it's mJr M

IT IS NATIONAL DATA PROTECTION COMMISSION

RESOLUTION/2020/277

I. Introduction

1. The Institute of Systems and Computer Engineering, Science and Technology - INESC TEC submitted, on June 15, 20201, to the prior consultation of the National Data Protection Commission (CNPD) an impact assessment on data protection in regarding the STAYWAY COVID system, for tracking the spread of COVID-19, through the voluntary use of an application for personal mobile devices.

2. The system is an initiative of INESC TEC and the Institute of Public Health of the University of Porto (ISPUP)2, within the scope of the INCoDe.2030 program, and the work began to be developed in collaboration with the international project consortium DPA3T3, in response to the pandemic situation, and coinciding with the gradual lack of definition of the population in Portugal.

3. Its authors intend that the STAYAWAY COVID application works as a complementary measure, within the scope of a global strategy to combat the pandemic, thus seeking to make a significant contribution to the rapid interruption of infection chains, making available to the State the possibility to alert a user if he has been in close contact with other users of the application, who have been diagnosed with COVID-19.

4. The data protection impact assessment (AIPD), provided for in Article 35 of Regulation (EU) 2016/679 - General Data Protection Regulation (GDPR), concerns only the development of a technological solution that, if used, will involve the processing of personal data, although this treatment is not the responsibility of the Applicant. Therefore, there are certain aspects of the STAYAWAY COVID system that are not yet fully defined, as they will depend on the specific application they may have, which must be determined by the data controller.

' An updated version of the impact assessment was sent to the CNPD on 6/22/2020.

2 STAYAWAY COVID was developed by both entities with the support of the companies Keyruptive and Ubirider.

3 Acronym for Decentralized Privacy-Preserving Proximity Tracing.

r

5. In this sense, the analysis of the CNPD is also conditioned to the architecture of the system and its essential functioning, leaving open some specific questions whose assessment is subject to the way in which the STAYAWAY COVID system will be operationalized. However, the CNPD already puts forward some considerations on the legal requirements applicable to a future use of this system.

II. Description of the STAYAWAY COVID system

6. STAYWAY COVID (hereinafter “STAYAWAY”) is a digital proximity tracking system (contact tracing)4, which is intended to be made available for personal mobile devices with iOS or Android operating systems, and using B/uetooth technology as a proximity sensor , more specifically with low energy consumption (B/uetooth Low Energy- BLE).

7. From a technical point of view, STAYAWAY assumes itself not so much as a tracking solution, but more as an application for notification of individual exposure to contagion risk factors. Its objective is precisely to be able to inform an application user that their mobile device was at a distance of less than 2 meters, for more than 15 minutes, from the device of another person using the application who was later diagnosed with COVID. -19, with a risk of contamination, given the physical proximity and duration of contact5.

8. The STAYAWAY system adopts a decentralized model, that is, data is not collected, stored and processed on a central server, but on the user's mobile device. Risk calculation and user notification are performed locally on that device.

4 According to the World Health Organization (WHO), proximity screening is the process of identifying, evaluating and managing people who have been exposed to a disease in order to prevent its transmission. When systematically applied, proximity screening will interrupt chains of contagion, thus becoming an essential public health tool in controlling infectious disease outbreaks. See https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing__apps-2020.1

5 These distance and time variables, to calculate the risk of contagion, can be reconfigured according to WHO recommendations. Proximity contacts from the last 14 days are taken into account.

E: JÊM' JJf

m: ãÈJr" M

9. The system is based on a semi-decentralized architecture, consisting of personal mobile devices (DMP)6 and two central servers: the Diagnostic Legitimation Service (SLD) and the Diagnostic Publication Service (SPD), the latter of which stores and makes available the pseudonymized data of users diagnosed with COVID-19.

10. STAYAWAY makes use of the Google-Apple Exposure Notification System (GAEN)7, a joint project of the two companies and developed specifically to enable the operation of applications for proximity tracking via B/uetooth. However, according to GAEN, “only public health authorities can use this system” and only one application per country is allowed to access.

11.0 GAEN provides access to features8 at the level of the mobile device's operating system (iOS or Android), which are therefore not directly executed by the application.

12. With the exception of the features provided by the GAEN system, all STAYAWAY system software is open and will be made public before its release. Google and Apple provide the protocol specification, algorithms and the respective interface9, although the GAEN system code is not open. Also, manufacturers announce that the interface is subject to change.

13. Users who wish to join this notification system of individual exposure to the risk of contagion, download the STAYAWAY application to their mobile device through the official Google Play stores, if they have an Android system, or Apple Store, if they have a iOS, it is not necessary to make any additional registration for this application or open a specific account.

6 To this component is added the BLE interface and the interface for Internet access, in order to communicate the DMP with the central servers.

7 Google-Apple Exposure Notification. See https://www.apple.com/covid19/contacttracing and https://www.google.com/covid19/exposurenotifications/

8 Such as access to the Bluetooth component, the key generation protocol, the dissemination of pseudo-random identifiers between mobile devices, the crossing of pseudo-random identifiers to calculate the risk of contagion.

9 API - Application Programming Interface.

14. Once installed and configured, the application will pseudo-randomly generate a unique TEK identifier key10 daily, from which up to 144 pseudo-random proximity identifiers are generated, called RPI11, in a time interval between 10- 20 minutes.

15. RPIs are broadcast via B/uetoothe received by the personal mobile devices of other application users, who are geographically within range of those Bluetooth signals, where they are stored for a pre-defined period of 14 days12. In this way, all close encounters between users of the application are registered in a pseudonymized form on their personal mobile devices.

16. In the event that a user of the STAYAWAY application is diagnosed with COVID-19, the doctor accesses the Diagnostic Legitimation Service (SLD) of the application, through authentication, and obtains a code13, consisting of 12 digits, which he gives to the patient, externally to the system, that is, in person, by telephone or other means of communication. This is the way to validate that the diagnosis was made by an authorized healthcare professional.

17.0 SLD also records the date of the first symptoms or, in the case of asymptomatic infected, the date of the COVID-19 test, as well as the date on which this data must be destroyed.

18. At this stage, the patient, through the application, enters the code given to him by the doctor, which is valid for a single interaction, for a period of 24 hours, triggering the sending

10 TEK - Temporary Exposure Key. The initial TEK key is generated on the first run of the DMP after the application starts up, from the native pseudorandom number generators of the Android (Java) and iOS (Swift) platforms. TEK keys are stored in the respective DMP for 14 days.

11 RPI - Rolling Proximity Identifiers

12 RPIs are stored together with other data, namely date, duration and estimated distance of the contact.

13 The SLD simultaneously generates a pseudorandom legitimation code (CL) and a pseudorandom access code (CA), storing the CL and CA pair locally. The health professional receives the CL that he gives to the user/patient.

automatic TEK keys from the last 14 days, stored on your mobile device, to the application's Diagnostic Publishing Service14.

19. The Diagnostic Publishing Service (SPD) of the STAYAWAY application stores, on its server, for a period of 14 days, all TEK keys sent by users of the application diagnosed with COVID-19.

20. In order to calculate the risk of contagion with an infected person, it will be necessary to cross-reference the RPI received from other mobile devices with which each user was geographically close and which are registered on their own device with the RPI of users of the application infected with COVID-19. To this end, the application downloads the TEK keys stored there from the SPD, four times a day, at random times15. These keys will reproduce the initially generated RPIs and cross-reference them with the RPIs stored on the device to check if matches between the RPIs are detected. If so, the level of individual exposure to risk is calculated, based on physical distance and duration of close contact16, and an alert is presented to the user.

21. The alert of the existence of a risk contact does not mean that the person has been infected. Along with the alert, information is provided to the user on how to proceed.

22. On the mobile device, the application can present the user with three different states: no risk, alert of potential risk contact, diagnosed with Covid-19. In each of these states, additional information is displayed. In the case of a positive diagnosis, after the TEK keys have been communicated, by user action, the user is informed that the

THE

14 In this step, the DMP accesses the SLD without authenticating itself, provides the CL and obtains the corresponding CA in response. Then, the DMP authenticates itself to the SPD with the obtained CA, which is also only valid for one interaction, and submits the TEK identifier keys, which are stored locally in the SPD.

15 This is done incrementally, by reference to the last update.

16 This entire process is carried out in the DMP operating system through the GAEN interface. The contagion risk calculation takes into account the BLE signal strength, as well as the distance and contact time variables, configurable according to the WHO recommendations. At this time, they are established for contact less than 2 meters and lasting more than 15 minutes. Any positive hits that do not meet these conditions are not considered for the risk exposure risk calculation.

ave. D. Carlos I, 134 -1

1200-651 LISBON | WWW.CNPD.PT | TEL:+351 213 928 400 | FAX: +351 213 976 832

Go

STAWAWAY application “stops tracking contacts”, and the application must be reinstalled after recovery and return to normal life to restart the process17.

23. Finally, it is foreseen that the application will also have a Remote Switch functionality, which allows the platform administrator to temporarily suspend the operation of the system, if necessary, no longer collecting and disseminating codes, and reactivate it later .

24. According to the impact assessment carried out, the STAYAWAY system is expected to be discontinued at the end of the pandemic and the consequent erasure of all data.

III. appreciation

a) Data protection impact assessment

25. The data protection impact assessment (AIPD) was submitted to the CNPD, under the terms of Article 36(1) of the GDPR, as it was considered that, despite the identified risks being satisfactorily mitigated through measures proportionate to their impact and probability of occurrence, there are still potential risks, mostly inherent to the characteristics of the models, which should not be negligible, mainly due to the possible wide universe of users, to which others will be added, eventually, not yet identified, and may make the risk high.

26. It is understood that to carry out the processing of personal data resulting from the STAYAWAY system, it is legally required to carry out an IAPD, in accordance with subparagraph b) of paragraph 3 of article 35 of the RGPD, as there is in this context large-scale processing operations relating to personal health data, within the meaning of Article 4(1), 2), 5) and 15) of the GDPR.

27. The IAPD develops essential aspects, such as the description of the system, the analysis of risks and vulnerabilities, the application of data protection principles and the questioning of the future responsible for data processing, although some aspects are not

17 The app features a ‘tracking’ option (on/off), which is automatically turned off when the user communicates their TEK keys to the SPD, which means that they have been diagnosed with COVID-19.

sufficiently treated or not evaluated at all, which will be pointed out later. Therefore, and as stated in the AIPD itself, it should be reviewed and updated to reflect all aspects of the processing of personal data. After defining all outstanding issues regarding the operation of the STAYAWAY system, this reassessment is necessary to ensure that the implementation details of the application do not lead to increased risks for the privacy of data subjects.

28. The IAPD contains the opinion of the Data Protection Officer (DPO), under the terms of Article 35(2), who mostly classified the data processing, in its different perspectives, as "acceptable with recommendations" .18. In addition to measures to mitigate the identified risks, the EPD also recommended carrying out a pilot test under real conditions, limited to a portion of the national territory, before its wider and unrestricted availability. The CNPD recognizes that carrying out a pilot test, in which the application is only available to a specific and restricted group of users, can be beneficial for identifying and correcting security flaws.

b) The voluntary nature of the use of the application

29. With the evolution of the SARS-CoV-2 virus pandemic, technological solutions have multiplied in the world, in particular associated with the location of people as a way of identifying and reducing the spread of contagion, which immediately gave rise to a wide range of of concerns from the point of view of data protection and privacy, as they jeopardize these fundamental rights, and other fundamental rights are also affected, such as the right to non-discrimination, the right to circulate anonymously, the right to assembly.

30. Undoubtedly, the adoption of measures that, regardless of their technical design, always represent a risk of tracking the location and movement of citizens, should not have a mandatory nature, imposed by public authorities, because they clearly violate the principle of proportionality in a democratic rule of law. Despite an exceptional health emergency situation

18 On a scale of Acceptable/Acceptable with recommendations/Not acceptable

THE

public, the imposition of such a control - as if it were a panacea - would not comply with the principles of adequacy, necessity and proportionality.

31. The WHO, in guidelines dated 28 May this year, regarding ethical considerations for the use of digital proximity screening

technologies19, states that the effectiveness of this digital proximity screening as a means of detecting contagion chains is yet to be prove. On the other hand, it frames this type of solution as a way of intervening in a broader context of policies, interventions and investments. According to the WHO, this type of resources can exacerbate inequalities, as not everyone has access to these applications20 and can only benefit from them very indirectly, underlining that the bet on digital proximity tracking to the detriment of traditional approaches can reduce access. essential services to already marginalized populations, in particular the elderly or those living in poverty.

32. Taking into account all the reasons set out above, one can only fight for the voluntary nature of the application, which does not diminish the need to guarantee at all times the protection of the privacy of users and their personal data.

33. The STAYAWAY application, in the way it is designed, reinforces the voluntary aspect and the user's self-determination, giving him, in several stages, the possibility of choosing and controlling the data, even if pseudonymized, to be processed by the application. The first manifestation of will takes place when the application is installed on your personal mobile device. Subsequently, if you have a positive diagnosis for COVID-19, you still have the possibility of not communicating this information to the application, just by not informing the doctor that you are a STAYAWAY user or, even if

19 https://www.who.int/publications/i/item/WHO-2019-nCoV-Ethics_Contact_tracing_apps-2020.1

20 Not all smart phones can make use of this application, requiring newer versions of the devices, which reduces the universe of potential subscribers. Google announces that you must have at least one Android device version 6.0. (API version 23): https://static.googleusercontent.eom/media/www.google.com/en//covid 19/exposurenotifications/pdfs/Android-Exposure-Notification-API-documentation-v1.3.2.pdf

Apple indicates iOS version 13.5 or later: https://developer.apple.com/documentation/exposurenotification/buiiding_an_app_to_notify_users_of_covid-19_exposure

do so, do not subsequently enter the legitimation code into the system. This set of actions is entirely at your disposal and under your complete control.

34. In addition, there is also the possibility for the user to deactivate B/uetoothúo on his mobile device at certain times, stopping sending and receiving RPI codes (for example, when he is at home or in places where there is no proximity to other people), or turning off proximity contact tracking in the app's settings, with the same effect. Finally, you can also uninstall the application at any time, which would mean deleting your data. However, strictly speaking, the result of these actions is no longer under the control of the user, but essentially of the operating system managed by Apple or Google.

35. In short, the voluntary nature of the use of the application is essential, which must always be supported by respecting the principles of transparency, good faith and the lawfulness of the other participants in the system (cf. point a) of no. 1 of article 5 of the GDPR).

c) The use of BLE technology

36. The development of an application based on Bluetooth Low Energy (BLE) technology represents, in general, a less intrusive option than other technologies based on the direct geolocation of their users. As described, STAYAWAY fulfills its purpose of alerting users of the risk of possible contagion, by physical proximity to an infected person for more than 15 minutes, without it being necessary to know their location or that of third parties or the place where that encounter. risk occurred, let alone the identity of the other user.

37. In this way, the principle of data minimization (see Article 5(1)(c) of the GDPR) is observed, in particular by excluding data that are highly sensitive and especially protected from processing. by legislation on privacy in electronic communications21.

21 Law No. 41/2004, of 18 August, last amended by Law No. 46/2012, of 29 August.

38. However, the use of BLE is not excluded from user location risks22. In fact, this technology also allows mobile devices to be located with high precision, also when these devices are emitting signals, as in these cases, which can be read by receivers placed anywhere (in shopping centers, on the street, at airports , at railway stations, etc.).

39. The fact that the ST AY AW AY application only works with the BLE active23 forces the user, in order to use it, to leave the Bluetooth function active, making their device visible almost permanently, with the risk of tracking their location and your travels by third parties; unlike what happens now where BLE is mostly used for pairing devices, so its usual use can be easily controlled by the user and reduced in time. Even a careful user who carefully controls the features of their mobile device that

can indicate their location, such as GPS or WIFI, will be subject to location tracking through BLE when having the application installed.

40. Furthermore, according to wireless communication protocols, the transmission of active signals contains unique identifiers, such as the MAC address24 of the controller of the wireless network card25, which more easily make it possible to recognize and monitor a device, thus potentially a individual.

41. However, to minimize the risk of identifiability, it is possible to use a feature known as 'Bluetooth LE Privacy'26, which allows manufacturers to replace the MAC address of the Bluetooth interface with a random value that is changed at intervals, making it impossible the relationship with a single device and preventing tracking. The technical specifications of the GAEN system provide that a

22 Working Paper on location tracking from mobile device communications,

from the International Working Group of Data Protection in Te/ecommunications (IWGDPT), October 2015, in “Data Protection Forum”, no. 3, July 2016, p. 74

https://www.cnpd.pt/home/revistaforum/forum2016_3/files/assets/basic-html/page-74.html

23 According to what was confirmed by INESC TEC and which also results from the information publicly made available by GAEN.

24 MAC address (Media Access Control). Also referred to in this case as an advertiser address or vice address Bluetooth.

25 WNIC - Wireless Network Interface Controller.

26 https://www.bluetooth.com/blog/bluetooth-technology-protecting-your-privacy/

mechanism of that kind that generates a random address for the communication of RPI27 codes. It remains to be seen whether, for Google and Apple, who have the true address of the Bluetooth interface, it is possible to follow this chain or reverse the process. However, this procedure only applies to data transmission within the scope of the STAYAWAY application. Outside this context, the unique identifier of the BLE of the mobile device is transmitted, which raises the privacy issues described above in paragraphs 38-40.

d) The decentralized model of the system and its transparency

42. The semi-decentralized architecture of the STAYAWAY system, because it sends the storage of keys and identifiers received from third parties with whom a close contact has been made to the personal mobile device, as well as the crossing of identifiers to calculate the risk of exposure to the contagion, is a more appropriate choice from the point of view of data protection than having the information centralized in a single database.

43. On the other hand, this distributed model has safeguards in terms of pseudonymization, offering more guarantees of non-re-identification28, and makes it difficult to use data for other purposes, as well as its interconnection with other data processing.

44. It is also worth noting the public availability of the application's source code, which will allow an extended scrutiny of its behavior by the community, detecting possible security risks or risks to rights, freedoms and guarantees.

e) The system provided by Google and Apple

45. The STAYAWAY application is dependent on the GAEN system provided by these two great giants of the digital world for its functioning in the current way. if, for one

27 The document “Exposure Notification - Bluetooth Specification” provides the following: “The advertiser address type shall be Random Non-resolvable.” Available at

https://blog.google/documents/70/Exposure_Notification_-_Bluetooth_Specification_v1.2.2.pdf

28 Without prejudice to the observations made in paragraphs 58, 60-61, regarding the risks of re-identification.

On the other hand, this guarantees the robustness and security of technological solutions, at the same time that it allows the processing of information at the operating system level, on the other hand, it subtracts a substantial part of the operationalization of the application from the control of its creators.

46. On the other hand, the GAEN API code is not open, therefore not subject to scrutiny, although the technical specifications of the protocol, the cryptographic algorithms and the respective interface are publicly available.

47. One of the issues that raises the most reservations concerns the fact that the GAEN system can be changed, in an

uncertain direction29, by unilateral decision of those companies, which could put the behavior of the interface in crisis, with possible negative consequences for the application and for users.

48. As these companies already have large information repositories and provide very varied services at a global level, there remains a reasonable doubt about the possible benefit (current or future) that they may derive from the availability of this platform for contact tracing. proximity, through a technology that is in an ascending phase of use and that can constitute, for all intents and purposes, a supplementary means, perhaps more granular, to the existing localization methods.

49. If the data processed in the context of this type of application is somehow used for other purposes, the system's guarantees are compromised, first of all because pseudonymization is impaired and the risk of user identification is much greater. It is admitted, however, that this is a difficult issue to overcome, and that it only accentuates the need for users to make informed choices.

50. This aspect is, of course, one of the critical points of this type of application, which also includes STAYAWAY. In any case, any changes to be made to the GAEN interface must be promptly notified to users, so that they fully understand the practical consequences of the change.

29 As stated in the preliminary analysis carried out by the suppliers of the GAEN system, it is subject to modification and extension.

r

NATIONAL COMMISSION

DATA PROTECTION

f) Processing of personal data in the STAYAWAY system

51. The STAYAWAY system essentially provides for the treatment of pseudonymized data, the probability of re-identification of which will be dealt with later on when we focus specifically on the analysis of risks and vulnerabilities, without prejudice to the critical remarks made in this chapter.

52. Pseudonymized data is, however, personal data, and non-pseudonymized data is also processed. In general terms, it is considered that there was a concern for respect for the principle of data minimization, for the principle of accuracy, and for the principle of limiting the conservation of data, which have a short storage period30, in strict compliance with the fulfillment of the

purpose of processing (cf. points b), c), d) and e) of Article 5(1) of the GDPR). However, there are some notable shortcomings that need to be addressed.

53. The AI PD states that people who want to download the application do not need to create an account or identify themselves. Now, if this is not specifically required by reference to STAYAWAY, the truth is that it is not possible to download any application from official Google or Apple stores, even free ones, without the user authenticating himself, so it becomes, at least , of the direct knowledge of these companies that that person, identified (even with an associated credit card), is a user of STAYAWAY.

54. As for the data processed during the regular operation of the system, it appears that the RPI are associated with the date, thus making it possible to know the date of exposure to the infected person. This information is assumed to be useful, but nothing is said about the benefit of using it and how this information will be used or transmitted, which would naturally be relevant.

55. It is also noted that the exposure risk alert that is presented to the user, when a close contact with an infected person is detected, based on the last occurrence, remains in the application until it is uninstalled. Now, this situation can

The identifiers are kept for a period of up to 14 days, in any component of the system; Risk alerts are kept on the mobile device with the date of occurrence of the most recent proximity contact that gave rise to it until the application is uninstalled.

no longer correspond to the truth if the user, following the notification, performed a COVID-19 test with a negative result, so the status presented should be 'no risk'. This procedure should therefore be reviewed so that the information is updated at all times, in compliance with the principle set out in subparagraph d) of paragraph 1 of article 5 of the RGPD.

56. As for the data treated in the SLD, on the date of the first symptoms or the date of the test in the case of asymptomatic individuals, neither is advanced nor explained the purpose of this information. In addition, it is unknown how this information is introduced into the system, whether by the health professional and, in this case, with the knowledge and prior authorization of the patient; directly by the patient. It is also not explained when this information is entered and, therefore, if filling in these fields is a condition to proceed with obtaining the legitimation code. Furthermore, an automatic erasure of this information seems to be foreseen, since an expiration date for the data entered is also stored in the SLD, but the period of retention is unknown.

Even assuming that, in the context of epidemiological control or the analysis of the effectiveness of the application itself, knowledge of these dates is relevant, it will be necessary to clarify their purposes and the conditions for the processing of these data.

57. Still in terms of the SLD, it is understood that nothing is advanced regarding the context and form of authentication of health professionals to obtain the CL codes, although it is admitted that this will be one of the issues deferred to a later stage legal framework and definition of the controller. In any case, it is extremely important that the solution adopted does not jeopardize the security of the system.

58. With regard to the data processed in the SLD and SPD, it is also verified that a universal unique identifier (uuid) is treated without reference to what is being identified. Indeed, in the description of the data structure of the AI PD servers31, there is the treatment

31 This universal unique identifier is also integrated into the access code (CA), which is subsequently stored in the SPD, although it is not described for how long or if this coincides with the retention period of TEK keys, which is 14 days.

of this data. It should be noted that nothing is mentioned about the purpose of processing this data, how it is used or how long it is kept.

59. Depending on what this unique identifier refers to, its treatment may have an impact on the user's privacy if it somehow allows the user to be unequivocally individualized and, therefore, to be able to monitor their interactions with the central servers of the STAYAWAY system. In order to assess its suitability and necessity, it is essential to explain its objective within the scope of operating the system. It must be demonstrated that the processing of this personal data in the SLD and in the SPD complies with the data minimization principle set out in Article 5(1)(c) of the GDPR.

60. Regarding the processing of data relating to the IP address of the user who communicates with the SPD, it is stated that this is processed for purposes of system security and control of intrusion attempts and only accessible by system administrators. It is recalled that the IP address is personal data, as it makes it possible to identify, without disproportionate

effort or cost, who was the person who accessed the server via the Internet (cf. point 1) of article 4 of the GDPR and jurisprudence of the Court of Justice of the European Union (Case Breyer, C-582/14, points 44-49, ECLI:EU:C_2016:779).

61. Even without resorting to information held by third parties to identify the user, the IP address immediately makes it possible to know an approximate geographic location of the users32. Bearing in mind that application users access the SPD four times daily, and that, in addition, some users can be referred to as people with a positive diagnosis for COVID-19, when they authenticate to send their special TEK keys Safeguards must be adopted regarding the processing of this personal data.

62. The purpose indicated for storing IP data, for a short period of time, is considered legitimate, although it must be sufficient to fully fulfill the purpose in view. However, to minimize the risks of misuse and in line with the best practices followed in this field, the STAYAWAY system must introduce a reverse proxy mechanism, masking the users' IPs, which should

32 In case users access from an institution where they work, for example, the IP may also reveal the user's association with that institution.

t

preferably be managed by a separate team, that is, the administration and support functions of STAYAWAY must be segregated from those of infrastructure security.

g) The rights of users as data subjects

63. One of the key points for a transparent processing of personal data that allows the data subject to make an informed choice and, also to that extent, truly free because it stems from a conscious choice, is the prior information provided to him in relation to the conditions of the proposed treatment of your personal data.

64. According to AI PD, it is expected that information will be provided to the user, either on the STAYAWAY website or in the application itself. It is important that this information is provided in compliance with the intelligibility requirements of Article 12 of the GDPR and taking into account the different audiences that may be at stake here, in particular more vulnerable groups such as children, who have modern mobile devices (in versions necessary for run the application) from an age below 13 years33.

65. The information regarding the operation of the application itself must also be clear, so that users can use it correctly, thus contributing to the fulfillment of its objective, without prejudice of course to your option of not providing any more data or

uninstalling the application at any time. .

66. With regard to the exercise of the other rights provided for in the RGPD, as it is not possible to identify the data subject from the processed data, the rights are not applicable under Article 11(2) of the RGPD.

h) Other risks and vulnerabilities

67. When carrying out an analysis of system risks and vulnerabilities, in addition to some risks already mentioned above, the AI PD examines various scenarios of attempts to re-identify data subjects using external systems or inference from the data subjects themselves.

33 With reference to the age provided for in Law No. 58/2019, of 8 August, implementing Article 8 of the GDPR, to consent to the processing of your personal data when information society services are specifically addressed to you.

users, and in the latter case, this is intrinsic to an individual exposure notification system, which leads to an attempt to reconstruct past contacts when there is a case of infection. The success of this exercise largely depends on the particular conditions in which each user moves (number of proximity contacts, locations/pace of travel). In general, the CNPD agrees with the result of the analysis carried out and with the measures planned to mitigate these risks.

68. The severity and probability of the listed risks, in relation to threats and sources of risk, with the implementation of certain controls and policies, is classified by the IAPD as 'limited' or 'negligible'34.

69. The possibility of creating false alerts based on malicious forwarding of illegitimate RPI from users diagnosed with COVID-19 was also analyzed. Since these interactions take place in the mobile device's operating system, this vulnerability would have to be resolved by GAEN, without prejudice to other forms of mitigation that can be implemented at the system level.

70. In short, from the point of view of data processing security, important measures provided for in article 32 of the GDPR were adopted, in particular the pseudonymization of data, to complement relevant measures arising from the application of the principle provided for in article 25. ° of the GDPR, regarding data protection by design and by default. The automatic erasure of data and its short storage are essential in order to minimize the level of impact on people's rights in the event of security

incidents. It should be noted that the creators of the STAYAWAY application do not have full control of the data processed, since the treatment carried out by the operating system of the user's mobile devices is the responsibility of the GAEN system.

IV. Future use of the system

71. As mentioned in the Introduction to this determination, there are still some uncertainties regarding the operation of the STAYAWAY application, resulting not only from the lack of knowledge of the

34 On a scale of Undefined/Insignificant/Limited/Significant/Maximum.

r

responsible for the treatment and its determinations in relation to specific issues, such as the intervention of the health professional in this system, but also the evolution of the scenario of interoperability with other applications for the same purpose in the European Union space and in other geographic spaces.

72. However, the CNPD cannot fail, in this context, to put forward some elementary considerations for a future use of STAYAWAY or another similar application.

73. As stated by the Apple/Google partnership, access to the GAEN interface for operating exposure notification applications based on proximity contact tracing is only granted for use by public health authorities and only to a single application per country, considered an official application.

74. Consequently, for the functioning of STAYAWAY to be possible, there must be the active involvement of the public health authority, hence the indispensability of the data controller being a national public entity with attributions in the area of health and specific competences adjusted to the purpose of the application.

75. On the other hand, given the very purpose of the application, which is assumed as a complementary means in the national strategy to combat the pandemic, providing an additional instrument to detect people potentially infected or at risk of contagion, directing them to medical surveillance and / or confinement and, thus, contribute to interrupting the disease transmission chains, the public availability of the application must be integrated into national planning appropriate to this scenario.

76. Indeed, from the point of view of data protection, in light of the provisions of Article 9(2)(i) of the GDPR, it is necessary that a legal framework be given to the controller who, in turn, it must be able to take certain decisions, possibly based on the

important public interest of protecting public health in a pandemic situation, but always guided by the principle of proportionality and with adequate safeguards, as prescribed by the GDPR.

77. Especially because, throughout this process, the essential intervention of a health professional (physician), to validate the diagnosis and be able to advance the detection of possible close contacts at risk and the corresponding notification system, also

r

i live

§ NATIONAL DATA PROTECTION COMMISSION

seems to depend on a legal framework for the application to work, therefore the user's voluntary adhesion is not enough.

78. In fact, considering the relevance, for the reliability of the information system, of this medical intervention, it seems essential to foresee and regulate it at the legal level, not only to legitimize it, but above all to ensure that it occurs, under penalty of the functioning of the notification system is left to the physician's availability.

79. It is also very important for the overall security of the STAYAWAY system and for the maintenance of the pseudonymization of the data processed in the application that the form of authentication of the doctor in the SLD, as well as the conditions of his interaction with the system, are duly safeguarded.

80. It should be noted, however, that the requirement of legal regulation of this treatment does not rule out the voluntary nature of the use of the application by the user - and that it is essential to maintain it, as indeed follows from the recommendations of the WHO, the European Commission35 and the European Committee of Data Protection36; The condition of lawfulness of processing proximity and health data is, in the first place, the consent of the holder, corresponding to his unequivocal expression of will to install the application on his mobile device, provided that the four requirements that make his valid consent (provided for in Article 4(11) of the GDPR).

81. But as the operation of the application implies different processing operations that involve different categories of holders (users and health professionals), in addition to the requirement made by the GAEN system for the operation of the application, the data processing carried out requires a double condition of lawfulness of this treatment, which only reinforces its legitimacy and makes the treatment more proportionate.

82. Finally, mention should also be made of the issue of the interoperability of the national application with other applications within the Union, following the agreement reached this month between the Member States on a set of technical specifications37, with a view to exchanging information between national proximity contact applications based on

35 https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:52020XC0417(08)&from=EN

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

https://ec.europa.eu/health/ehealth/key_documents_en#anchorO

THE

decentralized models. The European Commission is expected to provide a platform through which information on the various national applications will be exchanged when users travel within the Union.

83. Not everything is defined yet and there are different options to identify the countries through which a given user traveled. In any case, it is clear that more personal data will be processed. On the other hand, interoperability brings additional risks regarding the protection of personal data and privacy, as the system becomes open and interacts with other systems that, even with similar models, will have different data structures, different safeguards, different forms of administration.

84. It is therefore of the utmost importance to ensure that with interoperability, data protection safeguards do not succumb to a lowest common denominator; on the contrary, a high level of protection should be sought, presided over by the transparency of the entire process and with scrupulous respect for the principles of purpose limitation, data minimization, conservation limitation, integrity and confidentiality.

V. Conclusions

Based on the above grounds, the CNPD considers that:

85. The STAYAWAY COVID system, initiated by INESC-TEC and ISPUP, maintains some uncertainties as to its functioning, which depend on the concrete execution that they may have, to be determined by the data controller, so the pronouncement by this Commission on some specific issues will also be deferred to a later date;

86. The system must preserve its voluntary nature, and the user must be provided, as foreseen, several moments in which he

can freely make choices regarding the treatment of his data, including the effective possibility of turning off Bluetooth, configuring the application not to trace proximity contacts and uninstall the

application, resulting in the interruption or permanent erasure of your personal data;

87. The use of Bluetooth technology appears to be less intrusive than the use of a technology that allows the immediate recording of the user's location; however, it is not without risks and, as it is essential that the BLE is active for the application to work, it is enabling the constant tracking of the location and movements of users by third parties;

88. The decentralized model of the STAYAWAY system is more suitable from the point of view of data protection as it disperses processing operations, avoiding centralized processing of all data, which would entail additional risks of misuse, data interconnection or re- identification of users. The fact that the application's source code will be made public is an important transparency factor;

89. The use of the Google and Apple interface is one of the most critical aspects of the application, as there is a crucial part of its execution that is not controlled by the authors of the application or the controllers. This situation is even more problematic because GAEN declares that its system is subject to modifications and extensions, by unilateral decision of the companies, without being able to anticipate the effects that this may have on users' rights;

90. In compliance with the principle of transparency, data subjects must always be aware of all aspects of the operation of the application and its implications for the processing of their personal data and for their privacy, and must maintain control of their data. . This is all the more important as many interactions occur automatically, without the user being aware of them;

91. Although it is recognized, in the design of the system, that there was a concern for the principle of data minimization and for the pseudonymization of data, it is foreseen the treatment of some data in addition to the pseudorandom identifiers that support the notification system, which are not are evaluated in the AIPD, their purpose, their insertion in the system, their transmission or their retention period being unknown,

, so it is essential that this be clarified;

92. The impact assessment must be reviewed, taking into account the critical aspects highlighted by the CNPD and which were not analyzed, namely the omission regarding the purpose and conditions of data processing (cf. date of the RPI, date of first symptoms or COVID test date for asymptomatic, universal unique identifiers), as well as taking into account some additional recommendations made, regarding the indefinition of some conservation periods or regarding the IP of users when communicating with the Diagnostic Publications Service.

Still on the subject of the impact assessment carried out, but regarding aspects of the treatment of personal data that are not yet defined, the CNPD recommends that:

93. A legal framework is given for the operation of the STAYAWAY system, not only because access to the GAEN interface is only granted to public health authorities, and only to one application per country, but also the reliability of the system depends on the validation of the medical diagnosis , so it is essential to foresee and regulate the intervention of that health professional at the legal level. Special safeguards must be adopted regarding the way the doctor authenticates himself and interacts with the system to guarantee the global security of STAYAWAY and to maintain the pseudonymization of the processed data;

94. The requirement of legal regulation of this treatment does not detract from the voluntary nature of the use of the application by the user. The legal condition of personal health data and the respective proximity contacts is, in the first place, the consent of the data subject, corresponding to their unequivocal expression of will to install the application on their mobile device, provided that the four requirements that make your valid consent. Given the way in which the application works, which involves different processing operations, involving two categories of data subjects, the processing will require a double condition of lawfulness, which only reinforces its legitimacy;

95. Interoperability between national proximity contact tracing applications implies the processing of more data, more communications and more recipients, so it is necessary to ensure that the options taken in this context respect the principles of data protection, in particular the principle of minimization. Likewise, it must be ensured that, with interoperability, data protection safeguards

do not succumb to a lowest common denominator, but rather seek to achieve a high level of protection for the privacy of their

users.

Approved at the meeting of June 29, 2020

Filipa Calvão (President)