□0

2018/8359 1 f

CNPD

National Data Protection Commission

RESOLUTION/2021/1566

I. Report

1. On May 7, 2018, a participation was filed with the National Data Protection Commission (hereinafter "CNPD") against the Agency for Administrative Modernization, I.P. (hereinafter "AMA"), NIPC 508184509, headquartered at Rua de Santa Marta, 55,1150-294 Lisbon.

2. In this participation, it was reported that AMA workers, assigned to the Citizen's Space of the Loja do Cidadão de Braga, in order to assign a Digital Mobile Key (hereinafter "CMD") to citizens, in the back-office, would have to authenticate themselves, either with your Citizen Card (hereinafter "CC"), or with your own personal CMD.

3. On May 14, 2018, the Defendant - AMA - was notified to comment on the terms of participation, in order to clarify which digital certificate it makes available to its workers when they choose not to use their CC, for the purposes of authentication.

4. By letter dated 21 May 2018, the Defendant commented on the aforementioned notification.

5. Subsequently, on July 22, 2021, the CNPD issued Draft Deliberation No. 18/2021.

6. In this, it ordered AMA to provide an alternative means for authenticating its workers to comply with the requirements set out in the General Data Protection Regulation1 (hereinafter “RGPD”), and in Law No. 7/2007, of 5 of February.

7. The Defendant was notified of the content of the aforementioned Draft Deliberation and invited, wishing to, to exercise the right to a prior hearing of interested parties, within a period of 10 (ten) days (cf. articles 121 and 122 of the Code of Administrative Procedure, hereinafter "CPA").

8. The Defendant presented her answer, having alleged, in short, that:

The. Having analyzed the attributions and powers of the CNPD, it is not competent to order the AMA to issue professional certificates to its workers, so that these constitute an alternative to the use of the CC and CMD in their authentication (identification) in the electronic platforms, necessary for the exercise of its functions;

B. The use of the CC or the CMD in the electronic systems of the Public Administration stems from the law when it determines

the CC as an authentic document that contains the data of each citizen.

1 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and the free movement of such data and which repeals Directive 95/ 46/EC.

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

relevant for their identification, being obligatory for all national citizens to obtain them. These will be, from the perspective of AMA, the most appropriate means of authentication in the electronic systems of the Public Administration;

ç. The AMA already provides an alternative means of authentication to electronic authentication through the CC, this being the CMD. In turn, worker authentication via CMD is based on a double security factor and allows the numerical code generated for this purpose to be received in the worker's professional email, instead of his personal cell phone;

d. The means of authentication currently used - CC and CMD - are the most secure and adequate;

and. Public bodies are obliged to optimize and dematerialize processes within the scope of reducing paper consumption;

f. Authentication procedures would always have to use workers' personal data. In this context, AMA does not understand how issuing professional certificates to its workers would contribute to safeguarding the fundamental right to the protection of personal data. This issuance would indeed imply an additional processing of personal data and additional means, which would inevitably lead to an increase in security risk. II.

II. appreciation

9. The CNPD, as the national authority for controlling the processing of personal data, is competent, to the extent necessary, to receive reports and to investigate them [cf. article 3 of Law No. 58/2019, of August 8 (hereinafter "LERGPD"), law that implements the GDPR, cf. also, subparagraph f) of paragraph 1 of article 57 of the GDPR].

10. The CNPD is also responsible for monitoring compliance with the provisions of the RGPD and other legal provisions relating to the protection of personal data, correcting and sanctioning compliance with them (cf. paragraphs 1 and 2 of article 58 of the RGPD and Article 6(1)(b) of the LERGPD).

11. In view of the answer presented by the Defendant, it is necessary to assess the arguments in fact and in law presented therein.

So:

i. On the competence of the CNPD as a national supervisory authority

12. The Defendant alleges that, having analyzed the attributions and powers of the CNPD, it is not competent to order the AMA to issue professional certificates to its workers, which constitute

an alternative to using the CC or CMD when authenticating on electronic platforms of the Public Administration, necessary for the exercise of its functions.

13. Such an understanding is not accepted.

Let's see:

14. The CNPD has powers of investigation, correction, consultation and authorization in relation to the processing of personal data (cf. paragraphs 1, 2 and 3 of article 58 of the RGPD and paragraph b) of n. 6 (1) and (2) of the LERGPD).

15. Within its powers of correction, the CNPD has the option of "ordering the controller or processor to take measures to ensure that the processing operations comply with the provisions of this regulation and, if necessary, in a and within a specified period" (cf. point d) of paragraph 2 of article 58 of the GDPR).

16. It may also impose on the controller a temporary or permanent limitation or prohibition on the processing of personal data (cf. Article 58(2)(f) of the GDPR).

17. Since the use of CC or CMD for certification with professional attributes implies the processing of personal data of the respective holders, the CNPD is competent to exercise all the powers indicated above.

18. In the present case, the CNPD came to exercise a power of correction, ordering the controller - in this case, AMA - to make available to its workers an alternative means of authentication in the exercise of their functions, which meets the requirements of the RGPD, when the same is necessary for the exercise of the functions by them.

19. It should be noted that public entities, such as the Defendant, are no exception, being subject to the CNPD's powers of correction, as provided for in the RGPD and the LERGPD (see paragraph 3 of article 44). of the LERGPD).

20. Thus, the Defendant's argument regarding the CNPD's incompetence cannot prevail. It is clear that the latter can exercise its corrective powers to order the controller to adopt measures so that the processing operations it carries out comply with the GDPR.

ii. On the arguments of the suitability of the means of authentication used and the availability of an alternative means of authentication

21. The Defendant claims that the use of the CC or CMD to authenticate workers in the electronic systems of the Public Administration, in the exercise of their functions, is the most appropriate means of authentication.

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

22. It is based on the fact that the CC represents an authentic document, and its acquisition is mandatory for all national citizens (cf. paragraph 1 of article 3 and article 2 of Law 7/2007, of 5 of February).

23. It concludes, therefore, that these are the suitable means to guarantee the authorship of the acts carried out by workers in the Public Administration.

Let's see,

24. The CC is, in fact, an authentic document that must be obtained by nationals, whose function is to prove the identity of the

holder to third parties (cf. paragraph 1 of article 3, article 2 and n. 2 of article 6 of Law 7/2007, of 5 February).

25. The CMD consists of an "alternative and voluntary system for the authentication of citizens in the portals and websites of the Public Administration", with the management and security of the technological infrastructure that supports it being the responsibility of AMA (cf. article 1 and n. 8 of article 2 of Law No. 37/2014 of 26 June).

26. Assisted digital service is "the indispensable complement to the digital provision of public services" and is regulated in Decree-Law No. 74/2014, of 13 May.

27. This legal diploma establishes "digital as a rule", but provides for a system of "assistance to the citizen or economic agent in accessing and interacting with the portals and websites of the Public Administration", this assistance "provided by a worker of a partner entity duly accredited by AMA, I. P." (cf. no. 1 of article 6 of Decree-Law no. 74/2014, of 13 May).

28. Now, if, on the one hand, the employer may, at first, request the personal identification of its workers, to certify it and even to generate credentials that allow the identification of its workers accurately; on the other hand, it cannot demand that they use their personal identification document as a professional tool on a daily basis.

29. In fact, there is no provision in Decree-Law No. 74/2014, of 13 May, that establishes the obligation to use the CC or CMD for the purposes of authentication of Public Administration workers, nor that define the CC as a necessary instrument for the exercise of professional activity.

30. In fact, the wording of the law is clear when it establishes that the CC holder only uses its electronic certification features "[whenever he wants to" (cf. paragraph 5 of article 18 of Law No. 7/2007 , of 5 February).

31. However, it is possible to certify professional, business and public attributes through the CC and CMD, through the Professional Attributes Certification System ("SCAP").

32. Although this is true, it should be noted that, once again, this certification is purely optional, depending entirely on the will of the citizen in question, whether the CC is used or the CMD is used for this purpose (cf. n. 1 and 3 of Article 18-A of Law No.

7/2007, of February 5, and Article 3-A of Law No. 37/2014, of June 26, as well as paragraph 1 of article 3 of Ordinance no. 73/2018, of 12 March).

33. In the present case, authentication through the use of the worker's CC or CMD does not depend on his will, being necessary for the exercise of his functions, since there is no alternative means (as we will see) that allows the worker to be authenticated without resorting to to the data contained in your personal identification document.

34. In fact, the argument presented by AMA, according to which workers would have an alternative means, as they have the CC or CMD at their disposal for the purpose of certification with professional attributes, impedes in the circumstance that the law provides for the voluntary nature the use of both means for this purpose (cf. above, points 27, 31 and 33).

35. It is good to see that the requirement, which AMA makes to its workers to assign a CMD in the back-office, to use one of the means, alternatively, for certification with professional attributes subverts the legal norms already mentioned - maximum n 1 and 3 of Article 18-A of Law No. 7/2007, of February 5, and Article 3-A of Law No. 37/2014, of June 26 -, as it implies that they are obliged to authenticate themselves with professional attributes with their CC or CMD.

36. In fact, if the use of any of these means for this purpose (certification with professional attributes) is, under the terms of the law, voluntary, the imposition of the use of one of these means changes the voluntary nature that the law manifests and expressly establishes.

37. Now, given that the use of the CC or the digital CMD implies the processing of personal data, if the law makes the execution of the processing conditional on the expression of will of the respective data subject, then the specific conditions must be met. required by the national legal system for the expression of that will, so that the basis of lawfulness of the processing of personal data can be verified.

38. In this case, this expression of will (or consent) for the processing of personal data must meet the requirements set out in Article 4(11) of the GDPR, a provision of direct application in the national legal system. Thus, the manifestation of will has to be: free, specific, informed and unequivocal.

Av. D. Carlos 1,134,1st

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

39. However, in the specific case, the expression of will of the workers assigned to the Citizen's Space of the Loja do Cidadão de Braga regarding the use of CC or CMD for the purpose of certification with professional attributes was not demonstrated; moreover, the holdings that gave rise to this process are proof of that.

40. But, above all, the existence of conditions of freedom for the expression of that will has not been demonstrated, which depend on there being an alternative to the use of those means, because any of them supposes the voluntary and free use by the workers.

41. In fact, if an alternative to the use of those means is not guaranteed, the processing of personal data is unlawful, as shown below. And, therefore, it becomes irrelevant to assess the adequacy of the means to achieve the purpose.

iii. About the illegality of the treatment

42. Despite this being mentioned in the Draft Deliberation, the Defendant did not comment on the legal basis it uses to process its employees' personal data when they have to authenticate through CC or CMD.

43. However, for the purposes of this Resolution, the issue is of significant importance and cannot be overlooked.

So:

44. As mentioned above, the use of CC or CMD by AMA workers constitutes a personal data processing operation, with the Defendant being responsible for the treatment (cf. paragraphs 2 and 7 of article 4. ° GDPR).

45. This is because, as is evident, the Defendant provides the means and defines the purpose of these processing operations, by imposing them on her workers.

46. However, for a data processing operation to appear lawful, it must be legitimized on a lawful basis, as set out in Article 6 of the GDPR.

47. Since the Defendant has not indicated the legal basis that legitimizes this processing of personal data, it is relevant to carry out a brief analysis of the possibilities, in order to determine whether the treatment in question is based on a valid legal basis.

48. A careful reading of article 6 of the RGPD allows us to easily conclude that there is no legal rule that imposes, or makes it possible, that the employer requires its workers to use their CC or CMD as

0

2018/8359 4

CNPD

National Data Protection Commission

working instruments (cf. Law No. 7/2007, of February 5, Decree-Law No. 74/2014, Law No. 37/2014 of June 26).

49. Thus, it is not possible to frame the processing of personal data in the need to comply with a legal obligation under the terms of Article 6(1)(c) of the GDPR.

50. Nor is it clear how it could be claimed that the use of the CC or the CMD is necessary for the satisfaction of a public interest [cf. Article 6(1)(e) of the GDPR], nor could the pursuit of the public interest prevail, without further ado, over the fundamental rights to the protection of personal data and privacy (cf. Articles 266). , 35 and no. 1 of article 26, all of the Constitution of the Portuguese Republic), since the processing of personal data in question - authentication through CC or CMD in the exercise of certain professional functions, by workers - still that is done by the data subjects, does not cease to represent a risk to their rights, freedoms and guarantees.

51. The legal basis that could be more plausible to justify, in this particular, the processing of personal data would be the legitimate interest of the controller [cf. Article 6(1)(f) of the GDPR], It turns out that the GDPR itself rules out this possibility, by expressly dictating that the legitimate interest "does not apply to the processing of data carried out by public authorities in the carrying out their tasks electronically" (cf. second subparagraph of Article 6(1) of the GDPR).

52. Obtaining the worker's consent would constitute the ultimate alternative to substantiate the lawfulness of data processing. But, as explained above, consent, in order to be valid, depends on the fulfillment of very demanding requirements, which aim to guide the rights, freedoms and guarantees of the holders of personal data [cf. Article 6(1)(a) of the GDPR],

53. Thus, consent, to be valid, must result from a manifestation of free will (cf. Recital 32 of the GDPR).

54. However, as has already been analyzed, in the present case, there is no possibility of consent resulting from any manifestation of free will, since workers are conditioned by the need, in order to perform their professional functions, to use the CC or CMD.

55. In fact, consent, in the context of legal and labor relations, is hardly an adequate legal basis, due to the contractual position of imbalance in which the worker finds himself vis-à-vis the employer (cf. Recital 43 of the GDPR).

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

56. Faced with this imbalance, it is not possible to defend the existence of free consent, as the worker will always be conditioned by the employment relationship, bearing in mind that, as a rule, the worker's subsistence depends on the income obtained from his work.

57. Which would depend on there being an alternative means that would allow a free choice of the worker.

58. It follows, therefore, that the processing of personal data at issue here lacks a valid basis of lawfulness.

59. Therefore, it must be concluded that the processing of personal data is unlawful.

iv. On the argument that the CNPD deliberation project implies the use of bureaucratic and less secure means

60. Regarding the Defendant's argument, which argues that public bodies are obliged to optimize and dematerialize processes in the context of reducing paper consumption, it should be noted here that the CNPD did not suggest a bureaucratic alternative, which excludes digital media and technological.

61. The requirement of an alternative means of authentication through CC or CMD does not imply materialization, on paper, with multiple alternatives available to the Defendant, which are innovative, which do not imply the mandatory use of the workers' personal means of authentication.

62. The Defendant claims that the use of electronic services requires secure authentication mechanisms, which securely certify the identity of users.

63. Considers, in this context, that the CC or the CMD are the most secure mechanisms for authentication, as they are used

on public electronic sites with the highest adherence, as well as on the sites of various private entities.

64. It also claims that, if authentication through CC or CMD were not used, the worker would authenticate himself in the system using a username and password, which by nature are transferable data that do not guarantee the necessary levels of security.

65. It also argues that the CMD "(...) is based on a double safety factor:

a) First, a unique personal code (from 4 to 6 digits) and non-transferable, chosen by the user and known only to him;

b) Secondly, a randomly generated numerical code, which the user receives on their mobile phone, or selected email address, and which is used only once to complete the authentication and/or signature, with only 5 minutes long".

66. The Defendant also considers that it would not be satisfactory, in terms of information security, for a worker to be able to access the back-office, necessary to assign a CMD, through a less secure authentication mechanism than the one that will assign .

67. Finally, it argues that it does not understand how issuing professional certificates to its workers would contribute to safeguarding the fundamental right to the protection of personal data, as this would imply additional processing of personal data and additional means, which would translate into a inevitable increase in security risk.

68. These arguments cannot be upheld.

Let's see:

69. It is true that information security is an extremely important factor in the context of the processing of personal data.

70. Moreover, the data must be "processed in a way that guarantees its security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage, adopting appropriate technical or organizational measures" [cf. principle of integrity and confidentiality, provided for in Article 5(1)(f) of the GDPR],

71. It is precisely for this reason that the RGPD establishes obligations, in the sphere of the controller, which aim to guarantee the security of the treatment.

72. The controller must apply technical and organizational measures, as well as policies, adequate to ensure compliance with the GDPR and to safeguard the rights, freedoms and guarantees of the holders of personal data (cf. Article 24(1) of the GDPR).

73. The measures adopted must take into account several factors and, imperatively, guarantee a level of security appropriate to the risk of the data processing in question (cf. Article 32(1) of the GDPR).

74. It is important to bear in mind that these measures cannot be implemented in a generic way, and must take into account the processing of data in question and the relationship between the controller, the data subject and the purpose of the treatment.

75. For these reasons, the GDPR also stipulates that these measures must be applied both when defining the means of processing and at the time of processing itself (cf. Article 25(1) of the GDPR).

76. This is because data protection must exist by design and by default.

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

77. "From conception" or "by design" means that all data processing must be thought out, and designed, with the objective of safeguarding the rights, freedoms and guarantees of its holders. In other words, the protection of personal data must be guaranteed, even before the treatment itself, when planning it.

78. "By default" or "by default", in turn, means that the controller must implement measures that guarantee only the processing of personal data "(...) that are necessary for each specific purpose of the treatment. ", privileging the defense of the interests, freedoms and guarantees of the holder of the personal data, in relation to the interests of the controller (cf. paragraph 2 of

article 25 of the RGPD).

79. There is no denying that secure authentication is a crucial factor in information security. However, the Defendant's arguments cannot be granted.

80. First of all, there are authentication mechanisms capable of guaranteeing at least the same level of security as worker authentication using CC or CMD.

81. And that also resort to the two-factor authentication.

82. Allowing workers to authenticate their identity and perform their duties, without resorting to their own CC or CMD.

83. A practice, by the way, used in other professions, where the professional's identity is equally relevant, such as doctors, lawyers, forces of authority, military forces, among others.

84. It should be added that the fact that the authentication mechanisms used by the Defendant are widely available for use by citizens on public electronic sites with greater adherence and sites of various private entities does not allow us to deduce, without further ado, that they are the most authentication security.

III. Conclusion

85. Under Article 58(2)(d) of the GDPR and Article 6(1)(b) of the LERGPD, on the grounds set out above, due to the manifest lack of lawfulness of the processing of personal data resulting from the imposition of use of CC or CMD on the employees of the Agência para a Modernização Administrativa, I.P., for the purpose of their certification with professional attributes to assign a CMD in back-office, the CNPD orders the Agency for the Administrative Modernization, I.P., provide an alternative means for certifying workers when it is necessary for them to perform their duties, within six months.

0

CNPD

National Data Protection Commission

Approved at the meeting of December 21, 2021

Filipa Calvão (President)

Av. D. Carlos 1,134,10

1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

2018/8359 6

geral@cnpd.pt

www.cnpd.pt