

PRE/2021/4

CNPD

National Data Protection Commission

OPINION/2021/137

## I. Order

1. The Directorate-General for Education (DGE) submitted two documents to the National Data Protection Commission (CNPD) for an opinion: the Privacy Statement for the Collection of Personal Data relating to the FITescola® Program and the protocol to be signed between that institution and the Faculdade de Motricidade Flumana of the University of Lisbon (FMH), hereinafter referred to as Protocol 2021, which establishes the objectives to be pursued and the obligations of each of the parties in the pursuit of the commitments assumed under the protocol signed in 2018 between these and other entities within the scope of the development and application of said Program.

2. The CNPD issues an opinion within the scope of its attributions and powers, as the national authority for controlling the processing of personal data, in accordance with the provisions of subparagraph I) of paragraph 1 of article 57 and paragraph 2 of article 36 of Regulation (EU) 2016/679, of the European Parliament and of the Council, of 27 April 2016 (General Data Protection Regulation, RGPD), in conjunction with the provisions of article 3 and paragraph 2 of article 4 and subparagraph b) of paragraph 1 of article 6, all of Law no. internal legal system, of the RGPD - LERGD).

3. The request was also accompanied by a copy of the Protocol signed in 2018 (hereinafter referred to as the 2018 Protocol), between the parties and other entities.

## II. Analysis

### i. Treatment purposes

4. Under the terms of recital II of the 2021 Protocol, the FITescola® Program's mission is to «contribute to the improvement of the processes of development and assessment of physical fitness and counseling of students, physical and sports activity and sedentary behavior, from pre-school education up to secondary education', objectives that are set out in more detail in clause 1.a of the Protocol of

5. The FITescola® program is based on an «information management platform, which can be used intuitively and interactively

by teachers, students and guardians, and allows for greater efficiency in the management, organization and dissemination of information by the Directorate-General for Education».

2018

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

PRE/2021/4

1v.

r

Through the protocol to be signed between the DGE and the FMH, submitted for consideration by the CNPD, the parties establish the objectives to be pursued and their obligations in pursuing the purposes of development, optimization, evolution, updating and technological deepening of the FITescola® program and its respective platform and aim, as their main objective, to establish the bases that allow the development of the Platform, through the optimization of its current functionalities and the creation of new functionalities, including the creation of mobile applications for use by teachers, students and guardians. The Privacy Statement presented already confirms the creation of this application, which is called appFITescola®, of optional use, through which it aims to facilitate the collection and consultation of the results obtained by the students, during the performance of the various tests.

6. In order to achieve the objectives set out in the 2018 Protocol, the FITescola® Program promotes the application of tests to assess physical fitness and identify students with high potential for sports performance (recital III of the 2021 Protocol) and involves the development and use of an information management platform to be used by teachers, students and families, which will allow «the processing, analysis of data [...] and its crossing with information available from the education system, reported by schools to the Directorate-General for Statistics of Education and Science' (cf. recital IV).

7. Both the Platform and the appFITescola® are available to Physical Education teachers of all study cycles. Although it is

mentioned in that recital that the platform allows interaction with students and guardians, nothing is said about how this interaction will take place.

8. The purpose of the data processing to be carried out by the DGE through the Platform and appFITescola® (see page 3) is identified in the Declaration as «facilitating the application of essential learning and the curriculum of the Physical Education discipline, namely in the areas of physical activity, physical fitness and sedentary behavior, aerobic fitness, body composition, neuromuscular fitness; improvement of the processes of development and assessment of fitness and physical activity; consolidate the current vision of the national situation; cross-referencing data with information available in the educational system, in order to contribute to the improvement of educational policies and the national sports system.

9. The purpose of «[administering the database of the FITescola® Program platform and organization of relevant information for the purpose of evaluation/monitoring, by the DGE, aiming at the application of the previously explained legal diplomas», is also mentioned. is explained too vaguely.

10. In relation to a previous protocol signed between the DGE and FMH within the scope of this same programme, the CNPD issued Authorization No. 9342/2014.

0

PRE/2021/4 2 r

CNPD

National Data Protection Commission

11. The Privacy Statement informs that, «under the terms to be signed between DGHE and Faculdade de Motricidade Humana [...] it is allowed to make available to FMH data collected from teachers, students and guardians». However, given the purposes set out in the 2018 Protocol and those included in the Protocol that is now intended to be signed, there is no reason for the data of teachers and guardians to be transmitted to FMH.

ii. Legitimacy for data processing

12. The DGE, of the Ministry of Education, is the body of the direct administration of the State, endowed with administrative autonomy, whose mission is to «ensure the implementation of policies related to the pedagogical and didactic component of pre-school education, basic and secondary education and of extra-school education, providing technical support for its formulation and monitoring and evaluating its implementation, as well as coordinating the planning of the various tests and

exams.» (cf. no. 1 of article 2 of Decree-Law no. 14/2012, of 20 January, with the changes introduced by Decree-Law no. 266-F/2012, of 31 December) .

13. Pursuant to the provisions of subparagraphs a) and f) of number 2 of that article, in order to pursue that mission, it is incumbent upon it, namely, "[to develop the curricula and programs of the subjects, the guidelines relating to non-disciplinary areas, as well as to propose the respective revision in coherence with the objectives of the education system» and «[to promote research and technical studies, namely follow-up and evaluation studies, within the scope of curriculum development».

14. On the other hand, Article 3 of Ordinance No. 258/2012, of 28 August, which defines the core structure of that Directorate-General, gives the Directorate of Curricular Development Services (DSDC) the competence to « [d]evelop the study of curricula, programs, subject programs and guidelines relating to curricular areas and non-disciplinary curricular areas and propose the respective revision, in coherence with the objectives of the educational system»

15. Through Protocol 2021, now submitted for consideration by the CNPD, the parties express their «common will to promote the development, optimization, evolution, updating and/or deepening of the technological resources allocated to the FITescola® Program and the respective IT Platform» and establish the objectives to be pursued and the obligations of each of them for the pursuit of that FITescola® Program, in compliance with the 2018 Protocol.

16. It is, therefore, within the scope of its competences, that the DGE submits to the CNPD the Protocol 2021 and the Privacy Statement identified above.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

PRE/2021/4

2v.

r

iii. Responsible for data processing

17. The functions to be performed by each of the parties are provided for in the 2018 Protocol. Thus, the DGE is responsible for the management and coordination of the FITescola® Program and, in particular, for what matters now, it is responsible for validating the functionalities of the FITescola® Program platform, guaranteeing the maintenance of the IT platform and the development of the new functionalities that deemed relevant for optimizing the system, administering the platform database of the program in question and ensuring and managing access authorizations to information (cf. clauses three and four).

18. For its part, FMH is responsible, among others, for «designing and monitoring the integration of the computer functionalities of the FITescola® program platform» and «submitting prior validation to the DGE of all information, communications and publications that may be produced based on the data contained in the FITescola® program platform (cf. clause seven of the same protocol).

19. In order to fulfill these functions, the third clause of Protocol 2021 establishes that the DGE is also obliged to "decide on the possibility of access and use by the other Parties of data relating to teachers, students and guardians, in the scope of this Protocol' (cf. point f.).

20. The Data Collection Privacy Statement identifies DGE as the data controller (page 6).

21. Now, taking into account the provisions of the three documents mentioned above - Protocol 2018, Protocol 2021 and Data Collection Privacy Statement - the "platform that integrates the program will allow the processing, analysis of data and the production of reports [ ...] and its crossing with information available from the education system, reported by schools to the Directorate-General for Education and Science Statistics».

22. On the other hand, paragraph 2 of clause 6.a of the 2018 protocol, which constitutes a "function" of the DGEEC, "[to] store the FITescola® platform on the computer server", information that is reinforced by the Declaration of Privacy, referring that DGEEC is the «entity where the FITescola® Platform is hosted, not constituting the entity responsible for data processing» (cf. page 6) and the information contained in the Privacy Statement (cf. . page 6), that, in the execution of the subcontracting contract, Soporsoft may have to go to the DGEEC, as the entity in which the FITescola Platform is hosted. However, in this regard, there seems to be an inconsistency between the documents presented, which should be clarified, since the same Privacy Statement on page 5 states that the data

CNPD

National Data Protection Commission

personal data are «centrally archived on a DGE computer server» and, in the last line of the same page, that «personal data are stored on DGE's own servers».

23. It is also up to the DGEEC to «[ensure the design and implementation of the development of IT functionalities and procedures necessary for the articulation of the FITescola® Program platform with Escola360 and/or other IT systems that may be developed in articulation with the DGE » (cf. paragraph 3 of clause six of the 2018 Protocol).

24. The Escola 360 Program (E360) is an application for managing the school pathway accessible at <https://e360.edu.gov.pt>, through which the DGEEC «provides other bodies of the Ministry of Education with a system which aims to centrally consolidate [...] the school management processes of pre-school, primary and secondary school students" and which "allows education bodies to manage the student's life cycle, providing a complete view about their educational path, providing real-time information about students".

25. On the other hand, in order to fulfill the proposed objectives, the Program provides for cross-referencing with information available from the education system, reported by schools to the Directorate-General for Education and Science Statistics".  
personal data that will be made available to the Program.

26. In view of the foregoing, and considering that the GDPR defines the data controller as "the natural or legal person, public authority, agency or other body that, individually or jointly with others, determines the purposes and means of data processing personal data», there is no doubt that DGEEC is also responsible for data processing, in the reuse of personal data within the scope of its specific competences, assuming the quality of subcontractor in the scope of data processing for which DGE is responsible .

27. Therefore, it is understood that the DGEEC should also be part of this protocol.

iv. Data subjects and personal data processed

28. The data subjects are primary and secondary school students who attend compulsory education and their legal representatives, whose data are collected by the teachers who teach the curriculum of the Physical Education discipline or are responsible for School Sports (cf. Privacy, page 5).

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

PRE/2021/4

3v.

29. With regard to the identification of data with relevance in terms of data protection, the Privacy Statement alludes to the treatment authorized by the National Data Protection Commission in process No. 9342/2014 and identifies as parameters for the collection the data relating to the attributes of physical fitness and physical activity of students included in the Physical Education discipline program approved by the Ministry of Education and Science.

30. The variables considered are indicated, which are: weight, height, waist circumference, percentage of fat mass, number of shuttle runs, energy expenditure, maximum number of sit-ups, maximum number of push-ups, maximum jump height vertical, maximum distance in horizontal jump, shoulder flexibility through yes or no classification and flexibility of the lower limbs, trunk flexibility, time on plank, number of arm raises, time of performing 4x1 Om, number of lateral jumps, number of of lateral transfers, time accomplished in the 20 and 40 m and test of alternate launching to the wall (repetitions).

31. These parameters are applied to students throughout the school year, in accordance with the Essential Learning and National Physical Education Programmes.

32. From the foregoing, it follows that anthropometric data are at stake which, together with other data -namely those from the Escola360 Program or others, as provided for in the protocol - allow the deduction of risks to health or the existence of pathologies, diseases or morbidities. They can also allow inferring lifestyles, namely related to eating habits or sedentary lifestyle. In this sense, they can be considered to be included in the special categories of data, subject to the special regime of article 9.

v. Legal basis

33. The Privacy Statement explains that the processing of data is legitimized “under the General Data Protection Regulation

(RGPD), article 5 (Principles regarding the processing of personal data), paragraphs 1, subparagraphs a) to f) and 2, article 6 (in the context of the processing of data carried out by public entities in the pursuit of their tasks by electronic means) and article 9 (processing of special categories of data').

34. Now, with regard to the applicability of Article 5, it is observed that this statement, being conclusive, proves to be insufficient, since the mere reference to the rule is not enough, but it must be demonstrated to what extent the principles enshrined therein are respected. That is, among others, it will be necessary to demonstrate that,

0

PRE/2021/4 4

r

CNPD

National Data Protection Commission

in the specific case, it is a question of a lawful, loyal, transparent, adequate, relevant and not excessive treatment and that the data are treated in a safe way. Furthermore, the controller must be able to prove compliance with the provisions of the aforementioned article, which will be analysed.

35. As regards the legality ground, it is necessary to analyze the relevance of the rules invoked.

36. Previously, however, it is reiterated that, just as the CNPD had the opportunity to comment on cases previously submitted to it for consideration by the DGE, the legal basis for this treatment can never be that provided for in subparagraph f) of Article 6(1), as this provision, in the second subparagraph, excludes its applicability to data processing carried out by public entities.

37. On the other hand, as recognized by the DGE, the information collected is likely to reveal aspects of students' lives that are subsumed under the category of specially protected data under Article 9(1) of the GDPR, as is the case with data relating to health consistent with situations of functional limitations in the case of School Sports, or gender, so the basis of legality will have to be found in the list of paragraph 2 of article 9 and not in article 6.

38. First of all, with regard to consent, in addition to the previous generic reference, it is also added in that Declaration that "the basis of legitimacy is consent, with the holders being minors, taking into account the legal provisions and determination of authorization No. 9342/2014 , of the CNPD, this will be with the legal authorities, taking into account the best interests of the child, with the minors themselves being heard and giving their assent, taking into account their age and maturity" (cf. page 4).



39. As for consent, there seem to be two situations to consider: on the one hand, the data collected specifically within the scope of the FITescola® Program and, on the other hand, the data with which they will be crossed, namely those contained in Escola 360 or, eventually, of the School Sports Programme, with the CNPD having previously commented on the latter.

40. Thus, assuming the optional nature of the students' participation in the FITescola® Program, that is, in the event that there is a possibility that parents do not allow their children to be submitted to this program, there will be room for the consent of the holders or their representatives. In this case, it will be necessary to clarify how to provide that consent, as well as the content of the information that must be provided, how the DGE can prove that it has been obtained and its content and how the data subjects or their representatives can withdraw this consent.

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

PRE/2021/4

4v.

41. Thus, the fact that the Privacy Statement states that "the fundamental basis of lawfulness [is] the fulfillment of its attributions and competences" is not relevant here, and the informed consent of the students' representatives must be provided, after hearing that they are these, according to their age and maturity, as explained by the CNPD in the aforementioned authorization. Only then would it not be so if it were a legal obligation.

42. With regard to a possible crossing of data collected for the purposes of the FITescola® Program and data collected within the scope of School Sports, it is recalled that, according to the information made available on the School Sports platform<sup>1</sup>, the student's guardian who wish to participate in the activities of the School Sports Program must sign a "Declaration of prior consent of the holder of personal data", made available by the Directorate-General for School Establishments (DGEstE). Apparently, this consent would be given at the time of enrollment in the School Sports program. Thus, if new treatment is added through the crossing of data with the FITescola Program, consent will have to be obtained, now for this new purpose.

43. With regard to the availability of data by the DGE to FHM, the Privacy Statement (page 4) explains that it is «based on a legal, legal and contractual obligation». However, it is not clear to what extent such availability can be supported by a "legal obligation", since there seems to be no regulatory provision imposing such transfer and use of data in this context. It seems, however, that it will be based on an obligation assumed through the conclusion of the 2018 Protocol and more explicit in the 2021 Protocol.

44. Therefore, it is necessary to ensure that, before giving consent, data subjects and their representatives are clearly and completely informed about which data will be collected and transmitted, the purpose of treatment and retention period, as well as what rights they have, how they can exercise them and until what time.

45. The registration of consents and knowledge of the data processing conditions is the responsibility of the DGE.

1

[https://desportoescolar.dge.mec.pt/sites/default/files/vfinal\\_de\\_20\\_21\\_declaracao\\_de\\_consentimento\\_previo\\_do\\_titular\\_dos\\_dados\\_0.pdf](https://desportoescolar.dge.mec.pt/sites/default/files/vfinal_de_20_21_declaracao_de_consentimento_previo_do_titular_dos_dados_0.pdf)

0

PRE/2021/4 5

CNPD

National Data Protection Commission

saw. Rights of holders

46. The rights of holders are set out in the Privacy Statement, and an email address is indicated so that holders can obtain clarification on the processing of their data. It is advisable to make clear the email address so that the holders can exercise the other rights - for example, the right of rectification and elimination when the established retention period is exceeded - whether this or another means.

vii. Anonymization of personal data

47. It is said that only teachers will be able to access the nominal data and test results of the students, in order to, if necessary, contact the parents of the students and that "later" the data will be anonymized (cf. Protocol 2018, clause d) of clause twelfth).

48. It is also stated that the DGE assumes the obligation to decide on the access and use of the personal data of teachers, students and guardians by FMH, «considering anonymized processing and personal data, kept in a coded form» (cf. . Protocol

2021, clause three, item f., as well as, by way of example, pages 1,4, 6 of the Privacy Statement)

49. In this regard, one cannot fail to point out the lack of coherence and contradiction resulting from the reading of the documents sent to the CNPD, which prevents the CNPD from analyzing this relevant aspect of data processing.

50. On the one hand, because anonymization and codification are irreconcilable concepts.

51. On the other hand, because it is claimed that the data are, after all, transmitted by the DGE to the FMH in a “pseudonymised format”, a concept that is also different from anonymization (cf. Paragraphs 8 of page 5 and 3 of page 6 of Privacy Statement).

52. However, it is important to bear in mind that anonymization, by definition, presupposes the irreversibility of this process, therefore, the absolute impossibility of re-identifying the natural persons to whom the information concerns.

53. The CNPD does not know, because nothing is said in this regard, when and how this anonymization/pseudonymization will be carried out. Thus, CNPD cannot comment on the anonymization or pseudonymization process because the necessary elements for such an evaluation have not been provided. In any case, it recalls that for a real anonymization, sufficient technical measures must be adopted to guarantee the robustness of this process.

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

PRE/2021/4

5v

54. Therefore, it recommends, at least and to the strictest extent necessary to achieve the purpose of scientific research, that the pseudonymization of these data be specifically ensured, so that the provisions of paragraph 1 of article 31 of the Law No. 59/2019, of 8 August, and only with the consent of the data subjects.

viii. Subcontractors

55. Paragraph f. of the third clause of the 2018 Protocol establishes, as an obligation of the DGE in its relationship with FMH,

"to decide on the possibility of access and use by the other Parties<sup>2</sup>, of data relating to teachers, students and guardians, within the scope of this Protocol considered processing of anonymised personal data, stored in a coded form, in subcontracting, under the terms set out in article 28 of the RGPD, for preventive, corrective and evolutionary maintenance of the FITescola Platform and app». This formulation is not clear as to the entity that may subcontract for this purpose.

56. Furthermore, the reference to the subcontracting relationship under Article 28 of the GDPR is not understood if, in fact, the data are anonymised. It is therefore important to clarify whether or not there is anonymization of the personal data of the different holders before they are made known to FMH. In the event that the non-re-identifiable information is guaranteed, there is no need to talk about subcontracting. If, on the other hand, the personal data are only pseudonymised, then, because the access or communication of personal data, as well as their analysis, are personal data processing operations, it is important to regulate the relationship established between DGE and FMH. and qualify it as subcontracting if it carries out such operations on behalf of the DGE, specifying the operations to be carried out by the latter.

57. In fact, if, as stated above in the Privacy Statement, if all copyright, as well as intellectual property rights on the Platform and the FITescola brand belong exclusively to FMH, then the subcontracting relationship with this entity is much broader than clause f. of the 2018 Protocol indicates.

<sup>2</sup> It is believed that the reference to 'other parties' will constitute a mistake, since the aforementioned protocol is signed only with another entity and only before that can the DGE be bound in these terms and that the reference may intend to refer to any entities subcontractors.

0

PRE/2021/4 6

f

CNPD

National Data Protection Commission

58. Furthermore, doubts about subcontracting are intensified in two situations. On the one hand, it is stated in the Privacy Statement (see page 6), that "[e]it is contemplated in the aforementioned Collaboration Protocol on the FITescola Program signed on March 12, 2018, clause six, in the obligations of DGE , the subcontracting of an entity', which does not correspond to the text of the protocol, since clause six enshrines the obligations of the DGEEC, and not of the DGE, and in clause four, which

implements the obligations of the DGE, no obligation at that level.

59. On the other hand, that Privacy Statement refers to the subcontracting of Soporsoft by the DGE, without specifying the scope of this subcontracting.

60. Furthermore, it focuses on the subcontracting, by FMH, of Altice Labs, which will be responsible for the development of the mobile application (iOs and Android), through which teachers introduce the results of tests carried out in the classroom and who will not have access to the database. If the mobile application is made available in the context of a subcontracting relationship between FMH and Altice Labs, then it is important to specify that what is at issue here, in relation to the DGE, is subcontracting, which must be authorized by this entity as responsible for the processing of personal data.

#### ix. Treatment conditions and conservation periods

61. In the "Storage conditions and respective conservation periods", provided for in the Privacy Statement, it is stated that "the databases generated and processed by the DGE services may also be made available in a format suitable for the purposes for which is intended, protected by password, with conditioned access to the respective Director of Curriculum Development Services and the technicians indicated by him, on their service computers, also protected by password. This data is hosted on DGE's own servers».

62. However, the mechanisms for recording access to the platform for auditing and inspection purposes, which must exist, are nowhere indicated.

63. If there is, in addition to the exposition on its implementation, it is important to indicate the period of retention of access logs for audit purposes.

64. It is stated that all copyrights, as well as intellectual property rights over the Platform and the FITescola brand, belong exclusively to FMH. This entity is also responsible for optimizing and creating new features in the software.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

6v.

f

65. Finally, in the obligations of FMH it is indicated "to submit prior validation to the DGE all information, communications and publications that may be produced based on the data contained in the FITescola® Program platform". These statements indicate that FMH has full knowledge of the software, the database and that it works on the information held therein, although apparently anonymously. However, in the protocol, nothing is mentioned about how the FMH has access to this information.

66. In the risk analysis contained in the Privacy Statement document, it is stated that "with regard to processing operations, DGE will implement the necessary security measures to only allow access to workers accredited for the purpose and, in particular, the controls access to the information resources involved, as well as the registration of access to personal data». As this is a mechanism for recording access to the platform for auditing and inspection purposes, it is essential to indicate the period of retention of access records for these due audit purposes, which must be explained.

67. Also as a security measure, there will be no "backdoor" for system administration access.

68. The data collection will be done by the teachers through the Fitescola platform, with the DGE being responsible for the treatment, after which the data, already anonymized, will be sent to FMH for statistical processing. As for the terms of this shipment, it is not explained in what form it is processed. Therefore, it is completely impossible to assess from the documentation sent what the impact on data protection of this transmission will be.

69. Therefore, it is important to define whether the protocol for sending the data, and in particular, is carried out through the transfer of files or databases, manual or automatic; the username/password and/or other authorization mechanisms installed in the infrastructure of the controller and the recipient will be used; how access is managed, whether they are personal and non-transferable or institutional (eg sending by email), whether the file will have some type of cipher to guarantee the confidentiality and integrity of the data contained therein and what are the audit mechanisms for accesses to the file in your repository on the controller's side.

70. In the documentation sent by the DGE, the application for mobile devices of the FITescola platform is identified. The smartphone application provided in the order elements was downloaded in the Android version to be tested.

71. Tests were carried out on the application, during which a serious security flaw was detected in the initial version of the

application that was made available at the time of the request for an opinion by the DGE, on April 22,

0

PRE/2021/4 7

4

CNPD

National Data Protection Commission

which leads to the conclusion that on that date the application did not comply with what was stated in the "Personal Data Collection Privacy Statement", that "KeyCloak is a software that allows access management and will be prepared to perform local authentication in the existing database. All communication between the App and the server components will be done using HTTPS». However, during the tests this version stopped working and was replaced by another one, provided on April 29, which no longer had the identified vulnerability.

72. The Privacy Statement also contains the following statement, on page 3: «Both the app and the FITescola® platform use a security system with the application's own key through a SHA-1 hash algorithm, where access requires a secure authentication through SSL protocol, similar to the FITescola® website». However, the SHA-1 hash algorithm is no longer secure. Weaknesses in SHA-1 could allow an attacker to spoof content, perform phishing attacks or man-in-the-middle attacks when browsing the web. Google<sup>3</sup>, Mozilla<sup>4</sup> and Microsoft<sup>5</sup> discontinued support for this type of certificate a few years ago.

73. Temporary session cookies are used, which remain on file until the user leaves the website. The information obtained is only intended to determine the number of uses of the websites for statistical purposes through Google Analytics.

AI However, the solution cannot be based on this tool, taking into account the impossibility of guaranteeing the general requirements of Chapter V of the GDPR regarding the transfer of personal data to third countries, namely in relation to countries that do not guarantee an adequate level of protection, such as this is the case of the United States of America, given the absence of effective measures to prevent access by government entities<sup>6</sup>.

3 <https://security.googleblog.com/2015/12/an-update-on-sha-1-certificates-in.html>

4 <https://blog.mozilla.org/security/2017/02/23/the-end-of-sha-1-on-the-public-web/>

5 <https://blogs.windows.com/msedgedev/2016/n/18/countdown-to-sha-1-deprecation/>

6 In this regard, see Recommendation 1/2020 on complementary measures to transfer instruments to ensure

compliance with the EU Personal Data Protection Level and 2/2020, both from the European Data Protection Board, available at [https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement\\_pte\\_2/2020](https://edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_pte_2/2020), on the application of Article 46(2)(a) and Article 46(3)(b) of Regulation (EU) 2016/679 on transfers of personal data between authorities and public bodies established in the EEA and outside the EEA, respectively, and also the Judgment Schrems II, of the Court of Justice, accessible at <https://curia.europa.eu/iuris/document/document.isf?text=&docid=228677&paaeIndex=0&doclano=pt&mode=req&dir=&occ=first&p art=1 &cid=14967925>.

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](http://www.cnpd.pt)

PRE/2021/4

7 v.

75. After consulting the DGE website, it appears that, regarding the use of cookies, the following information is displayed:

«This website uses cookies to provide a better browsing experience and use of platform features. By continuing to browse or closing this alert, you agree to the use of cookies».

76. The CNPD draws attention to the inconsistency of this notice with the law, since, pursuant to article 5 of Law No. 41/2004, in the version updated by Law No. 46/2012, the storage of information and the possibility of accessing the stored information depends on the prior consent given by the subscriber, based on clear and complete information previously provided under the terms of the applicable legislation in terms of data protection, that is, the RGPD.

77. However, the GDPR defines consent of the data subject as "a free, specific, informed and unequivocal expression of will, by which the data subject accepts, by means of an unequivocal positive declaration, that personal data concerning him are subject to treatment".

78. Thus, the message displayed on the DGE website is not sufficient for the purpose of consent, and must be replaced by another that allows the subscriber to express, through a positive and unequivocal act, their consent or, on the contrary, their



refusal of this treatment<sup>7</sup>.

#### x. Scratches

79. The last page of the Privacy Statement is reserved for additional information from the EPD. However, that information is limited to concluding that the calculated risk is medium (risk sources: unlikely/little significant; vulnerabilities: unlikely/significant; severity: likely, significant), without identifying the risks, without any elements that support such an assessment are presented.

7 It should be noted that the same legal disagreement can be found on other sites of the Ministry of Education, e.g., on the DGEEC site. It should be noted that the solution provided on the DGEstE website only in appearance resolves this issue as it allows choosing one of two options "I accept" and "more information". Thus, if the user chooses the second option, this does not amount to a refusal. In fact, reading the information seems to allow the conclusion that cookies will always be collected even if the "accept" option is not chosen - therefore, only in appearance there will be an option - and that they should be disabled in the browser, a solution that is not compliant with the requirements of article 5 of the GDPR, since the holder may wish not to accept cookies from the DGEstE website, but accept cookies from other platforms.

0

PRE/2021/4 8 /

CNPD

National Data Protection Commission

80. As for mitigating measures, the following are indicated: encryption of data in communication and storage, measures to raise awareness in the context of data protection for workers who, by virtue of the functions they perform, may have contact with the data.

#### xi. Security measures

81. As security measures, surveillance of the DGE facilities is indicated; the elimination of personal data when they become unnecessary, it is advisable to determine the mechanisms of destruction, including identification of the persons authorized to handle such documents for this purpose; the storage of active printed data in a locked locker and in a restricted location, although nothing is said as to who has the availability of the key/s/ of these lockers; supervision of print and digital assets; Furthermore, it is said that storing the computer in a secure and locked place, which is incompatible with the fact that teachers

can access information through their computers and cell phones, through the app.

82. In addition, regular backups of information, the request for a password/login with an access password and the use of encrypted/pseudonymized data, among others, are added.

83. It is indicated that the documentation treated only by DSDC technicians - it is assumed that it is intended to refer to the treatment before anonymization, since the referred information will be transmitted to FMH, under the terms of the Protocol.

xii. shelf life

84. The data retention period - is delimited, corresponding to the end of compulsory schooling, and the backup period is not indicated. Nothing is said about the retention period of backup copies.

### III. Conclusion

85. On the grounds set out above, the CNPD takes the view that, as they stand, the documents provided by the DGE do not constitute an effective impact assessment that allows the CNPD to pronounce itself as determined by paragraph 2 of article 36 of the GDPR

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213928400

F (+351) 213 976 832

geral@cnpd.pt

www.cnpd.pt

PRE/2021/4

8v.

86. Also, due to the omissions and contradictions noted, the CNPD understands that, as it stands, the Protocol is not in a position to be signed, and the DGE must consider the above recommendations for full compliance with the legal requirements, highlighting here the following:

The. Preparation of a document providing for the consent to be given to parents and students, which must be clear and appropriate, in accordance with Articles 12 and 13, namely with regard to the data to be processed, the purpose of treatment, the retention period, the rights recognized and the exercise of the data subjects' rights, in particular access, rectification and

erasure;

B. Consideration of the need for a new consent to be provided by parents and students whenever data collected for other purposes are crossed for the purposes of pursuing the purposes of this protocol:

ç. Documentation of the provision of information on the processing of data, so that the DGE can prove its existence and the terms under which it was provided;

d. Carrying out an effective impact assessment on data protection, which clearly contains the elements provided for in Article 35(7) of the GDPR, and adopting measures to mitigate the risks that may be detected;

and. Setting a deadline for the conservation of access records, for audit and inspection purposes;

f. Adoption of a technical solution for anonymization that guarantees a strong level of security and description, with a greater degree of concreteness, of the procedures and conditions relating to the transmission of data to the FMH;

g. Clear definition of the terms for sending the information to FMH, in accordance with the above, in paragraph 69;

H. Integration of DGEEC, as a party, in the Collaboration Protocol to be signed between DGE and FMH;

i. Presentation of another solution for collecting consent for the use of cookies, in accordance with the attributes that the GDPR requires for consent.

Approved at the meeting of October 19, 2021

Filipa Calvão (President)