AVG Process/2020/349 1

r

g mm »

AND; ff

M NATIONAL DATA PROTECTION COMMISSION

DELI BERATION/2020/262

I. REPORT

The National Data Protection Commission (CNPD) received several participations reporting vulnerabilities of the tool called Trace COVID-19, for monitoring contact tracing of patients in surveillance and self-care. The content of the participations pointed to existing features in the tool with an impact on the security and confidentiality of personal data, by making it possible to consult without apparent limitation in the available universe and to export, without any control, personal data listings to Excel tables.

The CNPD investigated the reported situations, in the use of its attributions and competences as an independent administrative authority with authority powers to control the processing of personal data, conferred by paragraphs f) and h) of paragraph 1 of article 57, in conjunction with paragraphs 1 and 2 of article 58, all of Regulation (EU) 2016/679, of 27 April 2016 - General Regulation on Data Protection (hereinafter, RGPD), in conjunction with the provisions of article 3 and paragraph b) of paragraph 1 and paragraph 2 of article 6, all of Law no. the GDPR.

Trace COVID-19 Platform

The National Health Authority issued Standard No. 4/2020, of March 23, 2020, which establishes the procedures to be adopted by health professionals in Primary Health Care and Public Health Teams and Health Authorities on the Trace platform COVID-19, which has as its object “the management of patients in self-care and outpatient clinics” and corresponds to “a support tool, so that, through a set of tasks generated by the system, they implement effective clinical follow-up and preventive measures”. Public Health suitable for patients with suspected or confirmed COVID-19”.

There is information on the website relating to this platform1 which indicated that it was developed by SPMS - Serviços Partilhados do Ministério da Saúde, E.P.E. (hereinafter SPMS), on April 8 and 20, several clarifications were requested from this entity, as well as documentation regarding the architecture and operation of the Trace COVID-19 tool

1 Available at https://tracecovid19.min-saude.pt/

r

and also the Impact Assessment on Data Protection, provided for in paragraph 1 of article 35 of the GDPR.

Subsequently, it was clarified that SPMS acts in this processing of personal data as a subcontractor2 of the Directorate-General for Health (DGS), an answer was presented to the questions posed and the following documents were sent: diagram of database tables; Database DDL script3; requirements specification book; and user manual.

An investigation was carried out on the 19th of May, at the SPMS facilities to verify the functioning of the platform and requested elements for the instruction of the process and, finally, on the 22nd of May, to verify if there was a vulnerability in the consultation of patient data.

From the analysis of the elements provided by SPMS, it is noted that authentication in the Trace COVID-19 tool is being delegated to servers in the doud"of Microsoft's Azure platform". The accounts used are those that professionals from the National Health Service (SNS)) and the Ministry of Health already have, which identifies them in their systems, also allowing access to “email and productivity services” (Office 365)4. The accounts are defined on the local Active Directory (AD)5 servers of the various healthcare entities, are managed by them, and are synchronized with Azure AD (AAD)6 to allow access to various tools available online, namely Trace Covid-19.

For private health entities, “guest” accounts are created, with exclusive access to the tool, in the SNS AAD, and the management of these credentials is the responsibility of the respective private entities. SPMS justifies these “guest” accounts on the fact that “some users want[re]to be followed by their attending physician in private clinics/hospitals”. The SPMS stated that these institutions outside the SNS can use the Trace COVID-19 application to carry out surveillance of their patients.

2 Cf. Article 4(8) of the GDPR

3 i.e., Sequences of statements which when executed create the structure of a database.

4 Office 365 references MS O/f/c productivity toolset made available online on doud Azure

5 Active Directory is the system created by Microsoft that stores, organizes, and provides access to information in a central directory in order to access network resources.

6 Azure Active Directory - doud-based identity and access management service

AVG/2020/349 Process 2

t

' NATIONAL COMMISSION

■ DATA PROTECTION

SPMS refers the criteria for granting access and login procedures for each Trace COVID-19 user to the “Normative Circular to be published on April 17th”7. Subsequently, on April 20, SPMS stated that the Normative Circular would not yet be completed and that it had “expected to be able to issue it last week, however, the Circular is still being articulated and closed with the DGS.” . SPMS declares that “generally, all professionals must request access via ServiceDesk and with the express authorization of the Clinical Board or Board of Directors of the respective institution”.

With regard to the profiles for accessing the Trace COVID-19 tool, the entity clarifies that “there are 3 different profiles: Local, Regional, and National, depending on the number of institutions to which the user has access”. For the definition of the user profile, “at the time of requesting access, the entity with direct responsibility for the professional (...) indicates the applicable profile.”.

The operations allowed for all profiles are the insertion and updating of patients/tasks/surveillance, and the “transfer of users between the unit responsible for surveillance”.

The Local profile can access the data of the “respective ACeS8 and Functional unit or hospital institution”; the Regional profile accesses data from “Regional ACeS and Functional Units”; the National profile accesses data from all institutions.

The management of accesses, with regard to the assignment and alteration of profiles, is the responsibility of SPMS, with the information on the profiles being stored on its servers located in the datacenter in Porto, where the systems that support the tool and the database also reside.

In this regard, it also states that profiles are managed following “principles of identity, through unique and individual users (nominal users) and principles of minimum access, with high-privilege accounts restricted to the minimum necessary for management, administrative and administrative functions”. and operation”.

7 Answer given on April 16, attached to the file.

8 The Health Center Groups are health services with administrative autonomy, consisting of several functional units, which

integrate one or more health centers.

AVG/2020/349 2v process.

For the administration of the Trace COVID-19 tool, there are two profiles: “Local Admin - Users with access to national information and Dashboards” and “Solution Administrator - Users with access to the management and configuration of security tools and mechanisms. Users with this profile will automatically have access to information on all models.”.

It is also stated that in the consultation of personal data “there is an automatic and native selection (filter built into the application, which cannot be removed by the user) so that it can only consult the users assigned/under surveillance by the respective ACES/unit.”.

According to SPMS, “mechanisms continue to be progressively implemented to prevent the alteration of identifying data of users, or that come from the integration of information from other systems, namely not allowing to change the fields of name, SNS number, identification document. , contact.”.

Regarding the relationship with other applications, it is explained that the Trace COVID-19 tool currently "receives data from other SNS systems, but (...) does not send data to other information systems (...)", adding that “data from the National User Registry (RNU), the SNS24 line and the Electronic Health Registry (SER) are integrated.” From the specification specification it is concluded that it is possible to import data from “Files (flat , xml, excel, csv)”.

Regarding the import of data contained in Excel files, SPMS comes to clarify that this process “is not yet automated”, and that it would have made sense at the beginning of the project, since some units (ACeS and UF) carried out surveillance using Excel files, adding that “we do not see any use or priority in the development of this automatism, at the moment”.

It was stated that at the time the documents were sent to the CNPD, the Trace COVID-19 tool had 72,375 users with a Local profile, 27 users with a Regional profile, and 18 users with a National profile, with 125,461 users in surveillance. Subsequently, in the inspection on 19 May, it was found that the number of users was 73,486 and 372,184 users were registered under surveillance.

Regarding the personal data processed in the Trace COVID-19 tool, the following were indicated: name; birth date; address; telephone contact and email; user number and/or NIF and/or identification document “(in order to accommodate users without a user number)”; surveillance state; examination status; start and end date of surveillance;

origin of the user; location (home, hospital or other); Epidemiological/contact Hnk; death record. Added to these data are those recorded in surveillance: “information regarding a surveillance”; “summary of symptoms and questions asked (eg: Temperature, Cough, Sore Throat, Body ache, etc)”; "Comments"; “Calculation of a risk score based on symptomatology”.

The tool allows the creation of reports and dashboards* that “are not specific to a single functional area and that cross information [from] National Aggregate Vision [and] Daily Indicators”. These documents produce indicators such as “Number of People Under Surveillance”, “Number of Surveillance carried out”, “Number of Users by surveillance state”.

Information was given on the transmission of data between the application server9 10 and the database and on the technical specifications.

As for the answers given in the section referring to the audit records, inconsistencies were detected, namely because this functionality only points to the “second phase”. Therefore, further clarifications were requested on 20 April. The following day, the information that arrived confirmed the existence of these records, but not the mechanisms capable of consulting them - “We may not have been clear. The audit mechanism already exists and is already being performed. What does not exist is the availability of the functionality to query the data collected.”.

Regarding the records of accesses (/og of accesses) to the Trace COVID-19 tool, it was clarified that they were stored in the AAD. In contrast, application activity records {/og applications) “are stored in the infrastructure at the SPMS Datacenter in Porto”.

The database of the Trace COVID-19 tool is subject to daily backups, with only the “operations team and the SPMS datacenter team” having “permission to access and manage the backup repository”.

"Access to the tool's support database is restricted to the Trace COVID-19 application.".

9 Tables that show metrics and indicators in a visual way, facilitating the understanding of the processed information.

10 Web server where the Trace COVID-19 tool is run and which responds to client requests (browsers).

Regarding the impact assessment on data protection requested by the CNPD, SPMS stated that it is “in preparation at the time of the collection of the elements under analysis”, and has not, so far, been sent to the CNPD.

As for future developments already foreseen for this tool, reference was made to the “development and implementation of an integration with the National Epidemiological Surveillance System (SINAVE), to collect data on laboratory tests, essential for effective patient surveillance”.

In this regard, SPMS clarified “that integration with SINAVE-Lab and SINAVE-Med will be contemplated; automatic circuits; Contact and daily follow-up with the citizen, in order to allow the proper signaling of cases that require another type of care”.

The development of a “reporting functionality of clinical outcomes (temperature; cough; ...) that will integrate with Trace Covid is also planned, so that the health professional accompanying the citizen can have access to them”. This “self-insertion” functionality will be included in the Citizen Area of the SNS Portal and the data collected there will be integrated into the Trace COVID-19 tool. In parallel, and for the same “self-insertion” functionality, an app11 will be developed.

During the inspection on May 19, it was found that Trace Covid-19 was already integrated with SINAVE-Lab.

The use of data from the support base for the Trace COVID-19 tool, after the emergency period that justified the creation of this tool, is still being considered by the DGS.

ASSESSMENT

a) Legal basis

The DGS assumes itself as responsible for the treatment, and the application was developed by direct determination of the DGS.

Article 9(2)(i) of the GDPR allows the processing of personal health data for reasons of public interest in the field of public health, based on the right of the

11 Application for mobile devices.

Member State providing for appropriate and specific measures to safeguard the rights and freedoms of the holder, in particular medical confidentiality.

However, Law No. 81/2009, of 21 August, which establishes a public health surveillance system, admits, in article 17, an exceptional regulatory power to the member of the Government responsible for the area of health, under proposal by the Director-General for Health, as a national health authority, for the adoption of essential measures in the event of a public health emergency in order to prevent the spread of infection or contamination. In turn, Decree-Law no. 124/2011, of 29 December, last amended by Decree-Law no. 12,012, empowers the DGS to issue norms and guidelines on public health. It is in this context that the processing of personal data known as Trace Covid-19 finds its forecast in DGS Norm No. in self-care and outpatient clinics in the context of the Covid-19 pandemic.

It should be noted that Article 9(2)(i) of the GDPR requires that adequate and specific measures be provided for to safeguard the rights and freedoms of the holder, in particular medical confidentiality, and these measures are not included in the Standard 4/2020, with the exception of the confidentiality requirement.

b) Authentication mechanism

Authentication in the Trace COVID-19 tool is being delegated to servers in the doud of Microsoft's Azure platform, with the synchronization of accounts created and managed on the AD servers of the various health entities with Azure AD.

The justification presented by SPMS for this option was the possibility of wider access to the Trace COVID-19 tool and because it allows the use of accounts already used in the SNS and the Ministry of Health (MS) and allows authentication to private entities external to the private health network. In addition, it allows the concentration of monitoring information on COVID-19, by aggregating, on a single platform, the management of infected users by the various health units, spread throughout the country.

12 Cf. also items a) and b) of paragraph 2 of article 2 of Regulatory Decree no. 14/2012, of 26 January.

AVG/2020/349 4v process.

National territory. It adds that it intends to extend the use of this authentication mechanism in the AAD platform in order to allow single sign on.

When choosing the authentication mechanism, it is important to bear in mind that the various applications used in the SNS contain highly sensitive information, which is subject to reinforced confidentiality rules (cf. Article 9(3) and subparagraph b)of Article 32(1) of the GDPR); and Trace COVID-19 is no exception, insofar as, for its purpose of managing patients with

suspected or confirmed Covid-19 in self-care and outpatient clinics, it contains the identification of these patients, as well as their home or place where are in confinement.

However, if it is recognized that the Azure AD mechanisms are secure to guarantee the authenticity of the access credential, one cannot help but express perplexity at the fact that a federated authentication model is not used for all SNS platforms, especially given that having each institution its own AD, the natural solution would be its federation in a distributed solution. And this is because the option chosen implies a centralization of all users of the SNS platforms (all health professionals and SNS workers) in Azure, which, regardless of the security measures adopted by Microsoft, unnecessarily duplicates user information.

Duplication of information is always a risk (i/.g., because synchronization can fail, because there are more points where changes can be made, even if carelessly) and if not necessary, it violates the principle of data minimization enshrined in the Article 5(1)(cj) of the GDPR.

In addition, AAD's contractualization is included in a "more general package for the provision of various services [...] and follows the standard contract" used by Microsoft, which assumes in this processing of personal data the quality of subcontractor (cf. paragraph 8) of Article 4 of the GDPR). In this way, the processor, in compliance with article 28 of the GDPR, should be contractually bound, among others, to the processing of personal data in accordance with the documented instructions of the person in charge, a situation that in Microsoft's standard contracts has not been to occur. It is therefore important that the controller corrects the situation in compliance with Article 28 of the GDPR.

c) Procedure for creating a user account

For professionals from institutions within the network of the Ministry of Health, requests for access to the Trace COVID-19 tool are validated by the service of origin and can be made in a reserved area on the Service Deskou portal, by sending a letter, issued by the Clinical Council or by the institution's Board of Directors. Requests can be made to one or more users and their respective institutional accounts are indicated.

For private health entities providing care within the scope of Covid-19, access to the tool is provided upon request made by the

institutions to which the professionals belong, including in the request the institutional email address of the users to whom it is intended. give access, for sending the respective credentials. The account is created directly at AAD, by SPMS, and the platform sends an email to the user's address with instructions for validating the account.

The person responsible for the treatment does not validate the professional profile of the access requests, leaving this responsibility on the side of the institution that requires the creation of access.

However, this procedure does not guarantee that users of Trace COVID-19 are effectively health professionals subject to professional secrecy, which weakens compliance with the provisions of subparagraph i) of paragraph 2 of article 9 of the GDPR. In fact, the person responsible for the treatment does not have any information that allows him to verify the reliability of the information transmitted by the institution that requires the creation of accesses, having no way of confirming whether it is a health professional subject to a duty of secrecy. When it is true that, as for the public institutions of the SNS, it is possible to carry out an integration with the MS systems for the users of these institutions.

In these terms, and taking into account that, regarding this processing, adequate and specific measures are not established in the national legal system to defend the fundamental rights and interests of the data subject, as required by subparagraph /^ of paragraph 2 of the Article 9 of the GDPR, it is important to create, at least, a mechanism that guarantees, on the side of the controller, that access is only granted to those who are health professionals subject to the duty of professional secrecy, as follows from the same rule.

d) Access profiles

The submissions received at the CNPD referred to the possibility of accessing the platform without apparent limitation in the universe of information available on it.

From the analysis of the information received, it can be concluded, as already mentioned, that there are three distinct profiles: local, regional, and national. For the definition of the user profile, “at the time of requesting access, the entity with direct responsibility for the professional (...) indicates the applicable profile.”.

That is, it is not possible to say that all the information is available to all users and, with the exception of users with a national profile, there is a limitation guaranteed by a filter built into the application, which cannot be removed by the user.

Regarding the local profile, in the SNS institutions, within each ACES there may be functional units and, within these, subunits. When dealing with a user of a health unit such as a Family Health Unit (USF) or Personalized Health Care Unit (UCSP), the smallest possible consultation universe includes data referring to all units belonging to the same grouping of the center. of health where your unit is located. In short, a user who works in a functional unit, within a given health center, will have access to the records of patients monitored in all units of the health centers belonging to the same ACES.

In the case of private entities, the visible universe of records does not have the same rule as public health institutions, being more limited. For private health groups, which aggregate several establishments, each of them has its own area in the Trace COVID-19 tool, and can only be consulted by the health professionals of the institution accompanying the patient. Users of the other entities of the group do not have access to this data.

Health authorities, local, regional and national, also have access to records corresponding to their area of competence.

The operations allowed for all profiles are the insertion and updating of patients, recording of tasks and surveillance, and the possibility of “transferring users between the unit responsible for surveillance”.

m: M'M: m

..1 NATIONAL COMMISSION

, ' DATA PROTECTION

Users only have access and registration privileges for information and, according to the SPMS, “mechanisms continue to be progressively implemented to prevent the alteration of user identification data, or that come from the integration of information from other systems, namely not allowing to change the fields of name, SNS number, identification document, contact.”.

Thus, it is concluded that, as regards public health institutions, although there are some mechanisms to limit access, the way in which the tool is built allows the sharing of personal data of all patients registered in the functional units dependent on an institution hierarchically higher, as is the case, for example, in the case of ACES.

Bearing in mind that an ACES can have several dozen functional units, the tool allows a user from any of these units access to the personal data of all patients registered in the set of functional units of the same group. However, this solution is not acceptable as it violates the principle of data minimization, enshrined in Article 9(1)(c) of the GDPR. In fact, since patients are only monitored by a functional unit, it is unnecessary for other users, outside that unit, to have access to the entire universe of

ACES patients.

e) Personal data processed

When consulting patients, the user has access to the following personal data: name, SNS user number, telephone contact, email address, taxpayer number, citizen card number, identification number of the social security, date of birth, gender, nationality, profession, educational qualifications, address, postal code, postal location, district, county and parish, health unit, body temperature, medication, cough, muscle pain, sore throat, headache, tiredness, dyspnea, risk score based on symptomatology, no symptoms, other symptoms.

The fields body temperature, medication, cough, muscle pain, dyspnea, tiredness, headache and no symptoms are binary (y/n) and mandatory. The body temperature field is numeric and is also required.

Data on test results are also processed by integration with SINAVE-Lab, surveillance status, surveillance start and end dates, start dates

and end of symptoms, and various surveillance records as well as date of discharge and death. Separate information about other symptoms/complaints or about the medical condition, past or present, can be entered in free text boxes.

During the inspection, doubts arose as to the need for the given address, which was, in a later communication, justified by the fact that, occasionally, there are teams of health professionals who carry out follow-up visits to the homes of patients under their supervision.

Personal data tax number, citizen card number or social security number, if justified at the time the person is entered on the platform, to prevent duplication in the absence of the SNS user number, have no relevance in clinical follow-up. of the patient under surveillance and, therefore, in compliance with the principle of minimization and confidentiality, provided for in subparagraphs c) and f) of paragraph 1 of article 5 of the GDPR, should not be available to users who do not have access privileges. data change.

Also with regard to recovered and deceased patients, given the purpose of treatment - monitoring and surveillance of patients in self-care - it is not understood why they remain in the database. Thus, the principle of data minimization, enshrined in Article

5(1)(c) of the GDPR, is again at issue.

f) Audit system

The Trace COVID-19 platform makes an audit record of the operations carried out, storing a wide range of information, including the following data: type of operation, date and time, username and IP address of the client machine. All information presented to the user, in the various operations performed, is also included in the audit log.

In the case of a user data query, the CNPD confirmed that the audit record includes the date and time the operation was performed, the user who performed it, the address of the machine where the query was performed, and the result of the search performed (all information presented to the user).

In practice, the audit record of the information consulted results in a reproduction of the clinical information of the users surveyed, which is clearly excessive.

However, an audit record to fulfill its purpose does not require the reproduction of all the information.

In fact, knowledge of the data that each user accesses can be obtained through the existence of a history of changes, with which it is possible to reconstitute the existing information at a given moment and which is subject to the same data protection rules implemented on the platform, along with the parameters used in the research, which were recorded in an audit.

On the other hand, it does not appear from the collected elements that the audit records contain information on the number of results returned by the search (e.g. no results, one result, multiple results), this is because it is also important to know the number of failed attempts.

Therefore, the content of the audit logs should be changed accordingly and a cryptographic mechanism must be applied that guarantees the integrity of the audit log, such as a digital signature.

g) Potential vulnerability 13

13

h) Traceability and notification mechanism

Pursuant to the provisions of paragraph 6 of article 29 of Law no. .

This mechanism is not implemented on the Trace COVID-19 platform, so the person responsible must make the necessary changes to comply with this legal obligation and, in this way, allow the data subject greater control over the processing of information concerning him, in the pursuant to article 35 of the Constitution of the Portuguese Republic.

i) Impact Assessment on Data Protection

Pursuant to Article 35(1) of the GDPR, whenever a processing of personal data, taking into account its nature, scope, context and purpose, is likely to entail a high risk for the rights and freedoms of individuals individuals, the controller is obliged to carry out, before starting the processing, an impact assessment on the protection of personal data. It is true that subparagraph b) of paragraph 3 of the same article specifies this obligation in cases of large-scale processing involving specially protected data, listed in paragraph 1 of article 9 of the GDPR, among which are data relating to health, there is no doubt that the RGPD imposes this obligation in the present case, assuming that the assessment can be carried out by the subcontractor, as follows from paragraph 8 of article 35.

However, the Trace COVID-19 platform was designed, implemented and used without this evaluation having taken place.

However, the importance of carrying it out is evident in the specific case. Indeed, if it had been carried out before the design of the technological solution, certainly the analysis of the impact of the processing of the data would have allowed to have detected some of the risks generated by it and the prevention of the (unnecessary) affectation of the rights and

freedoms of data subjects, through the adoption of appropriate measures to mitigate this impact, under the terms determined by Article 25 of the GDPR.

The fact that this assessment was not carried out and that, within it, data protection solutions were not considered from the start, adjusted to the risks that this platform entails, precisely led to the need for successive corrections in this information system. , as those risks were being communicated by users or detected by the subcontractor.

It can, with truth, be argued that the platform was created in a situation of public health emergency, to ensure a more efficient monitoring of patients and people suspected of infection, an emergency that even deserved the framework in the Decree of the

President of the Republic. 14-A/2020, of 18 March, and in subsequent decrees, declaring a state of emergency. And to invoke that, in view of the urgency in adopting measures that would guarantee the best response to this pandemic in good time, the performance of the impact assessment had taken a back seat in the priorities of the national health authority.

It should be noted, however, that the obligation imposed by Article 35 of the GDPR is considered crucial for compliance with the principles and rules of protection of personal data. In fact, this importance reflects the fact that such an obligation is not included in the set of obligations of the person in charge that can be excluded in the abstract by the legislator of the Member States of the Union, under the terms of Article 23 of the GDPR. In other words, the recognition of that legislative power derogating from the rights and obligations provided for in the GDPR does not cover, even in situations of constitutional exception of the Member States, the obligation to assess the impact on data protection.

Bearing in mind the raison d'être and the importance of this obligation imposed by the RGPD, it is nevertheless admitted that the public health emergency situation with which the DGS has struggled may constitute a situation that legitimizes concrete administrative actions praeter tegem, as well as as against legume. Indeed, it is common ground that both the state of administrative necessity (enshrined in Article 3(2) of the Code of Administrative Procedure) and the state of administrative emergency (regulated by special laws) are grounds for exclusion from illegality of concrete administrative actions to safeguard

AVG/2020/349 8v process.

the public interest which is in grave danger14. The question may arise whether a declaration of a state of emergency by a Member State is sufficient to justify the concrete action of the national administrative authority against an imposition of Union law, but it would seem that the urgent reasons of important public interest that legally legitimize an administrative action in violation of national law, they may also serve as a justification to legitimize the same action in violation of Union law. As long as, it is insisted, the concrete action of a public authority is at stake and not an abstract rule defined by the political-legislative power - because the latter, as we have seen, is excluded by Article 23 of the GDPR.

In any case, it seems relevant, in this specific exceptional framework of action of the controller, is that the function of the impact assessment (a function that is the reason for the non-derogation of the obligation to carry it out by national law) has been promoted in another way. In other words, it is important that, even if in another way, the final objective of the imposition of carrying out the impact assessment (i.e., the ratio of article 35) is pursued so that an “exceptional legality” can be affirmed.

This objective corresponds to the consideration of the means to be adopted to achieve a certain end, in the context of an identification of risks and the balance between the rights of data subjects and the purpose of public interest. As, strictly speaking, it is on this judgment of adequacy and necessity between means and ends that all administrative action in a state of need or in a state of emergency must be based, the CNPD cannot say, without further ado, that such a balancing has been made by the DGS.

As evidenced by the facts found in the present case, it may not have been carried out in terms sufficiently adjusted as to the result of the protection of the rights of the data subjects, but it cannot be said that a weighting was not carried out, in the light of the principle of proportionality, the suitability and necessity of the processing of data to be carried out through the platform in relation to the intended purpose.

Thus, in the present case, taking into account the exceptional situation of public health emergency that justifies the processing of data carried out by the national authority

14 In this sense, Diogo Freitas do Amaral, Administrative Law Course, II, 2nd ed., Almedina, Coimbra, 2011, p. 377; Paulo Otero, Legality and Public Administration. The meaning of administrative linkage to juridicity, Almedina, Coimbra 2003, pp. 996-997; Pedro Gonçalves, Manual of Administrative Law, Almedina, Coimbra 2019, pp. 391-392, 396-397.

responsible for the pursuit of the public interest in jeopardy, and taking into account that the CNPD cannot claim that the function or ratio of the GDPR rule that imposes the obligation to carry out an impact assessment has not been, in this specific exceptional context, pursued by a In a different way, “substituting the standard of normative compliance of action”15 of the national health authority (complying with an “exceptional legality” or alternative), it cannot be concluded that the non-compliance with Article 35 of the GDPR is unlawful.

Even so, the CNPD recalls that the impact assessment on data protection is an instrument capable of carrying out the aforementioned “weighted judgment of the adequacy and necessity between means and ends” in the context of processing of personal data that present a high risk for human rights. of the holders, thus proving to be an adequate instrument for the consideration to be made in exceptional administrative situations. For this reason, the CNPD emphasizes that, in principle, the

imposition of its implementation should not be excluded, even in cases of administrative need or emergency16.

j) Possible reuse of the database

Finally, it is important to consider the hypothesis, which will be considered by the DGS, of using the data from the support base for the Trace COVID-19 tool, after the emergency period that justified its creation.

In this regard, it is recalled that the processing of personal data is governed by the purpose limitation principle, under the terms set out in Article 5(1)(b) of the GDPR. Although, in certain circumstances, the reuse of personal data may be considered admissible, the sensitive nature of the personal data in question, the very wide universe of data subjects and the emergency situation that justified its creation are sufficient grounds for reinforced restraint on reuse is required here.

Indeed, it is important to bear in mind that this was a database created in exceptional circumstances for a well-defined and predictably transitory purpose, with an insufficient legal framework, due to the absence of adequate measures to

15 Paulo Otero, ob. cif., p. 908.

16 Maintaining that action against legem should only occur when the values, goods or public interests that are intended to be safeguarded cannot be safeguarded through means that do not involve departing from the norms that are part of ordinary legality, Paulo Otero, ob. cit, p. 907.

r

guarantee the rights of holders, and not preceded by an impact assessment that could have contributed to fill this gap. Bearing in mind the special and exceptional legal framework for its creation, and considering the principle of limiting data retention only for the period necessary for the purpose for which they were processed, enshrined in Article 5(1)(e) of the GDPR , the CNPD recommends that the conservation of this database be limited to the pandemic/epidemic period, especially because clinical information exists, or should be integrated, in the clinical process of each patient17.

However, its reuse for the purpose of scientific research may be justified, but, in the wake of the guidelines of the European Data Protection Committee and by virtue of the principles of data minimization, limitation of conservation and confidentiality, the CNPD understands that the information contained in the database supporting the Trace COVID-19 tool can only be reused for epidemiological research, with reinforced guarantees of protection of the rights of the holders (v.gpseudonimization)18. For

other scientific research purposes, the identification or identifiability of the people to whom the information relates is not essential, so reuse will only be allowed after an effective (irreversible) anonymization of the data19.

III. CONCLUSIONS

Since in the processing of personal data carried out through the Trace-COVID-19 platform, despite the measures adopted in the meantime, some principles and rules of the personal data protection regime are still in crisis, the CNPD recommends to the DGS:

17 In the sense that Union law requires that measures that represent restrictions on the rights of holders of data, adopted in this context, are limited in time, v. Statement on restrictions on data subject rights in connection to the State of emergency in Member States, approved by the European Data Protection Committee, available at https://edpb.europa.eu/sites/edpb/files/files/file2/edpb_statement_art_23gdpr_20200602_en.pdf

18 Cf. Guide/ines 03/2020 on the Processing of data concerning health for the purpose of scientific research in the context of the COViD-19 outbreak, approved April 21, 2020, in particular, §§ 44-45 and 51, available at https:/ /edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_202003_healthdatascientificresearchcovid19_en.pdf

19 See the European Data Protection Board Guidelines, cited in the previous note, § 46.

■TfWÈ

mm B

NATIONAL COMMISSION I, DATA PROTECTION

1. For the full application of the data minimization principle, enshrined in Article 5(1)(c) of the GDPR, the adoption of appropriate measures to ensure that:

1. The person responsible for the treatment only grants access to those who are health professionals subject to a duty of professional secrecy, as stated in Article 9(2)(i) of the GDPR;

ii. The access profile granted to a user of any ACES unit does not cover the personal data of all patients registered in the set of functional units of the same group, but only those of the respective functional unit;

iii. Data on recovered and deceased patients are deleted from the database;

iv. Users who do not have data modification privileges are not provided with the data “tax number”, “citizen card number” or

“social security number”, in order to also comply with the principle of confidentiality, enshrined in paragraph f) Article 5(1) of the GDPR;

2. For reasons of security and confidentiality of personal information, pursuant to Article 32 of the GDPR, the adoption of appropriate measures to ensure that:

i. The content of the audit records is amended in accordance with the requirements specified above, in point II, f).

ii. The information presented in the users' URL is evaluated;

3. In order to comply with the provisions of paragraph 6 of article 29 of Law no. 58/2019, of 8 August, the creation of mechanisms for traceability and notification to the holder of any access to their personal data;

4. In order to guarantee respect for the principles of data minimization, limitation of retention and confidentiality, enshrined in subparagraphs c), e) and f), of no.

AVG/2020/349 10v process.

Article 5 of the GDPR, the conservation of this database restricted to the pandemic/epidemic period, with the exception of the possibility of its reuse for epidemiological research, with specific guarantees, in particular, of pseudonymization.

Approved at the meeting of June 17, 2020

Filipa Calvão (President)