CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2026/36

I. Pedido

1. O Presidente da Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de Parecer sobre o projeto de norma regulamentar (Projeto) que visa proceder a alterações das normas regulamentares n.º s 4/2023-R e 5/2023-R, de 11 de julho, e 13/2020-R, de 30 de dezembro.

2. 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, conjugado com a alínea *b)* do n.º 3 do artigo 58.º, e com o 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.

3. O Projeto não vem acompanhado de avaliação de impacto sobre a proteção de dados pessoais (AIPD) nos termos conjugados dos artigos 18.º n.º 4 da Lei 43/2004, 7.º da Lei 58/2019, e 35.º do RGPD.

II. Análise

4. Seguindo de perto o preâmbulo do Projeto, a Lei n.º 73/2025, de 23 de dezembro, executa na ordem jurídica interna o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro (Regulamento DORA).

5. Nos termos do n.º 1 do artigo 3.º da referida lei, a ASF é a autoridade competente para assegurar o cumprimento do Regulamento DORA, da lei e da legislação ou regulamentação europeia ou nacional aplicável em matéria de resiliência operacional digital, no que respeita às entidades sujeitas à respetiva supervisão.

6. Determina ainda o n.º 1 do artigo 2.º da Lei n.º 73/2025, de 23 de dezembro, que o regime previsto naquele regulamento, na referida lei e na legislação ou regulamentação europeia ou nacional relevante em matéria de resiliência operacional digital é aplicável às empresas de seguros e de resseguros com sede em Portugal às quais se aplica o regime jurídico de acesso e exercício da atividade seguradora e resseguradora (RJASR), aprovado pela Lei n.º 147/2015, de 9 de setembro, e às entidades gestoras de fundos de pensões autorizadas em Portugal às quais se aplica o regime jurídico da constituição e do funcionamento dos fundos de pensões e das entidades gestoras de fundos de pensões (RJFP), aprovado pela Lei n.º 27/2020, de 23 de julho.

7. Adicionalmente, nos termos da alínea *d)* do n.º 2 do artigo 232.º do RJASR, é aplicável às sucursais de empresas de seguros e de resseguros de um país terceiro o regime geral aplicável às empresas de seguros e de resseguros

com sede em Portugal, designadamente, o artigo 64.º, cujo n.º 6 determina que "*A fim de adotar as medidas necessárias para assegurar a continuidade e a regularidade do exercício das suas atividades, incluindo o desenvolvimento de planos de contingência, as empresas de seguros e de resseguros devem utilizar sistemas, recursos e procedimentos adequados e proporcionados e, em especial, criar e gerir sistemas de rede e informação em conformidade com o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022.*".

8. Por outro lado, da conjugação do disposto na alínea *o)* do n.º 1 com a alínea *e)* do n.º 2, ambos do artigo 2.º do Regulamento DORA, resulta que este é aplicável aos mediadores de seguros, de resseguros e de seguros a título acessório que não sejam microempresas ou pequenas ou médias empresas, na aceção dos pontos 60), 63) e 64) do artigo 3.º do referido regulamento. Assim, os mediadores de seguros, de resseguros e de seguros a título acessório que não sejam microempresas ou pequenas ou médias empresas, nos termos do Regulamento DORA, devem reportar à ASF informação em matéria de resiliência operacional digital, conforme previsto na presente norma regulamentar.

9. Neste sentido, cumpre proceder à introdução de novos deveres de reporte à ASF para efeitos do exercício das competências de supervisão que lhe estão legalmente cometidas, nos termos da Lei n.º 73/2025, de 23 de dezembro.

10. Assim, estabelece-se, através da presente alteração regulamentar, a prestação de informação sobre acordos contratuais relativos à utilização dos serviços de tecnologias de informação e comunicação (TIC) prestados por terceiros prestadores de serviços de TIC, bem como em caso de ocorrência de incidentes de carácter severo relacionados com as TIC e ciberameaças significativas, de acordo com o disposto no Regulamento DORA, e respetivos atos delegados e de execução.

11. Prevê-se ainda a possibilidade de a ASF solicitar o relatório de análise do quadro de gestão do risco associado às TIC, nos termos do Regulamento DORA, e uma estimativa dos custos e perdas anuais agregados causados por incidentes de carácter severo relacionados com as TIC, nos termos deste regulamento e de acordo com as Orientações do Comité Conjunto das ESA relativas à estimativa dos custos e perdas anuais agregados causados por incidentes de carácter severo relacionados com as TIC nos termos do Regulamento (UE) 2022/2554, assim se procedendo igualmente à respetiva incorporação no quadro jurídico aplicável.

12. Por último, regulamenta-se a comunicação à ASF da participação em acordos de partilha de informações específicas e sensíveis relativas a ciberataques, após validação dessa mesma participação ou, quando aplicável, após a cessação da sua participação, assim que esta produza efeitos.

13. São revogadas a Norma Regulamentar n.º 6/2022-R, de 7 de junho, relativa à segurança e governação das tecnologias de informação e comunicação (TIC) e subcontratação a prestadores de serviços de computação em nuvem, e a Norma Regulamentar n.º 7/2024-R, de 20 de agosto, relativa à segurança e governação das tecnologias

de informação e comunicação (TIC) e subcontratação a prestadores de serviços de computação em nuvem no âmbito da gestão de fundos de pensões. São ainda revogadas a Norma Regulamentar n.º 9/2024 R, de 26 de setembro, que regula a comunicação à ASF de incidentes de carácter severo relacionados com as TIC, e a Circular n.º 3/2025, de 8 de abril, sobre o reporte de incidentes de carácter severo relacionados com as TIC e de ciberameaças significativas.

14. Nos termos do n.º 1 do artigo 1.º a presente norma regulamentar procede à:

a) Quinta alteração à Norma Regulamentar n.º 4/2023-R, de 11 de julho, que regula a prestação de informação pelas entidades supervisionadas à Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) para efeitos do exercício das competências de supervisão que lhe estão legalmente cometidas, alterada pela Norma Regulamentar n.º 6/2024-R, de 20 de agosto, pela Norma Regulamentar n.º 10/2024-R, de 5 de novembro, pela Norma Regulamentar n.º 11/2024-R, de 20 de novembro, e pela Norma Regulamentar n.º 7/2025-R, de 26 de agosto;

b) Quinta alteração à Norma Regulamentar n.º 5/2023-R, de 11 de julho, que define o conjunto de relatórios e elementos de índole financeira, estatística e comportamental que as sociedades gestoras de fundos de pensões devem remeter à ASF para efeitos do exercício das competências de supervisão que lhe estão legalmente cometidas, alterada pela Norma Regulamentar n.º 6/2024-R, de 20 de agosto, pela Norma Regulamentar n.º 10/2024-R, de 5 de novembro, pela Norma Regulamentar n.º 11/2024-R, de 20 de novembro, e pela Norma Regulamentar n.º 7/2025-R, de 26 de agosto;

c) Quarta alteração à Norma Regulamentar n.º 13/2020-R, de 30 de dezembro, que regulamenta o regime jurídico da distribuição de seguros e de resseguros, alterada pela Norma.

   Procede ainda, nos termos do n.º 2, à incorporação no quadro jurídico aplicável das Orientações do Comité Conjunto das Autoridades Europeias de Supervisão relativas à estima de custos e perdas anuais agregados causados por incidentes de carater severo relacionados com as TIC nos termos do Regulamento UE 2022/2554, de 5 de junho de 2024.

15. As alterações propostas consistem essencialmente no aditamento de normas relativas à prestação de informação relacionada com a resiliência operacional digital, designadamente no que respeita a: i) acordos contratuais relativos à utilização dos serviços de tecnologias de informação e comunicação (TIC) prestados por terceiros prestadores de serviços de TIC; ii) incidentes de carácter severo relacionados com as TIC e ciberameaças significativas; e iii) gestão do risco associado às TIC e iv) participação em acordos de partilha de informações específicas e sensíveis relativas a ciberataques, após validação dessa mesma participação ou, quando aplicável, após a cessação da sua participação, assim que esta produza efeitos.

16. Porém o Projeto é omisso quanto aos dados pessoais constantes na informação a prestar, limitando-se a ASF, no ofício que formaliza o pedido de parecer, indicar que «serão objeto de eventual tratamento pela ASF

dados de identificação (nome e código LEI, caso esta informação permita a identificação inequívoca do titular) e dados de contacto (endereço de correio eletrónico e contacto telefónico).

17. Note-se, ainda, que nas normas a aditar às normas regulamentares supramencionadas, consta a relativa ao «meio de prestação da informação». Quanto ao aditamento à Norma Regulamentar 4/2023-R, de 11 de julho, o n.º 4 do artigo 39.º E, dispõe igualmente que «os formulários, os modelos de reporte e as instruções a utilizar para efeitos da prestação de informação previsto no presente título, bem como as alterações aos mesmos, são disponibilizados no sítio da ASF na internet, após aprovação pelo Conselho de Administração desta Autoridade», encontrando-se idêntica formulação no n.º 7 do artigo 15.º da norma regulamentar n.º 5/2023,-R, de 11 de julho e no n.º 4 do artigo 57.º E aditado à Norma Regulamentar 13/2020-R, de 30 de dezembro.

18. Assim, constata-se que o Projeto não densifica os dados pessoais a tratar em virtude das alterações às normas regulamentares elencadas no artigo 1.º, remetendo tal definição para formulários a aprovar. Porém, determina que, relativamente à Norma Regulamentar 5/2023-R, de 11 de julho, os elementos previstos na alínea b) do n.º 1 do artigo 39.º-A e no artigo 39.º-C, e quanto à Norma Regulamentar n.º 13/2020, de 30 de dezembro, na alínea b) do n.º 1 do artigo 57.º-A e artigo 57.º-C devem incluir, em anexo cópia do «formulário relativo ao tratamento de dados pessoais, o qual deve ser do conhecimento de todos os titulares cujos dados pessoais constem dos referidos relatórios».

19. Por outro lado, e considerando que é referido no Projeto que os elementos previstos na alínea b) do n.º 1 do artigo 39.º-A e no artigo 39.º- D da Norma Regulamentar 4/2023-R, os elementos de reporte previstos nos artigos 5.º a 9.º, 13.º-A, e 13.ºB da norma regulamentar n.º 5/2023-R, de 11 de julho e os elementos previstos na alínea b) do n.º 1 do artigo 57.º-A e no artigo 57.º-D da NR 13/2020-R, de 30 de dezembro , devem ser remetidos por endereço eletrónico impõe-se a adoção de medidas de segurança específicas.

20. Saliente-se que relativamente a esta comunicação por correio eletrónico, deverão ser observadas todas as boas práticas de segurança da informação, constantes na Diretriz n.º 1/2023 da CNPD. Aqui se incluem as seguintes: prevenir erros na introdução manual de endereços de correio eletrónico, assegurar que os ficheiros enviados em anexo contêm apenas os dados pessoais que se pretendem comunicar, equacionar a criação de regras com o objetivo de adiar/atrasar a entrega de mensagens de correio eletrónico contendo dados pessoais, mantendo-as na "caixa de saída", por um tempo determinado, permitindo verificação de conformidade , após clique em enviar; encriptar com código, ao qual só o destinatário tenha acesso, as mensagens de correio eletrónico e confirmar com o destinatário, antes de envio da mensagem contendo dados pessoais, o endereço de correio eletrónico preferencial para contacto.

21. Sublinha-se que, ainda que o Projeto remeta para um Anexo titulado "Informação Relativa ao Tratamento de Dados Pessoais" alguma informação sobre o tratamento de dados pessoais, deveriam constar no articulado da lei habilitante (Lei n.º 73/2025, de 23 de dezembro) os elementos essenciais do regime aplicável ao tratamento de dados pessoais, e das específicas informações/dados a serem recolhidos e seu tratamento e fundamento, e não apenas um conjunto informativo dos direitos dos respetivos titulares, que apesar disso se reconhece como positivo.

22. De facto, o direito fundamental à proteção de dados pessoais, previsto no artigo 35.º da Constituição da República Portuguesa (CRP), e princípios e direitos, liberdades e garantias fundamentais conexos, sua definição é da competência reservada da Assembleia da República, através de Lei (contendo todo o regime legal, e que lhe poderá ser submetida pelo Governo através de uma Proposta de Lei), ou através de Lei de Autorização legislativa concedida ao Governo (que para tanto deverá submeter uma Proposta de Lei de autorização)– cf. alínea *b)* do n.º 1 do artigo 165.º da Constituição da República Portuguesa (CRP).

23. Na ausência da definição do regime de tratamentos de dados, a aferição em concreto, por parte desta Comissão, das condições de tratamento particulares dos dados em causa afigura-se prejudicada.

24. Passando agora à análise do Anexo relativo à informação relativa ao tratamento de dados pessoais, consubstanciando o direito de informação plasmado nos artigos 13.º e 14.º do RGPD, aí se define o responsável pelo tratamento, o fundamento de licitude e as finalidades do tratamento, os prazos de conservação e destinatários.

25. O Anexo relativo à informação aos titulares dos dados consagra que tais transferências só serão possíveis se o país terceiro for detentor de uma decisão de adequação pela Comissão Europeia ou «Se os países terceiros ou organizações internacionais apresentarem garantias adequadas, nos termos previstos no RGPD, atestando-se que os titulares dos dados gozam de direitos oponíveis e de medidas jurídicas corretivas eficazes, informação que a ASF comunicará aos titulares ou disponibilizará através do sítio da internet.» Note-se que, neste caso, deverá existir um acordo de colaboração que apresente garantias adequadas e nele estejam previstos os direitos oponíveis e efetivos dos titulares dos dados, bem como medidas corretivas eficazes, nos termos impostos pelo artigo 46.º deste diploma da União.

26. Quanto à transferência de dados pessoais deverá, também, especificar-se com clareza quais as circunstâncias concretas em que estas possam ocorrer, bem como, desejavelmente, as informações constantes no artigo 13.º do RGPD, concretamente, os destinatários (ou categorias de destinatários) dos dados pessoais, e quais os fins que as justificam.

27. Quanto aos direitos dos titulares dos dados importa referir que pese embora a ASF invocar a alínea e) do artigo 6.º n.º 1 do RGPD como fundamento de licitude do tratamento de dados pessoais, a obrigatoriedade da prestação de informação à ASF acaba por constituir uma obrigação legal ou jurídica para as entidades abrangidas, pelo que, não se poderá falar de um direito de oposição ao tratamento, no sentido que é transmitido pelo ponto h) desse mesmo anexo.

28. Quanto às medidas de segurança a adotar referidas no ponto g) do Anexo onde consta a informação relativa ao tratamento de dados pessoais, sem prejuízo da necessidade de revisão periódica, as mesmas revelam-se adequadas, devendo estas ser transportas para o articulado em análise.

29. Por última, a CNPD sublinha que a presente Proposta Regulamentar deveria ser acompanhada por uma avaliação de impacto, nos termos conjugados dos artigos 18.º, n.º 4 da Lei 43/2004, 7.º da Lei n.º 58/2019, e 35.º do RGPD.

III. Conclusão

30. Nos termos e com os fundamentos expostos a CNPD recomenda:

I – Quanto ao texto do projeto de norma regulamentar:

a) Densificar os dados pessoais objeto de tratamento;
b) Indicar as medidas de segurança a adotar, nomeadamente face ao envio de informação por correio eletrónico;

II – Quanto ao Anexo da informação aos titulares dos dados:

c) Especificar a transferência de dados pessoais que possa vir a ocorrer, determinando-se as circunstâncias, destinatários, e fins que a justificam;
d) A remoção do direito de oposição plasmado no ponto h) do Anexo referente aos dados pessoais, por não aplicável;

III - Recomenda-se ainda a ponderação de realização de avaliação prévia de impacto, nos termos conjugados dos artigos 18.º, n.º 4 da Lei 43/2004, 7.º da Lei n.º 58/2019, e 35.º do RGPD.

Aprovado na reunião de 2 de junho de 2026

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2026.06.02 21:23:07+01'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

CARTÃO DE CIDADÃO