of minimization of personal data, enshrined in Article 5(1)(c) of the GDPR, the processing must involve a pseudonymisation operation (cf. Article 4(5) of the GDPR).

1

PAR/2021/90

two

National Data Protection Commission

11. Given that personal data relating to health are at stake, the basis for the lawfulness of data processing cannot be exhausted in subparagraphs c) and e) of paragraph 1 of article 6 of the RGPD, having to resort to pursuant to Article 9(2)(i) of the GDPR.

12. Indeed, the legal regime for the protection of personal data makes room for Union law or national law to provide for the processing of data with appropriate and specific measures to safeguard the rights and freedoms of data subjects, in particular confidentiality professional.

13. Now, considering the current pandemic situation, the relevance of vaccination in combating it and the monitoring and adaptation of planning, it seems admissible that, under the regulatory competence recognized by paragraph 2 of article 17 of the Law No. 81/2009, of 21 August, an exceptional and transitional solution is provided for and regulated by the Minister of Health, which is adequate and harmonizing the different rights and interests involved, with the guarantees provided for in the GDPR.

ii. Origin of information

14. The information indicated above, in point 3.b., can be found in the vaccine registration application. The one referred to in point 3.c. resides in the information system called SINAVE Lab and in the Ricardo Jorge National Institute (INSA). Regarding the information listed in point 3.d., the date of death is accessible in the SICO information system, and the other information resides in the systems of hospital institutions.

15. Regarding identification data (SNS number and date of birth), for information aggregation, they exist in all these systems.

iii. Information system and measures to mitigate the impact on personal data

16. The information referred to above, in point 3, to be sent by the systems indicated in point 14, must have as a reference any element that relates it to the Covid disease, either the registration of vaccines against Covid, or the positive result of the test , whether this is the pathology encoded at death or the hospitalization data in disease situations.

17. The information received will be stored in a database, on a server (virtual machine) residing in the General Staff of the Armed Forces (EMGFA) and application access will be made through two specific machines (PCs), which are articulated according to the existing technological architecture.

18. In order to comply with the regime provided for in the RGPD, the data stored in the database will be encrypted, communications with the equipment will be carried out by VPN with an IPSec tunnel and there will be protection between services, using LDAP authentication, using the mechanism of TLS.

Av. D. Carlos 1,134.1º I (+351) 213 928 400 geral@cnpd.pt

1200-651 Lisbon F (+351) 213 976 832 www.cnpd.pt

PAR/2021/90 2v.

19. The data will be kept and used in a "Black Box" system, using the statistical analysis software Matlab and SPSS, with an access profile defined for each of them.

20. User accounts will be individual, allowing unique identification.

21. Through the use of these mechanisms, it is guaranteed that there will be no access to individualized data, but only to statistics and indicators.

22. The system will be equipped with a log record to ensure its auditability.

iv. Access to identified data and measures to mitigate the impact on personal data

23. Bearing in mind the above, in points 9 and 10, access to identified personal data will be of an exceptional nature and the purpose must be contained in the tasks and powers of the Task Force. This access can only occur by determination of the Minister of Health, pursuant to Article 5(4) of Law No. 82/2009, of 4 April, amended by Law No. 135/2013, of 4 of October.

24. However, in order for this to be possible, the measure indicated above, in point 19, will have to be discarded, as it is necessary to invoke the encryption key. Since this entails a significant risk to the rights and freedoms of data subjects, it is necessary to adopt other measures that are capable of mitigating this new risk.

25. Such measures will go through mechanisms that, while not absolutely preventing access to the identified data (SNS number), oblige the user to justify it and trigger alerts to the hierarchical superior(s), who, way, it may intervene in the event of improper access. An example of this type of mechanism is the so-called Break-the-Glass system.

III. Conclusion

26. On the grounds set out above, provided that the measures listed above are adopted, in points 18 to 20 and 25, the CNPD has nothing to oppose the processing of personal data under consideration.

27. The CNPD reiterates the exceptional and transitory nature of a normative solution in this sense that, eventually, will be adopted, recommending that, as soon as the need for this treatment ceases, the database created for this purpose be deleted and the access profiles.

Lisbon, August 18, 2021

Filipa Calvão (President, who reported)