_ „„ ©

National Data Protection Commission

OPINION/2023/38

/

I. Order

1. The Securities Market Commission (CMVM) requested the National Commission for Data Protection (CNPD) to issue an opinion on the draft Regulation (Project) that regulates the Legal Regime of Audit Supervision, approved by Law No. 148/2015, of September 9, and amended by Law No. 35/2018, of July 20, and Law No. 99-A/2021, of December 31, on the registration of proofreaders auditors, statutory auditors, auditors and auditing entities from Member States with the CMVM, some aspects of the exercise of the audit activity and its supervision by the CMVM, as well as the communication of information to the CMVM. This regulation also repeals CMVM Regulation No. 4/2015, of 26 January.

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's electronic one-stop-shop (BUE), through which all interactions between the CMVM and its supervisees

will be mandatorily processed. Thus, it is necessary to regulate the formats and means of compliance with the reporting duties by auditors and other related supervised bodies, so that, both on the supervisory side and on the side of the referred supervised entities, it is possible, from the date of launch of the BUE, operationalization and maintenance of the legally due reports.

5. On the other hand, with the entry into force of Law No. 99-A/2021, of December 31, which amended, among others, the Statute of the Order of Chartered Accountants ("EOROC") and of the Legal Regime for Audit Supervision ("RJSA"), it is necessary to review the regulations on auditing

audit oversight. In this context, it is intended to replace CMVM Regulation No. 4/2015, of January 25, with the draft regulation under analysis.

6. Thus, this Project aims to regulate the registration and endorsements to the registration of Statutory Auditors (ROC), Firms of Statutory Auditors (SROC) and auditors and audit entities from other Member States with the CMVM; procedures relating to compliance with reporting duties by auditors and public interest entities to the CMVM and the exchange of information between the Order of Official Auditors (OROC) and the CMVM.

7. The draft Regulation results in the processing of personal data by auditors and SROC representatives, which makes it important to analyze their compliance with the legal regime for the protection of personal data.

8. The processing of personal data by the CMVM comprises the full name; type of identification document, identification document number; tax identification number (NIF); TIN country, date of birth; OROC registration number, position or position held; telephone contact, email address; address and postal code; enjoyment of civil and political rights.

9. Such data appear to be necessary and adequate for the purpose of supervising the CMVM, provided for in paragraphs 1 and 4 of article 4 of the Legal Framework for Audit Supervision, approved by Law No. 148/2015, of September 9, last amended by Law No. 99-A/2021, of December 31, and Article 353(1) and Article 359(1)(f) of the Securities Code, approved by Decree-Law No. 486/99, of November 13, in compliance with the principle of data minimization provided for in Article 5(1)(c) of

the RGPD.

10. However, under the terms of paragraph a) of Article 17 of the Draft Regulation, the OROC will report to the CMVM “The identification of the disciplinary and investigation processes that have ended and are ongoing with the Disciplinary Council of the OROC, with a summary of the respective causes and status of the process, pursuant to Annex 19».

11. However, there is no lawful basis for the communication of such data, in particular those relating to processes in progress with the Disciplinary Council of OROC. Such processes include personal data of particular sensitivity from the point of view of fundamental rights and freedoms, deserving specific protection, provided for in article 10 of the RGPD.

12. The CJEU has already ruled on the special sensitivity of these data in the Judgment of 9/24/2019, Case C-136/17, although in a different context, where it states “the purpose of the said provisions (articles 9 and 70 of the RGPD) consists of ensuring greater protection against such processing which, due to the specific sensitivity of these data, may constitute, as is also apparent from recital 51 of this regulation, interference

particularly serious in relation to the fundamental rights to respect for private life and the protection of personal data, guaranteed by Articles 7 and 8 of the Charter.”

13. Incidentally, such a solution, without support from a specific provision in a legislative act, will always be inadmissible given the administrative autonomy of OROC, as a professional order, as it is only up to the professional community that composes it to assess, for disciplinary purposes, professional conduct of its members. In effect, the communication that a disciplinary or inquiry procedure is ongoing, without any illicit commission having yet been demonstrated, could only be useful in allowing the CMVM to assess and draw consequences from the fact that a procedure of that nature has been opened. type against a certain professional, with which this entity would be invading the attributions of that professional order.

14. Thus, in view of the absence of legal grounds for the processing of the data in question, and the need to process them in view of the purposes of supervision of the CMVM, it is recommended that article 17 be reformulated and , consequently, of Annex 19, in order to contemplate the communication only of information related to disciplinary and investigation processes that have ended, in compliance with the principles of legality and minimization of data provided for, respectively, in paragraph

a) and c) of paragraph 1 of article 5 of the GDPR.

15. As for the initial accreditation of the main users, article 18 of the Draft Regulation provides that it will begin via email, adding for this purpose the elements contained in the regulation (for the time being still in draft) of the BUE of the CMVM .

16. It should be noted that an accreditation mechanism using strictly electronic mail does not guarantee the accuracy of the data or the confirmation of identity. In order to try to guarantee, at the very least, the accuracy of the data and the professional quality of the main users, it is proposed that the accreditation of this type of profile include, in addition to the immediate notification, via email, of the data holders requesting validation of the data, further contact , by telephone or post, with an identity verification code to activate the main user account.

17. It is also suggested as an authentication requirement, for this account profile with high permissions, the 2FA mechanism (double authentication factor).

18. In turn, article 3 of the draft regulation provides “when any of the Annexes to this regulation does not express the file format for reporting information, the report is carried out in a data file with the extension XLSX». Warnings are given to the low security of these files, as they do not have any kind of robust mechanism to encrypt the personal data contained therein.

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

19. Therefore, it is not recommended to carry out mandatory reports to the CMVM using this file format, namely the XLSX format, as it is an open format and prone to infection with malicious code. If the files are sent via email, they must be encrypted with a password, to be transmitted via an alternative channel (eg telephone, SMS).

20. Furthermore, the projected regime does not raise reservations from the perspective of its compliance with the legal data protection regime, except for data conservation data, in relation to 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. After the applicable limitation periods or others imposed by law, personal data may still be retained for the purposes of definitive or historical archiving, under the terms of the aforementioned Decree-Law.

21. 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 referring this 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.

22. Thus, the CNPD recommends specifying the retention periods of 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. Section a) Article 13(2) GDPR).

III. Conclusion

23. Essentially, the Draft Regulation does not raise reservations from the perspective of its compliance with the legal data protection regime, except for the period of retention of personal data, which does not comply with the principle of limitation of conservation, as well as for the communication of personal data relating to ongoing disciplinary and investigation processes, for which there is no legal basis, and which also appears to be irrelevant and unnecessary for the CMVM's supervisory role.

24. Thus, the CNPD, under the terms and with the grounds set out above, recommends:

The. Setting in the Project's articles the retention periods for the personal data being processed;

B. The reformulation of article 17 of the Project and, consequently, of Annex 19, so as to contemplate only the communication of information regarding disciplinary and investigation processes that have ended.

25. The CNPD also recommends the adoption of robust security measures in the processing of personal data, as suggested above, in points 16 to 19.

Approved at the meeting of April 11, 2023

_____——>

Filipa Calvao (President)

Av. D. Carlos 1,134,1o 1200-651 Lisbon

T (+351) 213 928 400

F (+351) 213 976 832

geral@cnpd.pt

wwwvr.cnpd.pt