National Data Protection Commission

OPINION/2023/3

I. Request

1. The Executive Manager of the National Strategy for the Integration of Homeless People 2017-2023 (ENIPSSA) asked the National Data Protection Commission (CNPD) to issue an opinion on the draft of the Collaboration and Management Protocol of the Platform for Monitoring and Management of Homeless People's Processes within the scope of ENIPSSA 2017-2023 (hereinafter Protocol).

2. The request for an opinion was accompanied by four additional documents to the draft Protocol, called the Partnership Protocol, Annex IV - Confidentiality Commitment, Consent and Impact Assessment on the Protection of Personal Data (AIPD).

3. From the analysis of the documents sent by ENIPSSA, doubts arose and it was verified that the document designated Impact assessment on the protection of personal data did not substantiate a true assessment of risks related to data protection, rather being an opinion prepared by the Sector of Risk Management /GAQGR of the ISS, IOP, on the AIPD, for which clarifications and the sending of documents were requested.

4. The CNPD issues an opinion within the scope of its attributions and competences as an independent administrative authority with authoritative powers to control the processing of personal data, conferred by paragraph c) of paragraph 1 of article 57, paragraph b) of paragraph 3 of article 58 and paragraph 4 of article 36, all of Regulation (EU) 2016/679, of April 27, 2016 - General Regulation on Data Protection (hereinafter RGPD), in conjunction with the provisions of article 3, paragraph 2 of article 4 and paragraph a) of paragraph 1 of article 6, all of Law no. 58/2019, of 8 August, which implements the GDPR in the internal legal order.

5. The National Strategy for the Integration of Homeless People (2017-2020), approved by Council of Ministers Resolution No. 107/2017, of June 29, and amended by Council of Ministers Resolution No. 2/202, January 16, aims to "[cjonsolidate a strategic and holistic approach to prevention and intervention, centered on homeless people, so that no one has to remain on the street due to lack of alternatives" (Point 1 of Annex I to Council of Ministers Resolution No. 2/202, January 16).

6. Under the terms established in those normative diplomas, ENIPSSA 2017-2023 is based on three strategic axes: Axis n.° 1 - Promotion of knowledge of the phenomenon of homeless people,

I. Analysis

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

information, awareness and education; Axis No. 2 - Reinforcement of an intervention promoting the integration of homeless people; Axis No. 3 - Coordination, monitoring and evaluation of ENIPSSA 2017-2023.

7. The intervention model to be used for the implementation of ENIPSSA "applies to all cases that are found in a homeless situation, which require specialized intervention, and during the necessary time until a solution is found and stabilized ", therefore, it is necessary to carry out a diagnosis of the situation and follow-up of cases of homeless people (point 4 of Annex I to Council of Ministers Resolution No. 2/202, January 16), through the bodies and structures provided by law.

8. The bodies and structures of ENIPSSA 2017-2023 are the Interministerial Commission, the Strategy Implementation, Monitoring and Evaluation Group (GIMAE) - composed of public capital entities and private entities listed in point 6.3 of Annex I to the Council Resolution of Ministers No. 2/202, January 16, and other entities that may be invited - , the Consultative Commission and the Homeless Planning and Intervention Centers (NPISA), the latter created within the scope of the Local Action Councils (CLAS) when the situation justifies it.

9. Furthermore, ENIPSSA 2017-2023 includes the executive manager who, under the guidance of the member of the Government responsible for the area of Labour, Solidarity and Social Security, ensures the management and coordination of ENIPSSA, being responsible, namely, for the articulation between the various bodies and structures of the Strategy, as well as the coordination of GIMAE and the executive core, as well as accompanying, monitoring, streamlining the pursuit of objectives,

resources and strategies for implementing measures and policies and intervention for homeless people (point 6.2. of Annex I to Council of Ministers Resolution No. 2/202, January 16).

10. Law No. 75-B/2020, of December 31, which approves the State Budget for 2021, provided for the interconnection of data between units, services and public bodies or other public institutions and the entities participating in ENIPSSA , 2017-2023, for monitoring the situation through a platform (paragraph d) of paragraph 1).

11. The aforementioned law provides that the "transmission of personal data between the aforementioned entities must be subject to a protocol that establishes the responsibilities of each intervening entity, whether in the act of transmission or in other treatments to be carried out" (no. two).

12. Paragraph 3 also enshrines, in a non-exhaustive manner, the content of the aforementioned protocols, as well as providing that they are ratified by the Government members responsible for the respective sectoral areas.

National Data Protection Commission

13. The Protocol under analysis, submitted to the CNPD for appreciation by the Executive Director of ENIPSSA, is signed between the Instituto de Informática, I.P., (II, I.P.) and some of the institutions with representatives at GIMAE -Instituto da Segurança Social, I.P., (ISS, I.P.), Santa Casa da Misericórdia de Lisboa (SCML), National Institute of Statistics, I.P., (INE), National Civil Engineering Laboratory (LNEC), National Federation of Rehabilitation Entities for the Mentally Ill (FNERDM), DLBC NETWORK Lisbon - Association for Community Based Local Development of Lisbon (REDE DLBC Lisbon) and European Anti Poverty Network Portugal - European Anti-Poverty Network/Association (EAPN Portugal).

14. 0 II, IP. intervenes in this Protocol by being the "public legal person that ensures the construction, management and operation of application systems and technological infrastructures in the areas of information and communication technologies of the services and bodies dependent on the Ministry of Labor, Solidarity and Social Security", into which ENIPSSA is integrated.

II. Object and purposes of processing

15. It is the purpose of the Protocol "to establish the terms and conditions of data access between entities, services and public bodies or other public institutions and the entities participating in ENIPSSA 2017-2023 for monitoring the situation of

homelessness through a platform (AidHound Platform), with a view to the future conclusion of an interconnection protocol, as provided for in paragraph d) of paragraph 1 and paragraph 2 of article 356 of the State Budget Law for 2021, approved by Law No. 75-B/2020, of December 31" (Clause One).

16. It is intended that, within the scope of ENIPSSA, Partnership Protocols (Annex III) be signed within the scope of the Social Network of Local Councils for Social Action (CLAS), between the social partners that constitute the Nucleus of Planning and Intervention Without -Shelter (NPISA), which aim to create and implement the respective NPISA, define commitments to be ensured by the partner entities (clause 1 .a of the Partnership Protocol).

17. These Partnership Protocols provide for the competences of the NPISA, emphasizing, for what matters now, carrying out a local diagnosis on the phenomenon of homeless people, monitoring the individual insertion processes (paragraphs a) of the no. 1 and c) of no. 2 of Clause 4.a).

18. Furthermore, it is established that the monitoring and management of processes of homeless people is carried out, namely, through the Information System (SaaS), which is used by different local, public and/or private entities involved in the process (No. 1 of Clause 6 of the Partnership Protocol).

Av. D. Carlos 1,134,1°

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

gerai@cnpcl.pt

www.cnpd.pt

19. It is said that the processing of personal data is intended to support technical interventions with homeless people who need to receive differentiated treatment, within the scope of monitoring the situation through a platform, as approved by the Law of State Budget for 2021, intending, with this application, to promote an essentially provident and protective action of the population of homeless people, in order to allow the consolidation of the strategic approach of prevention and integration pursued by ENIPSSA (Clauses Third and Fourth).

III. Data subjects and data categories

20. The data subjects are homeless people in mainland Portugal, in the geographic area of the NPISA, with data collection being carried out directly, through a face-to-face interview or telephone contact, with the collection of informed consent (n. 4 of Clause Two).

21. In accordance with the AIPD, special categories of data are processed on a large scale, specifically health data1- The personal data processed are contained in Annex II to the Protocol and comprise the following categories: Basic characterization data (name , date of birth, gender, nationality, telephone and email contact), Identification data (marital status, place of birth, citizen card numbers or identity card, SNS user, driving license, if you are a foreign citizen, also, the passport number and indication of the issuing country, residence permit number, situation in the country and means of entry into the country); Signaling, which comprises data that allow assessing the situation of homelessness or homelessness, the georeferencing of the place to stay overnight, the circumstances that led to the homelessness situation and the receptivity to the intervention; Data on education and employability, Financial sustainability, Physical and mental health data, including dependencies, are also collected; Data relating to the household and on the existence and characterization of an informal or formal/institutional support network; and Other records about the user (activities developed within the scope of the intervention), referring to the intervention plan, the forwarding of responses to the follow-up of services, among other aspects.

1 Assigned Family Physician? Yes No; Enrolled in the health center? Yes No; Diagnosed serious or chronic illness? Yes No; List of serious or chronic disease(s); Diagnosed mental illness? List of mental illness(ies); Physical disability diagnosed? List of physical handicap(s); Diagnosed dependencies? List of diagnosed dependencies; Do you have physical autonomy? Do you have psychic autonomy? Does it have intellectual autonomy?

IV. 0 data processing to be carried out and system operation

22. The Protocol regulates the use of the AidHound Platform, "a fully digital and online case management system [...], which falls under the category of SaaS and is accessed only via a browser".

23. The following objectives are identified in Clause Three of the Protocol and in the AIPD document: "Promote the technical quality of the intervention; Greater effectiveness and efficiency in the intervention; Guarantee the quality of responses and services provided; Ensure that no one is deinstitutionalized without measures and support have been activated to guarantee a suitable place to live, whenever justified; Ensure that no one has to remain on the street for more than 24 hours; Ensure technical support when leaving a Temporary Accommodation for the necessary time; Ensure the existence of conditions that guarantee the promotion of autonomy through the mobilization and contracting of all available resources according to the diagnosis of need; Foster the increase of accommodation solutions for homeless people; Allow use at national level of a unique concept of homeless people; Providing training, education, professional training and professional insertion solutions; Ensuring access to social protection measures; Ensuring access to health care; Ensuring access to measures to support the integration of migrants; Ensure the coordinated functioning of ENIPSSA bodies and structures."

24. According to the documentation sent with the request, this platform will make it possible to record the data of users who consent to the intervention, monitor and manage the processes of homeless people, share data with other systems and transmit data between public entities, services and bodies or other public institutions and entities participating in ENIPSSA 2017-2023.

25. Also according to this documentation, data processing is automated, with user profiles being defined that limit access according to geographic area, scope or type of data. There is also provision for the occasional or periodic review and update of access to the platform.

26. The retention of audit records (log) is also envisaged. From the complementary information provided by the MTSSS, it appears that logs are recorded for all operations (date, IP address, user ID and result of the operation), that all types of operations are the object of this record and that, in the case of queries, they are the input parameters are also recorded, and these logs are kept for two years.

Av. D. Carlos 1,134,10

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

27. Clause Twelve defines some means and security measures that the participants in the protocol must implement. However, the list presented there2 will still have to be added means to keep the systems that access the platform up to date. Ideally, taking into account the nature of the data processed, it is suggested that the platform be used via a dedicated connection or VPN.

28. Clause Ten establishes the sending of pseudonymized information to INE, “by encryption at the source through an executable (application of a hash with the SHAA256 algorithm) provided by INE, through secure communication channels, resorting to the encryption of communications (HTTPS communications protocol), using the INE private cloud" (n.º 3), however, the way in which the sending is triggered is not specified - manual, automatic, periodicity, nor who triggered it.

29. And, in fact, it is not clarified which personal data are the object of the pseudonymization process.

30. From the information received, it appears that by stating that the hash is applied to the "identifiers referred to in Annex 2", it is intended to say that it applies to all identification data - in particular, marital status, place of birth, number of CC or BI (if Portuguese nationality), NIF, NISS, SNS User Number, Driving License Number, Passport Number, Passport Issuing Country (if foreign citizen), Authorization Number Residence (if a foreign citizen), Year of entry into the Country (if a foreign citizen), Situation in the Country (if a foreign citizen), Means of entry into the Country - which could mean that the remaining data will be transmitted in clear, that is, identified , leaving the immediate doubt as to whether the basic characterization data are covered by the set of identifying data. It is important to clarify which data to send, which of these will be clear, that is, identified, and which will be pseudonymised.

31. In any case, we draw attention to the fact that the supposed irreversibility of the pseudonymization process, which is invoked in the complementary information transmitted to the CNPD, is easily invalidated, as the way in which data are constructed, such as the NIF or the NIC (BI/CC), thus being able to arrive at the numbers to which each hash corresponds and, consequently, the identification of the data subject.

32. It is further stated that "anonymous data are stored in the same database [as the others], but are not visible, being categorized in order to filter their visibility".

2 a) Use of secure equipment and connections to access the platform; b) Allocation of profiles to users respecting the need-to-know principle; c) Control over authorized users; d) Control or suppression of the production of copies or reproductions, preserving the information residing on the platform; e) Guaranteed closure of sessions on the platform, in the absence of authorized users; and f) Access profiles protected by a personal and non-transferable password

follows the practices recommended in the RGPD (cf. recital 29) for the pseudonymization process - which consists of maintaining "the separate storage of additional information that allows the attribution of personal data to a specific data subject" - and which applies, for the most part, to anonymized data, must be accompanied by guarantees regarding the form of research by legitimate entities only accessing anonymized data, so as not to allow free searches that lead to the identification of data subjects.

33. With regard to sending data to INE, and in accordance with the answers to the questions posed by the CNPD, ISS, I.P, SCML and II, I.P. may transmit data to INE's private cloud, manually, with a periodicity to be defined (predictably quarterly). In the case of a single system, to which the administrator profile has full access (paragraph i. of point 3 of Clause Nine), a tripartite referral to INE does not make sense. In order to minimize the risk, it is advisable that the remittance to INE comes from only one of the entities.

34. As mentioned above, the protocol specifically identifies those responsible for processing the ISS, I.P and SCML and the Processor II, I.P.

35. In Clause Ten it is stated that LNEC, FNERDM, REDE DLBC and EAPN Portugal consider themselves "responsible for accessing the anonymized information of the AidHound Platform, through the profile "statistical analysis" designed for the purpose, which will allow carrying out the evaluation of the entire process, within the scope of the activities defined in the National Strategy, specifically in the intervention axis "E1.0E2 - Ensuring the monitoring of the phenomenon" (No. 1) and which are considered "responsible for the processing of personal data only and to the extent that their responsibilities presuppose the

processing of such data" (paragraph 2).

36. They are also individually responsible for ensuring the integrity and confidentiality of all personal data that they access and that are collected, in the course of their duties within the scope of the Homeless Planning and Intervention Centers (NPISA), as provided for in the Protocol of constitution of NPISA and in accordance with the Draft contained in Annex III.

37. Now, it is the Protocol itself that provides, in paragraph 1 of that Clause, that the information that these entities access is anonymised. Now, unlike pseudonymized data, anonymized data, by their nature, do not allow the direct or indirect identification of people, so they are not personal data.

38. This inconsistency is emphasized by the text designated AIPD that accompanied the request, in which, without exceptions, all parties to the protocol are referred to as recipients of all data, according to the access profiles, referring there to Clause Nine of the Protocol. Now, taking into account that the grantors LNEC, FNERDM, REDE DLBC Lisbon and EAPN Portugal must access data

Av.D. Charles 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geraf@cnpd.pt

www.cnpd.pt

anonymized, it is not understood how these entities can have access to certain data, for example name, contacts and identification numbers.

39. In response to the request for clarification made by the CNPD, it is said that those entities “are considered responsible for accessing the anonymized information of the AidHound Platform, through the "statistical analysis" profile designed for the purpose, which will allow the evaluation of the entire process, within the scope of the activities defined in the National Strategy, specifically in the intervention axis "E1.0E2 - Ensuring the monitoring of the phenomenon", which is not enlightening. Thus, a clarification of the text of the protocol is suggested, avoiding confusion with the terminology adopted by the RGPD.

40. It is established that LNEC, FNERDM, REDE DLBC and EAPN Portugal only access anonymized data, but nothing is said about the method of anonymization, which undermines the possibility of assessing its effectiveness.

V. Fundamentals of lawfulness

41. Under the terms of Clause Four, the processing of personal data has, as a legal basis, "the free, specific, informed and unequivocal consent of the respective holder or his legal representative" [...] in accordance with the provisions of paragraph a) of paragraph 1 of Article 6, Article 7 and Article 14 of the General Data Protection Regulation". Since some of the data being processed are health data, the consent that must be given, in this regard, must also be collected in accordance with Article 9(2) of the RGPD, which is the legal basis for the processing of special categories of data, which expressly include data relating to health (Article 9(1)). Therefore, it is recommended that article 9(2)(a) of the RGPD be added to the clause.

42. On the other hand, since the Protocol states that the data will be collected directly, the regime provided for in article 13 of the RGPD must also be taken into account.

43. Consent is collected through a document called the Declaration of Informed Consent, the draft of which constitutes Annex I to the Protocol.

44. However, it is in this document that that information must be provided, which does not happen. Thus, the text contained in that document must be amended, in order to guarantee holders the right to information from holders, pursuant to articles 13 and 14 of the RGPD.

45. Also, when that text refers to the consent of the declarant for the processing of data relating to his household, it is presumed that non-individualized information of the members of the household is at stake, under penalty of such consent being legally irrelevant for not being given by the respective

holder of personal data. This is because consent is always a personal act that focuses on one's own data, and one cannot consent to the processing of third party data except in cases where there is representation, as in the case of an adult subject to the monitoring regime (and to the strict extent of what was decreed by the judicial sentence), or in the case of minors.

46. In other words, if the household data referred to in the informed consent statement is limited to that specifically set out in

Annex II of the Protocol under the designation of "household data", such information does not have to be highlighted in the statement of consent, recommending, even to simplify the text of the declaration, the elimination of the reference to "personal data of my household".

47. The mistake in writing should also be corrected by replacing the expression "by authorized means or not" with the expression "by automated means or not, although, at present, this distinction is irrelevant.

SAW. Persons responsible for data processing

48. ISS, IP are indicated as responsible for the processing of personal data. and SCML and, as a subcontractor, the II.IP. (Clause Seven), and the respective responsibilities in this scope are specified (Clause Eight).

49. Here, we invoke what has already been mentioned above, in points 37 to 39, regarding the incorrect classification of other entities as data controllers.

VII. Scratchs

50. The AidHound system uses dedicated servers in a data center in France and, to store files that are in file fields, when used in forms or profile areas, the Amazon S3 service, using EU (Paris) eu-west-3 as region.

51. Because Amazon is headquartered in the United States of America (USA), it is subject to compliance with the laws of that country.

52. It should be noted that, in compliance with the transfer regime set out in chapter V of the RGPD, taking into account the decision of the Court of Justice of the European Union Schrems II and the recommendations of the European Committee for Data Protection of November 2020, controllers must, in their risk assessments or, where mandatory, in their DPIAs carried out under article 35 of the RGPD, assess whether, in concrete terms, the proposed data processing operation jeopardizes the protection of data data; It is,

Av.D. Charles 1,134,1st

1200-651 Lisbon

T (+351) 213 928400

F (+351) 213 976 832

geral@cnpci.pt

www.cnpd.pt

if applicable, adopt the additional measures, of a technical and/or organizational nature, necessary to guarantee the adequate protection required by Union law.

53. The analysis document to the AIPD states that there is no transfer of data outside the European Union. The same is stated in the supplementary information. In this, it is added that Amazon is contractually obligated to respect the RGPD and that "AidHound stores the files in encrypted buckets and they are only decipherable by AidHound itself. Therefore, even if some data were transferred outside the EU, which does not happen, it would be encrypted".

54. The fact that the files stored on Amazon services are encrypted minimizes the risk associated with the use of this type of service. However, and because it is a company based in the USA, it is necessary that those responsible evaluate and consider this issue and adopt the necessary measures to guarantee protection. Thus, the CNPD draws the attention of those responsible to the fact that there are data transfers outside the European Union, contrary to what is indicated in the AIPD item "Transfers: fulfillment of obligations arising from the transfer of data outside the European Union", recommending reconsidering the conditions under which such transfers take place.

55. In Annex III to AIPD Opinion No. 01/2021 of the General Secretariat of the Ministry of Labor, Solidarity and Social Security, of April 26, 2021, the possibility is suggested that, in the future, "an APIREST will be implemented that will allow access data in AidHound by other systems of the organizations", whose requirements and "way of guaranteeing the protection of the data that will be transmitted by the same" are still being defined. Since this is a relevant change to the treatment in question, a change in the protocol and, consequently, a new consultation with the CNPD may be justified.

VIII. Data retention periods

56. It is foreseen, in the Sixth Clause of the Collaboration Protocol, that the personal data stored in the AidHound Platform information system will be kept until the extinction of ENIPSSA, "without prejudice to the provisions of Ordinance No. 182/2020, of 4 August".

57. The same rule is laid down for the retention of deadlines by the NPSIA (paragraph 2 of Clause Four). However, this obligation would be better integrated into the Partnership Protocol to be signed between the entities that will constitute each of the NPSIA; since, as these entities are not part of the Collaboration Protocol, they will not be bound by this last instrument.

58. The AIPD document, in section 2.2.1.3, mentions several deadlines, proposing a periodic review clause for the elimination of data in use relating to holders who are no longer being monitored. This one

document also proposes that the data on file be kept for a period of 10 years, basing the period on Ordinance No. 182/2020 of August 4, in which it was not possible to find reference to this duration.

59. At the request of the CNPD, the MTSSS further clarified that, although the period for the retention of data relating to homeless people is not specifically regulated in that Ordinance, the period specified therein for the information should apply relating to situations of social vulnerability (Code 650.20) of the annex to the Ordinance, that is, 10 years.

IX. Data Protection Officer

60. From the attached documentation, it is highlighted that the Impact Assessment was carried out by the "Data Protection Officer of the General Secretariat of the Ministry of Labor, Solidarity and Social Security", based on the lack of EPD by ENIPSSA. However, paragraph 2 of Clause Fourteen of the Protocol provides that the NPISAs designate an Interlocutor for data protection matters, who must collaborate with "the Data Protection Officer" in the matters indicated therein. On the other hand, in the Declaration of Consent the email address of the Social Security EPD is indicated. Therefore, it will also be necessary to clarify in the Protocol whether the EPD is, in fact, that of the MTSSS.

X. Rights of data subjects

61. The rights of data subjects are provided for in paragraph 3 of Clause Four of the Collaboration Protocol, which explains the rights to "know, correct and, except when their conservation is required by requirements of national/European legislation, delete the data relating to you, in this treatment, as well as revoke consent".

62. With regard to the mode of exercise of rights by the holders, there is a lack of conformity between the texts of the Declaration of Informed Consent and the clauses of the Protocol. In fact, although the Protocol provides that holders can exercise their rights with the ISS, IP. via email or via a form available on the internet (n.º 1 of Clause Fourteen), this does not occur with the Declaration of Informed Consent, which only indicates one of these means (sending the application via email).

63. Now, since it is through the information contained in the document in which he gives informed consent that the data subject is aware of his rights and how to exercise them, the information made available there should be complemented, adding the means of exercise of missing rights, a copy of this signed document being provided, in accordance with paragraph 2 of article 12 and recital 39 of the RGPD.

Av. D. Carlos 1,134,10

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

64. For the purposes of guaranteeing the exercise of rights by its holders, each NPISA indicates its "Designated Interlocutor for data protection matters, who [must] collaborate, without undue delay, with the Data Protection Officer" to, among other functions, provide “response to the exercise of rights, handling incidents of violation or requests for clarification, in its area of competence” (No. 2 of Clause Fourteen). The additional information that requests from the data subject of an informative nature will be answered by the ENIPSSA Manager, with knowledge of the EPD and that the fulfillment of any of the other rights will be managed directly by the ISS EPD with knowledge of the ENIPSSA Manager, does not allow understand which flow to use when exercising rights by holders, which should be established in advance.

65. Although the Fourth Clause of the Protocol regulates the consent and the rights of the holders, also in this aspect there is a non-compliance with the rights provided for in the Declaration of Informed Consent. In fact, the Protocol provides that the data subject may at any time, [..] and except when its conservation is required by requirements of national/European legislation, delete the data concerning him/her, in this treatment", the which complies with the regime provided for in the RGPD. However, in the information provided to data subjects for the purpose of providing consent - and which, therefore, supports their decision to consent or not to consent to the processing of their data -, it is stated , without any condition, your right to "[s]ask the person responsible for the processing of my personal data [...] the respective erasure".

66. Although it is understood that the language to be used with the data subjects must be simple, it is also true that the information to be transmitted must be true and complete, in order to allow the data subject to form his will. Now, when it is communicated to the data subject that he has the right to request the DPO to erase his data, such a formulation is likely to, with a very high probability, mislead the subject and make him believe that this request will result in the effective erasure, which will not necessarily occur, so clarification of the rights of the holders in the document relating to the provision of consent must be carried out.

67. It is also suggested to standardize the terminology3 of these documents and adapt them to the GDPR terminology for greater clarity.

3 For example, the Declaration of Consent refers to the right to "rectify data" and to "access and consult" your data, while the Protocol provides for the right to "correct" and the right to "know", respectively .

u—

, NPn

National Data Protection Commission

XI. Duty of confidentiality regarding personal data

68. In the Eleventh Clause of the Protocol it is foreseen that professionals, when granting access to the platform, are bound by a commitment of confidentiality, the draft of which constitutes annex IV of the Protocol.

69. Under the terms of the aforementioned document, professionals who have access to information considered confidential, either through access to the AidHound platform or by any other means, as long as it is in the exercise of their functions, undertake to keep confidential information confidential.

70. There is defined what should be understood by "Confidential Information", which includes personal data. Furthermore, the same document establishes that confidential information is not considered, among others, "[the] information that is admitted, by express and written authorization, to be disclosed to third parties". However, it is presumed that this authorization corresponds to the consent of the data subject. Therefore, it must be borne in mind that the consent of the holder may be limited to transmission to certain third parties, but not others, so that, in that case, the information will continue to be

confidential in this part.

71. On the other hand, there is an obligation to "keep the access codes to the computer system (username and respective password) assigned to me secret". It is possible that this is an imperfect wording, however, attention is drawn to the fact that the password cannot be "assigned", but must be defined by the system user, in order to guarantee security and personal access .

72. Furthermore, those responsible are obliged to "[communicate to the entities responsible for the platform any leak of information or incident of breach of personal data within a maximum period of 72 (seventy-two) hours from the respective knowledge". Perhaps it was intended to set a period identical to that provided for in paragraph 1 of article 33 of the RGPD for the controller to notify the National Authority, which is to say the CNPD, of any violation of personal data, but this period violates Article 33(2) GDPR, where the processor is required to notify the controller without undue delay. It is therefore recommended to correct the period indicated in Annex IV of the Protocol

73. Also in relation to the parties, the duty of confidentiality is regulated on all information that they have knowledge under the Protocol, or in relation to it (No. 1 of Clause Fifteen), establishing that such regime remains after the termination of the Protocol (paragraph 4).

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

/

XII. Conclusion

74. On the grounds set out above, the CNPD understands that the processing of personal data subject to the protocol is legitimate, the necessary data being processed and not excessive in relation to the intended purposes, however, the following

should be taken into account aspects.

i. With regard to the Protocol, it recommends:

The. The prediction that access to the system will be carried out through a dedicated line, or VPN, in order to mitigate the risks for data subjects;

B. The inclusion, in the list of Clause Twelve, of the need to keep the systems that access the platform up to date and the existence of a separate basis for pseudonymized, anonymized and identified data;

w. Consecration that the remittance of data to INE is carried out from only one of the entities, as opposed to the planned tripartite remittance, in order to minimize the risks, taking into account that it is a single system to which the administrator profile has to full access;

d. The concrete identification of the data that are accessed by each entity, indicating which ones are blank, pseudonymized and anonymized;

It is. Change in the wording of Clause Ten, insofar as it refers to responsibilities for the processing of data of the entities registered therein, when it is stated that they only access anonymized data;

f. It is also suggested to change the wording of paragraph 1 of Clause Five of the Partnership Protocol, in the part relating to normative instruments related to data protection, as it seems to assimilate Law no. 58/2019, of 8 August and the General Data Protection Regulation, suggesting that, as an alternative to the current wording, it appears in the foreseen terms, namely, the General Data Protection Regulation (RGPDj and Law n.0 58/2019, of 8 August.

ii. With regard to technical documentation:

The. Documentation of system characteristics and information on logging;

B. Review of the nomenclature used in various places in the documentation, adapting it to the GDPR nomenclature;

0

and ®

w. Indication of the specific security measures that guarantee effective data protection, taking into account that the AidHound system uses the Amazon service, as explained in point

d. Provision of the obligation to adopt mechanisms to test and evaluate the effectiveness of technical and organizational measures, in order to guarantee effective treatment safety;

It is. The prediction of access to anonymized data must be accompanied by the specification of guarantees regarding the form of research by entities legitimized for the purpose, so as not to allow free searches that lead to the identification of data subjects.

f. Forecast of user and password management rules or reference to an autonomous document that contains them.

iii. As for the Declaration of Consent model, the CNPD considers that:

The. Through this document, the information provided for in articles 13 and 14 of the RGPD must be transmitted to the holder;

B. Due to the personal nature of consent, the text of the Declaration of Consent model should be amended, eliminating the reference to the authorization of the processing of personal data of your household;

w. Also in this document, the mistake in writing should be rectified, replacing the expression "by authorized means or not", by the expression "by automated means or not", although, at present, this distinction is unnecessary;

d. The information made available should be complemented with regard to the means through which rights can be exercised, adding the possibility of exercising them through a form available on the internet, as provided for in the Protocol;

It is. It is recommended that the terminology adopted in the document be revised, adapting it to that of the RGPD and that the rights be clearly transmitted to the holders, so that they are aware of them, namely, reviewing the formulation of the right to erasure of data , as explained above.

Approved at the meeting of January 10, 2023

56;

Filipa Calvao (President)

Av.D. Charles 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt