

## PARECER/2023/35

### I. Pedido

1. A Comissão do Mercado de Valores Mobiliários (CMVM) solicitou à Comissão Nacional de Proteção de Dados (CNPDP) a emissão de parecer sobre o projeto de Regulamento que visa regular o balcão único eletrónico da CMVM. Procede ainda à revogação do Regulamento da CMVM n.º 3/2016, relativo ao modo de prestação de informação à CMVM por pessoas e entidades sujeitas à sua supervisão através do domínio extranet.
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 CNPDP 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, bem como a interação da CMVM com outros interessados que tenham interesse em beneficiar do acesso ao balcão único eletrónico, mas numa base voluntária. Excluem-se as interações relativas a processos de contraordenação promovidos pela CMVM, os quais seguem um regime legal próprio.
5. Do documento de consulta pública resulta que o BUE terá as seguintes funcionalidades: a) procedimento de autenticação eletrónica; Envio de informação imposta por regulamentação da CMVM por preenchimento de questionário ou formulário eletrónico; Entrega e depósito de documentação (ex. documentação necessária ao dossier de registo de atividade; documentação a entregar pelas entidades sujeitas a supervisão; documentação solicitada a entidades supervisionadas após supervisões presenciais); Envio e receção de comunicações entre a CMVM e os utilizadores, incluindo realização de pedidos e outros procedimentos por formulário eletrónico e mecanismo de consulta sobre o tratamento dos pedidos e estado dos procedimentos; Pagamento de serviços de supervisão e contrapartida por atos da CMVM, incluindo mecanismos de emissão automática de recibo;

Notificação eletrónica de cobrança de atos de supervisão, através de integração com a plataforma "Notificações Eletrónicas do Estado".

6. Nos termos do preâmbulo do Projeto, a segurança e o tratamento de dados pessoais no âmbito do presente regulamento da CMVM obedecem ao disposto no Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, e legislação nacional conexas.

7. Do projeto de Regulamento resultam tratamentos de dados pessoais dos supervisionados, dos utilizadores, dos utilizadores principais, dos terceiros e dos terceiros mandatários, na aceção das alíneas 7) a 11) do artigo 2.º, pelo que importa uma análise da sua conformidade com o regime jurídico de proteção de dados pessoais.

8. Nos termos da AIPD, o tratamento de dados pessoais dos utilizadores, dos utilizadores principais, dos terceiros e dos terceiros mandatários compreende o nome completo, número de identificação fiscal (NIF), email, telefone, fax. Note-se que o dado NIF é necessário para efeitos da faturação relativa a serviços solicitados pelos utilizadores através do BUE. Uma vez que o presente projeto regula apenas o funcionamento e o acesso ao BUE, tais dados mostram-se necessários e adequados à finalidade em causa, em cumprimento do princípio de minimização de dados previsto na alínea c) do n.º 1 do artigo 5.º do RGPD. Note-se que são ainda objeto de tratamento o nome e assinatura do supervisionado pessoa singular, bem como a qualidade/função, endereço eletrónico e assinatura dos membros de gestão dos representantes dos supervisionados pessoas coletivas.

9. O artigo 5.º dispõe que o acesso dos supervisionados ao BUE se efetua através dos seus utilizadores cuja nomeação é solicitada no momento em que pedem o ato pelo qual pretendem vir a ser supervisionados. O pedido de nomeação dos utilizadores dos supervisionados é *feito por utilizador* através do BUE nos termos dos Anexos I e II.

10. Ora, o n.º 2 do artigo 5.º do Projeto deixa dúvidas quanto ao sentido do termo utilizador, uma vez que o interessado ainda não foi nomeado como tal aquando da sua primeira interação na plataforma. Sugere-se, por isso, a clarificação da redação do preceito.

11. O Artigo 7.º do Projeto regula o processo de credenciação. Sugere-se que na execução do Regulamento se adote um mecanismo de autenticação robusto, que assente, por exemplo, no mecanismo de 2FA (duplo fator de identificação).

12. Ainda relativamente a este artigo importa notar que o n.º 1 dispõe que recebido o pedido de credenciação como utilizador no BUE, a CMVM envia imediatamente *mensagem* ao futuro utilizador com as instruções para finalizar a credenciação, prazo para o fazer e as consequências do não cumprimento tempestivo das instruções.

13. Tal disposição não esclarece o meio pelo qual tal mensagem é enviada, se por *email* ou por *sms*. Lembra-se que um mecanismo de credenciação efetuado estritamente por uma destas vias é fraco e não serve de garantia de exatidão dos dados e confirmação de identidade. Para tentar garantir, no mínimo, a exatidão dos dados e a qualidade profissional dos utilizadores propõe-se que a credenciação deste tipo de perfil inclua a notificação imediata, via correio eletrónico, dos titulares dos dados solicitando validação dos dados e ulterior contacto, por via telefónica (*sms*) ou postal, com um código de verificação de identidade para ativação da conta de utilizador.
14. Por sua vez, no documento de consulta pública enviado consta, entre as funcionalidades do BUE, a notificação eletrónica de cobrança de atos de supervisão, através de integração com a plataforma "Notificações Eletrónicas do Estado". Ora, o Serviço Público de Notificações Eletrónicas (SPNE) é gerido pela Agência para a Modernização Administrativa, I.P., (AMA, I.P.), pelo que, deverão a CMVM e a AMA, I.P., por acordo, estabelecer as respetivas responsabilidades pelo cumprimento do RGPD, definindo a qualidade em que cada uma destas entidades atua no âmbito das notificações por via da plataforma do SPNE, se como subcontratante ou corresponsável, nos termos do n.º 1 do artigo 26.º e n.º 3 do artigo 28.º do RGPD.
15. Nestes termos, a CMVM deve prestar informação clara aos titulares dos dados sobre esse tratamento e a medida da sua responsabilidade pelo mesmo.
16. Por sua vez, da consulta dos artigos 15.º e 16.º do Projeto de Regulamento verifica-se que são utilizados formatos de ficheiros não cifrados: Text/PDF e ASCII/XML. Da leitura do Artigo 14.º afere-se que a transferência destes ficheiros está cifrada (sFTP/FTPS), mas o seu repositório central na CMVM e controlos de segurança não são conhecidos. A CNPD recomenda que o Projeto contemple a definição de medidas técnicas e organizativas adequadas para assegurar um nível de segurança do tratamento adequado ao risco, nos termos do artigo 32.º do RGPD, e em conformidade com o n.º 3 do artigo 6.º do RGPD.
17. Adicionalmente, a propósito da análise da AIPD, constata-se que o mitigar o risco identificado, através do registo de um log, que é o único controlo de mitigação previsto é o registo eletrónico (*log*). Sugere-se que este controlo de mitigação de risco seja complementado com a política de permissões, gestão de histórico de alterações e, em situação extrema, cópias de segurança para poder recuperar dados indevidamente alterados.
18. No mais, o regime projetado não suscita reservas na perspetiva da sua conformidade do regime jurídico da proteção de dados exceto quanto aos prazos 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.

19. 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.

20. 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

21. No essencial, o Projeto de Regulamento não suscita reservas na perspetiva da sua conformidade do regime jurídico da proteção de dados, com exceção da falta de especificação dos prazos de conservação dos dados pessoais. Assim, a CNPD recomenda a fixação no articulado do Projeto dos prazos de conservação dos dados pessoais objeto de tratamento (cf. supra, pontos 19 e 20).

22. No mais, a CNPD recomenda também a clarificação do n.º 2 do artigo 5.º do Projeto de Regulamento, quanto ao termo *utilizador* face à ausência de credenciação nessa qualidade na primeira interação na plataforma (cf. supra, pontos 9 e 10).

23. Finalmente, a CNPD recomenda ainda a adoção de medidas de segurança robustas no tratamento de dados pessoais, nos termos sugeridos supra, nos pontos 11, 13, 16 e 17, e lembra o dever que recai sobre a CMVM de prestar informação clara aos titulares dos dados sobre o tratamento de dados pessoais realizado através do BUE e a medida da sua responsabilidade pelo mesmo (cf. supra, pontos 14 e 15).

Aprovado na reunião de 11 de abril de 2023



Filipa Calvão (Presidente)