CNPD

National Data Protection Commission

OPINION/2022/8G

I. Order

1. The Insurance and Pension Funds Supervisory Authority (hereinafter ASF) asked the National Data Protection Commission (CNPD) to comment on the draft protocol to be signed between the ASF and the Agency for Administrative Modernization, I.P. (hereinafter AMA), regarding the availability of data on the compulsory insurance certificate for motor vehicle liability, contained in the registration database, through the ID.GOV mobile application. (hereinafter APP).

2. The CNPD issues an opinion within the scope of its attributions, as the national authority to control the processing of personal data, conferred by subparagraph c) of paragraph 1 of article 57 and paragraph 4 of article 36 of the Regulation. (EU) 2016/679 of the Parliament and of the Council, of 27 April 2016 (General Regulation on Data Protection - RGPD), in conjunction with the provisions of article 3, paragraph 2 of article 4. ° and in paragraph a) of paragraph 1 of article 6, all of Law n.° 58/2019, of 8 August.

II. Analysis

3. The purpose of the Protocol under analysis (hereinafter “Protocol”) is to define the rules applicable to the provision of information on the compulsory motor vehicle liability insurance certificate, which is included in the registration database, through the ID mobile application. GOV., in order to make the provisions of subparagraph a) of paragraph 4 of article 85 of the Highway Code enforceable.

4. It provides that access by the respective data subject for the purpose of presenting it to third parties, with legal value equivalent to that of the original documents, under the terms of paragraphs 1 and 4 of article 4-A of Law no. 37/2014, of 26 June, ex vi article 85 of the Highway Code, approved by Decree-Law No. 114/94, of 3 May, with the changes introduced by Decree-Law No. 102 -B/2020, of December 9 (hereinafter C.E.).

5. ASF is a legal person governed by public law with an administrative nature independent from the supervision and regulation of the insurance sector and pension funds, in accordance with the terms of subparagraph g) of paragraph 8 of article 16 of the

respective Statutes approved by Decree-Law No. 1/2015, of 6 January, in its current wording (hereinafter Statutes), «/ to ensure the management of the information registration system relating to civil liability insurance for land motor vehicles and of other systems for recording information relating to other insurances that may be legally established".

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

6. It is, therefore, responsible for maintaining a register with information related to the insurance policies of land motor vehicles normally stationed in Portugal, either for the purposes of controlling the insurance obligation, or for the purposes of settling motor vehicle claims (henceforth enrollment database) - cf. Article 76(1) of Decree-Law No. 291/2007 of 21 August and Article 4(1)(a) of the Statutes),

7. The insurance certificate is one of the documents that the driver must carry when driving on public roads.

8. Let us see, then, in what terms the data protection issues that the carrying out of this treatment may raise are taken care of, the starting point for this purpose being the provisions of clause 4 of the Protocol under the heading "Data protection personal".

i. Responsibility for treatment

9. In paragraph 1 of Clause 4, AMA and ASF assume responsibility for the processing of data that the availability through the mobile application of information relating to the insurance certificate implies.

10. However, from the reading of the recitals that precede the clauses of the Protocol, and above all from the reading of the attributions and powers legally established to each of the granting entities, there is no basis for AMA to assume here the quality of responsible for the treatment of personal data covered by the Protocol, as defined in Article 4(7) of the GDPR.

11. In fact, only ASF is responsible for keeping a register with information on insurance policies for land motor vehicles (cf. Article 76(1) of Decree-Law No. 291/2007 and article 16, no. 8, point g), of Decree-Law no. 1/2015, of 6 January), record from

which the information to be made available is extracted under the terms provided for in the aforementioned article 85, No. 4, of the C.E., being certain that such operation is the exclusive responsibility of ASF.

12. In fact, it is enough to look at the attributions of AMA, to conclude that it only acts, in relation to this processing of personal data, as a subcontractor (cf, article 4, paragraph 7), of the GDPR). And its obligations, under the terms of Article 28 of the GDPR, are essentially portrayed in paragraph 2 of Clause 2.a of the Protocol.

13. The only data processing operation for which AMA is responsible - by legal determination - is the one relating to the process of authentication of citizens, but this is an operation that, although constituting a previous step in relation to the availability of the information contained in the register , is not subject to regulation

in the Protocol. 0 which is easily demonstrated when considering Clause 5.a thereof, which does not have any operative content on the processing of personal data associated with the authentication process, in addition to what results from Law No. 37/2014.

14. Thus, the duty to comply with the principles of the purpose of treatment, data minimization and data updating, as well as the obligation to ensure the security of the treatment by adopting technical and organizational measures regarding the personal data recorded in the database registration data, falls on the ASF as the entity responsible for the treatment (cf. articles 5 and 24, both of the RGPD), with the AMA having the function of acting on behalf of the ASF in the execution of the treatment in accordance with such principles and obligations.

15. Also in terms of guaranteeing the rights of data subjects, the obligations set out in paragraph 2 of Clause 4.3 fall on the ASF and not directly on the AMA.

16. In these terms, the CNPD understands that Clause 4.3 (in paragraph 1 and in paragraph 2) must be amended in order to clarify that the person responsible for processing personal data subject to regulation in the Protocol is ASF , and that AMA acts as a subcontractor.

17. And, to that extent, the obligations of AMA provided for in paragraph 2 of Clause 2.a must be assumed as obligations of the subcontractor for the purposes of Article 28(3) of the GDPR.

18. Since AMA is not responsible for the processing, and by virtue of the principle of data minimization (enshrined in Article 5(1)(c) of the GDPR), it must be made clear in the Protocol that the data exchanged between the APP and the WADA, the WADA's request to the ASF and the return path are carried out without the WADA having access to the data transmitted in these communications.

19. Finally, and bearing in mind the provision of Clause 2, no. 2, point g), of the Protocol, and on the assumption that, in the context of tests, diagnostic data and error monitoring will be collected in these new web Services to be developed, due to the need to guarantee their performance, it will always be necessary to request an additional, distinct and explicit consent for the testing period.

20. For the purposes of obtaining the consent of the data subject, ASF must bear in mind the provisions of Articles 4(11) as well as Article 7, both of the GDPR.

ii. Categories of personal data to be processed

21. Personal data will be those that are adequate and necessary to pursue the purpose of the treatment.

i

22. In this sense, it appears that Clause 4 is silent on this element of processing, although it is inferred from Clauses 1 and 2 that the personal data are those contained in the registration and concerning the elements of the insurance certificate.

23. Notwithstanding the relevance and adequacy of the personal data processed, it is still recommended to explain the personal data being processed in Clause 4, possibly by referring to Article 76(1) , of the C.E., and to the Regulatory Standard No. 11/2016-R, of October 20th.

iii. Information security

24. Bearing in mind the obligations of ASF and AMA, as controller and processor, respectively, the provisions of Article 5(1)(ej) and Article 32 must be considered in terms of processing security. .° of the RGPD, reminding the controller that under the terms of paragraph 2 of the aforementioned article 5, he is solely responsible for complying with and demonstrating that he has complied with the RGPD.

25. However, in Clause 2.a, no. 2, point d) and no. 3, point òj, it is established that the communication between AMA and ASF, for sending the data, will be via Web Services, with the provision of a VPN for this purpose.

26. Thus, in order to contemplate a system of access control, transmission and temporary and/or definitive storage of data, it is necessary to complement the obligations of implementing the system

27. It is also recommended that all communications be encrypted, using the Hl FPS protocol, using Trarsport Layer Security (TLS), in its most recent version.

28. Additionally, an authentication mechanism must be defined between the WADA system and the ASF system.

29. It is also recommended to implement a strong authentication system (preferably through certificates).

30. On the other hand, and in order to guarantee the authenticity of the information, it must be indicated which media the data is used for, whether it is digitally signed or a similar function.

31. In order to attest to the veracity of insurance certificates, it is important, in turn, that all these data can be unequivocally traced back to their origin.

32. In clause 2.a(3)(e), it is stated that the ASF must 'allow real-time access to data relating to the insurance certificate contained in the registration database'.

33. Pursuant to this requirement, it is necessary for the protocol to clarify whether data is transmitted whenever the document is invoked to be presented, or if, and when, downloaded is kept until its expiration. If this second hypothesis is confirmed, it is still necessary to define how, by whom and under what terms, the expiry of the insurance certificate is managed.

34. The protocol must also define which traceability is intended for the use of the system, as well as identify which audit

records are, with a time stamp and a pre-defined finite retention period.

35. It is also important to indicate who will have access to these audit records and what are the safeguards to ensure that they are of restricted access. An alarm should be created to identify situations of access or misuse.

36. Communication between the application available for installation on Android and iOS mobile systems must comply with communication security requirements, namely with regard to the encryption of personal data transmissions.

37. Based on the above grounds, the CNPD recommends revising Clause 4.a of the Protocol in order to clarify that the person responsible for processing personal data subject to regulation in the Protocol is the ASF, and that AMA acts as a subcontractor.

38. And, to that extent, must the obligations of AMA provided for in paragraph 2 of Clause 2.a, be assumed as

39. The CNPD also recommends that the other observations indicated above, in points 20, 23 and 25 to 35, be observed.

Lisbon, August 23, 2022

Conclusion

obligations of the subcontractor for the purposes of Article 28(3) of the GDPR.

Maria Cândida Guedes de Oliveira (Rapporteur)

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