

PARECER/2023/38

I. Pedido

1. A Comissão do Mercado de Valores Mobiliários (CMVM) solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de parecer sobre o projeto de Regulamento (Projeto) que procede à regulamentação do Regime Jurídico da Supervisão de Auditoria, aprovado pela Lei n.º 148/2015, de 9 de setembro, e alterado pela Lei n.º 35/2018, de 20 de julho, e pela Lei n.º 99-A/2021, de 31 de dezembro, relativo ao registo de revisores oficiais de contas, de sociedades de revisores oficiais de contas, de auditores e de entidades de auditoria de Estados-Membros junto da CMVM, de alguns aspetos do exercício da atividade de auditoria e da sua supervisão pela CMVM, bem como da comunicação de informações à CMVM. O presente regulamento procede ainda à revogação do Regulamento da CMVM n.º 4/2015, de 26 de janeiro.
2. Foi enviada em anexo uma Avaliação de Impacto sobre Proteção de Dados pessoais (AIPD) relativa ao presente projeto de regulamento da CMVM e o Documento para Consulta Pública da CMVM n.º 5/2023.
3. A CNPD emite parecer no âmbito das suas atribuições e competências, enquanto autoridade administrativa independente com poderes de autoridade para o controlo dos tratamentos de dados pessoais, conferidos pela alínea c) do n.º 1 do artigo 57.º, a alínea b) do n.º 3 do artigo 58.º e n.º 4 do artigo 36.º, todos do Regulamento (UE) 2016/679, de 27 de abril de 2016 – Regulamento Geral sobre a Proteção de Dados (doravante RGPD), em conjugação com o disposto no artigo 3.º, no n.º 2 do artigo 4.º e na alínea a) do n.º 1 do artigo 6.º, todos da Lei n.º 58/2019, de 8 de agosto, que executa na ordem jurídica interna o RGPD.

II. Análise

4. Nos termos do artigo 62.º do Código do Procedimento Administrativo, aprovado pelo Decreto-Lei n.º 4/2015, de 7 de janeiro, alterado em último pelo Decreto-Lei n.º 11/2023, de 10 de fevereiro, e do artigo 357.º-A do Código dos Valores Mobiliários, a CMVM pretende implementar o balcão único eletrónico da CMVM (BUE), através do qual irão processar-se obrigatoriamente todas as interações entre a CMVM e os seus supervisionados. Assim, revela-se necessário regulamentar os formatos e os meios de cumprimento dos deveres de informação pelos auditores e demais supervisionados conexos, para que, tanto do lado da entidade supervisora como do lado das referidas entidades supervisionadas, seja possível, a partir da data de lançamento do BUE, a operacionalização e manutenção dos reportes legalmente devidos.
5. Por outro lado, com a entrada em vigor da Lei n.º 99-A/2021, de 31 de dezembro, que procedeu, entre outras, à alteração do Estatuto da Ordem dos Revisores Oficiais de Contas ("EOROC") e do Regime Jurídico da Supervisão de Auditoria ("RJSA"), torna-se necessário proceder a uma revisão da regulamentação em matéria de

supervisão de auditoria. Neste âmbito, pretende-se a substituição do Regulamento da CMVM n.º 4/2015, de 26 de janeiro, pelo projeto de regulamento em análise.

6. Assim, o presente Projeto visa regular o registo e averbamentos ao registo de Revisores Oficiais de Contas (ROC), Sociedades de Revisores Oficiais de Contas (SROC) e auditores e entidades de auditoria de outros Estados-Membros junto da CMVM; os procedimentos relativos ao cumprimento dos deveres de reporte pelos auditores e pelas entidades de interesse público à CMVM e a troca de informações entre a Ordem dos Revisores Oficiais de Contas (OROC) e a CMVM.

7. Do projeto de Regulamento resultam tratamentos de dados pessoais dos auditores e dos representantes de SROC pelo que importa uma análise da sua conformidade com o regime jurídico de proteção de dados pessoais.

8. O tratamento de dados pessoais pela CMVM compreende o nome completo; tipo de documento de identificação, número do documento de identificação; número de identificação fiscal (NIF); país do NIF, data de nascimento; número de inscrição na OROC, cargo ou função exercida; contacto telefónico, endereço eletrónico; morada e código postal; gozo de direitos civis e políticos.

9. Tais dados mostram-se necessários e adequados à finalidade de supervisão da CMVM, prevista nos n.ºs 1 e 4 do artigo 4.º do Regime Jurídico de Supervisão de Auditoria, aprovado pela Lei n.º 148/2015, de 9 de setembro, alterada em último pela Lei n.º 99-A/2021, de 31 de dezembro, e no n.º 1 do artigo 353.º e na alínea f) do n.º 1 do artigo 359.º do Código de Valores Mobiliários, aprovado pelo Decreto-Lei n.º 486/99, de 13 de novembro, em cumprimento do princípio de minimização de dados previsto na alínea c) do n.º 1 do artigo 5.º do RGPD.

10. Porém, nos termos da alínea a) do Artigo 17.º do Projeto de Regulamento, serão reportados à CMVM pela OROC «A identificação dos processos disciplinares e de inquérito findos e em curso junto do Conselho Disciplinar da OROC, com um resumo das respetivas causas e estado do processo, nos termos do Anexo 19».

11. Ora não se encontra fundamento de licitude para a comunicação de tais dados, em especial dos relativos a processos em curso junto do Conselho Disciplinar da OROC. Tais processos integram dados pessoais de especial sensibilidade do ponto de vista dos direitos e liberdades fundamentais, merecendo uma proteção específica, prevista no artigo 10.º do RGPD.

12. Sobre a especial sensibilidade destes dados já se pronunciou o TJUE no Acórdão de 24.9.2019, Processo C-136/17, embora num contexto diverso, onde afirma «a finalidade das referidas disposições (artigo 9.º e 10.º do RGPD) consiste em assegurar uma maior proteção contra tais tratamentos que, devido à sensibilidade específica destes dados, podem constituir, conforme também resulta do considerando 51 deste regulamento, uma ingerência

especialmente grave nos direitos fundamentais ao respeito pela vida privada e à proteção dos dados pessoais, garantidos pelos artigos 7.º e 8.º da Carta.»

13. Aliás, uma tal solução, sem apoio em previsão específica em ato legislativo, sempre será inadmissível face à autonomia administrativa da OROC, enquanto ordem profissional, por caber somente à comunidade profissional que a compõe a apreciação, para fins disciplinares, das condutas profissionais dos seus membros. Com efeito, a comunicação de que um processo disciplinar ou de inquérito está em curso, sem que esteja ainda demonstrada a prática de qualquer ilícito, só poderia ter a utilidade de permitir à CMVM valorar e retirar consequências do facto de ter sido aberto um processo daquele tipo contra um determinado profissional, com o que esta entidade estaria a invadir as atribuições daquela ordem profissional.

14. Deste modo, face à ausência de fundamento de licitude para o tratamento dos dados em causa, de resto não se alcançando a necessidade de tratamento dos mesmos face à finalidade de supervisão da CMVM, recomenda-se a reformulação do artigo 17.º e, conseqüentemente, do Anexo 19, por forma a contemplar a comunicação apenas de informação relativa a processos disciplinares e de inquérito findos, em cumprimento dos princípios de licitude e de minimização dos dados previstos respetivamente na alínea a) e c) do n.1 do artigo 5.º do RGPD.

15. Quanto à credenciação inicial dos utilizadores principais, o artigo 18.º do Projeto de regulamento dispõe que a mesma terá início através de correio eletrónico, juntando para o efeito os elementos constantes do regulamento (por ora ainda em projeto) do BUE da CMVM.

16. Observa-se que um mecanismo de credenciação utilizando estritamente o correio eletrónico não garante a exatidão dos dados nem a confirmação de identidade. Para tentar garantir, no mínimo, a exatidão dos dados e a qualidade profissional dos utilizadores principais propõe-se que a credenciação deste tipo de perfil inclua, além da notificação imediata, via correio eletrónico, dos titulares dos dados solicitando validação dos dados, ulterior contacto, por via telefónica ou postal, com um código de verificação de identidade para ativação da conta de utilizador principal.

17. Sugere-se ainda como requisito de autenticação, para este perfil de conta com permissões elevadas, o mecanismo de 2FA (duplo fator de autenticação).

18. Por sua vez, o artigo 3.º do projeto de regulamento dispõe «quando em qualquer um dos Anexos ao presente regulamento não se encontre expresso o formato do ficheiro para o reporte da informação, o reporte é efetuado em ficheiro de dados com extensão XLSX». Adverte-se para a pouca segurança destes ficheiros, não possuindo qualquer tipo de mecanismo robusto que permita cifrar dados pessoais que dele constem.

19. Assim, considera-se não ser recomendável proceder aos reportes obrigatórios à CMVM recorrendo a este formato de ficheiro, nomeadamente o formato XLSX, por ser um formato aberto e propenso à infeção com código malicioso. Se o envio dos ficheiros for através de correio eletrónico, deverá ser cifrado com uma senha, a transmitir por canal alternativo (ex: telefone, SMS).

20. No mais, o regime projetado não suscita reservas na perspetiva da sua conformidade do regime jurídico da proteção de dados exceto quanto aos dados de conservação dos dados, em relação aos quais o Projeto é omissivo. De facto, limita-se a referir no preâmbulo que os mesmos são conservados em conformidade com os princípios do interesse administrativo e utilidade administrativa, previstos no Decreto-Lei n.º 16/93, de 23 janeiro, ou seja, pelo menos até à data em que se esgote a finalidade que fundamentou a sua recolha, acrescida dos prazos de prescrição, nomeadamente contraordenacional, tributária ou civil. Findos os prazos de prescrição aplicáveis ou outros impostos por lei, os dados pessoais poderão ainda ser conservados para efeitos de arquivo definitivo ou histórico, nos termos do referido Decreto-Lei.

21. Ora, como já referido no Parecer n.º 118/2022, aprovado em 21 de dezembro de 2022, a CNPD não discute o interesse público da CMVM na conservação da informação pessoal – interesse que o citado Decreto-Lei prevê –, mas assinala que, remetendo esse diploma legal para regulamento administrativo (Decreto Regulamentar) a fixação dos prazos de conservação (cf. n.º 2 do artigo 15.º do Decreto-Lei n.º 16/93), não pode deixar de se exigir também aqui, no contexto dos tratamentos de dados pessoais realizados pela CMVM, a fixação de prazos para a conservação dos dados pessoais objeto de tratamento, em função da necessidade da conservação de tais dados para as finalidades visadas, nos termos da alínea e) do n.º 1 do artigo 5.º do RGPD. Nesse sentido aponta também o n.º 3 do artigo 6.º do RGPD.

22. Assim, a CNPD recomenda a especificação dos prazos de conservação dos dados pessoais, até porque, nos termos do artigo 13.º do RGPD a CMVM tem o dever de prestar informação quanto aos mesmos aos titulares dos dados (cf. Alínea a) do n.º 2 do artigo 13.º do RGPD).

III. Conclusão

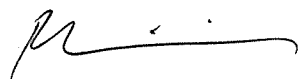
23. No essencial, o Projeto de Regulamento não suscita reservas na perspetiva da sua conformidade do regime jurídico da proteção de dados, exceto quanto ao período de conservação dos dados pessoais, que não cumpre o princípio da limitação da conservação, bem como quanto à comunicação dos dados pessoais relativos a processos disciplinares e de inquérito em curso, para a qual não se encontra fundamento de licitude, afigurando-se também não pertinente e desnecessária para a função de supervisão da CMVM.

24. Assim, a CNPD, nos termos e com os fundamentos expostos, recomenda:

- a. A fixação no articulado do Projeto dos prazos de conservação dos dados pessoais objeto de tratamento;
- b. A reformulação do artigo 17.º do Projeto e, conseqüentemente, do Anexo 19, de modo a contemplar somente a comunicação da informação relativa a processos disciplinares e de inquérito findos.

25. A CNPD recomenda também a adoção de medidas de segurança robustas no tratamento de dados pessoais, nos termos sugeridos supra, nos pontos 16 a 19.

Aprovado na sessão de 11 de abril de 2023



Filipa Calvão (Presidente)