f

National Data Protection Commission

OPINION/2023/35

I. Request

1. The Portuguese Securities Market Commission (CMVM) asked the National Data Protection Commission (CNPD) to issue an opinion on the draft Regulation aimed at regulating the CMVM's electronic one-stop shop. It also repeals CMVM Regulation No. 3/2016, on how to provide information to the CMVM by persons and entities subject to its supervision through the extranet domain.

2. An Impact Assessment on the Protection of Personal Data (AIPD) relating to the present CMVM regulation project and the CMVM Public Consultation Document No. 5/2023 has been attached.

3. 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 GDPR) , 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 of August, which implements the GDPR in the internal legal order.

II. Analysis

4. Pursuant to article 62 of the Code of Administrative Procedure, approved by Decree-Law No. 4/2015, of January 7th, last amended by Decree-Law No. 11/2023, of February 10th , and Article 357-A of the Securities Code, the CMVM intends to implement the CMVM electronic one-stop-shop (BUE), through which all interactions between the CMVM and its supervised bodies will be mandatorily processed, as well as the interaction of the CMVM with other interested parties who are interested in benefiting from access to the electronic one-stop shop, but on a voluntary basis. Interactions relating to administrative offense proceedings promoted by the CMVM, which follow their own legal regime, are excluded.

5. From the public consultation document, it appears that the BUE will have the following functionalities: a) electronic

authentication procedure; Sending information imposed by CMVM regulations by completing a questionnaire or electronic form; Delivery and deposit of documentation (eg documentation required for the activity registration dossier; documentation to be delivered by entities subject to supervision; documentation requested from supervised entities after on-site supervision); Sending and receiving communications between the CMVM and users, including making requests and other procedures via electronic form and query mechanism on the processing of requests and status of procedures; Payment of supervisory services and consideration for acts of the CMVM, including automatic receipt issuance mechanisms;

Av. D. Carlos 1,134,1° T (+351) 213 928 400 geral@cnpd.pt

1200-651 Lisboa F (+351) 213 976 832 www.cnpd.pt

Electronic notification of collection of supervisory acts, through integration with the "Electronic Notifications of the State" platform.

6. Pursuant to the preamble of the Project, the security and processing of personal data within the scope of this CMVM regulation comply with the provisions of Regulation (EU) 2016/679 of the European Parliament and of the Council, of April 27, 2016, and related national legislation.

7. The draft Regulation results in the processing of personal data of supervised persons, users, main users, third parties and third party agents, within the meaning of subparagraphs 7) to 11) of article 2. compliance with the legal regime for the protection of personal data.

8. Under the terms of the AIPD, the processing of personal data of users, main users, third parties and third party agents comprises the full name, tax identification number (NIF), email, telephone, fax. It should be noted that the NIF data is necessary for the purposes of billing for services requested by users through the BUE. Since this project only regulates the operation and access to the BUE, such data are necessary and adequate for the purpose in question, in compliance with the principle of data minimization provided for in paragraph c) of paragraph 1 of article 5 .° of the GDPR. It should be noted that the name and signature of the supervised natural person, as well as the quality/function, email address and signature of the management members of the representatives of the supervised legal persons are also subject to processing.

9. Article 5 provides that supervised persons access the BUE through its users whose appointment is requested at the time

they request the act for which they intend to be supervised. The request for nomination of supervised users is made by user through the BUE under the terms of Annexes I and II.

10. However, paragraph 2 of article 5 of the Project leaves doubts as to the meaning of the term user, since the interested party has not yet been named as such at the time of their first interaction on the platform. Therefore, it is suggested that the wording of the precept be clarified.

11.0 Article 7 of the Project regulates the accreditation process. It is suggested that in implementing the Regulation a robust authentication mechanism be adopted, based, for example, on the 2FA mechanism (double factor identification).

12. Still with regard to this article, it should be noted that paragraph 1 provides that upon receipt of the request for accreditation as a user on the BUE, the CMVM immediately sends a message to the future user with instructions to finalize the accreditation, the deadline for doing so and the consequences failure to comply with instructions in a timely manner.

13. This provision does not clarify the means by which such a message is sent, whether by email or by sms. It is recalled that an accreditation mechanism carried out strictly by one of these means is weak and does not serve as a guarantee of accuracy of data and confirmation of identity. In order to try to guarantee, at the very least, the accuracy of the data and the professional quality of the users, it is proposed that the accreditation of this type of profile include immediate notification, via email, of the data holders requesting validation of the data and further contact, via by telephone {sms) or by post, with an identity verification code to activate the user account.

14. In turn, the public consultation document sent includes, among the functionalities of the BUE, the electronic notification of collection of supervisory acts, through integration with the "Electronic Notifications of the State" platform. Now, the Public Service of Electronic Notifications (SPNE) is managed by the Agency for Administrative Modernization, I.P., (AMA, I.P.), for which reason, the CMVM and the AMA, I.P., should, by agreement, establish the respective responsibilities for compliance with the RGPD, defining the capacity in which each of these entities acts within the scope of notifications via the SPNE platform, whether as a subcontractor or co-responsible, pursuant to paragraph 1 of article 26 and paragraph 3 of article 28. ° of the GDPR.

15. In these terms, the CMVM must provide clear information to data subjects about this treatment and the extent of its responsibility for it.

16. In turn, consulting Articles 15 and 16 of the Draft Regulation shows that non-encrypted file formats are used: Text/PDF and ASCII/XML. Reading Article 14, it appears that the transfer of these files is encrypted (sFTP/FTPS), but their central repository at the CMVM and security controls are not known. The CNPD recommends that the Project include the definition of appropriate technical and organizational measures to ensure a level of security in the treatment appropriate to the risk, under the terms of article 32 of the RGPD, and in accordance with paragraph 3 of article 6. ° of the GDPR.

17. Additionally, regarding the analysis of the AIPD, it appears that mitigating the identified risk, through the recording of a log, which is the only mitigation control provided for is the electronic record {log). It is suggested that this risk mitigation control be complemented with the permissions policy, change history management and, in an extreme situation, backups in order to be able to recover improperly changed data.

18. Furthermore, the projected regime does not raise reservations from the perspective of its compliance with the legal data protection regime, except for the data conservation periods, regarding which the Project is silent. In fact, it is limited to mentioning in the preamble that they are kept in accordance with the principles of administrative interest and administrative utility, provided for in Decree-Law No. 16/93, of 23 January, that is, at least until the date on which the purpose for which it was collected expires, plus the limitation periods, namely administrative, tax or civil. Expiration of prescription periods

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

applicable or other imposed by law, personal data may also be retained for the purposes of definitive or historical archiving, under the terms of the aforementioned Decree-Law.

19. Now, as already mentioned in Opinion No. 118/2022, approved on December 21, 2022, the CNPD does not discuss the public interest of the CMVM in the preservation of personal information - an interest that the aforementioned Decree-Law

provides for -, but points out that, by transferring that legal diploma to an administrative regulation (Regulatory Decree) the setting of conservation periods (cf. no. 2 of article 15 of Decree-Law no. 16/93), it cannot fail to be required also here, in the context of the processing of personal data carried out by the CMVM, the setting of deadlines for the conservation of personal data subject to processing, depending on the need to conserve such data for the intended purposes, under the terms of paragraph e) of paragraph Article 5(1) of the GDPR. Article 6(3) of the GDPR also points in this direction.

20. Thus, the CNPD recommends specifying the retention periods for personal data, not least because, under the terms of article 13 of the RGPD, the CMVM has a duty to provide information regarding the same to data subjects (cf. paragraph a) Article 13(2) GDPR).

III. Conclusion

21. Essentially, the Draft Regulation does not raise reservations from the perspective of its compliance with the legal data protection regime, with the exception of the lack of specification of the retention periods of personal data. Thus, the CNPD recommends setting the retention periods for the personal data being processed in the Project's text (cf. above, points 19 and 20).

22. Furthermore, the CNPD also recommends clarifying paragraph 2 of article 5 of the Draft Regulation, regarding the term user given the absence of accreditation in that capacity in the first interaction on the platform (cf. above, points 9 and 10).

23. Finally, the CNPD also recommends the adoption of robust security measures in the processing of personal data, in the terms suggested above, in points 11, 13, 16 and 17, and recalls the duty that falls on the CMVM to provide clear information to data subjects on the processing of personal data carried out through the BUE and the extent of their responsibility for it (cf. above, points 14 and 15).

Approved at the meeting on April 11, 2023

Filipa Calvao (President)