

PARECER/2022/40

I. Pedido

1. A Autoridade de Supervisão de Seguros e de Fundos de Pensões (ASF) solicitou à Comissão Nacional de Proteção de Dados (CNPDP) a emissão de parecer sobre o projeto de norma regulamentar relativa à conduta de mercado e ao tratamento de reclamações por esta autoridade.
2. 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.
3. Foi, entretanto, a pedido da CNPDP, apresentada avaliação de impacto sobre a proteção de dados pessoais (AIPD).

II. Análise

4. 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 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, estabeleceram um conjunto de alterações em matéria de conduta de mercado dos operadores relativamente aos regimes que anteriormente regiam, respetivamente, o acesso e exercício da atividade seguradora e a atividade de gestão de fundos de pensões, que determinam a necessidade de revisão dos normativos atualmente aplicáveis, adaptando-os a nova legislação enquadradora das aludidas atividades.
5. Nos termos do artigo 159.º do RJASR e do artigo 149.º do RJFP, cabe à ASF estabelecer por norma regulamentar, as regras gerais a respeitar pelas empresas de seguros e pelas entidades gestoras de fundos de pensões no cumprimento dos deveres previstos em matéria de conduta de mercado, o que agora se concretiza.
6. Nos termos do preâmbulo, o presente projeto de norma regulamentar visa ainda proceder a uma atualização do regime aplicável à gestão de reclamações, ao provedor do cliente e ao interlocutor perante a Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF), e alarga o âmbito de aplicação da política de tratamento dos tomadores de seguros, segurados, beneficiários ou terceiros lesados à atividade de gestão de fundos de

pensões, regulando o relacionamento das entidades gestoras com os associados, contribuintes, participantes e beneficiários.

7. O projeto visa adaptar e sistematizar, ainda, os requisitos aplicáveis ao reporte para efeitos de supervisão comportamental e estabelece que as empresas de seguros e as entidades gestoras devem dispor de um sítio autónomo na Internet que inclua um separador específico com informação dedicada à matéria da conduta de mercado.

8. Por último, em consonância com o previsto nos artigos 157.º do RJASR, 198.º do RJFP e 76.º do regime jurídico da distribuição de seguros e de resseguros, aprovado pela Lei n.º 7/2019, de 16 de janeiro, concretizam-se os procedimentos aplicáveis ao tratamento das reclamações apresentadas à ASF relativamente a atos ou omissões das entidades supervisionadas.

9. Assim, o projeto contempla o tratamento de dados pessoais do provedor do cliente ou do provedor dos participantes e beneficiários e dos membros do respetivo órgão de gestão ou administração (dados de identificação e dados de contacto e *curriculum vitae*), nome completo e dados de contacto do reclamante e, caso aplicável, da pessoa que o represente; número do documento de identificação do reclamante; NIF, morada completa, idade, género, número de telemóvel, habilitações literárias e a descrição dos factos que motivaram a reclamação, com identificação dos intervenientes; dados de identificação interlocutor privilegiado para os contactos com o provedor; dados de identificação do interlocutor privilegiado para efeitos do contacto com a ASF, que incluem, para além da morada, o respetivo endereço de correio eletrónico. Nos termos da AIPD o tratamento de dados inclui ainda dados de categorias especiais (artigo 9.º do RGPD), em concreto dados relativos à saúde.

10. Os dados em causa são, em geral, adequados, pertinentes e limitados à finalidade de exercício dos poderes de supervisão da ASF e para tratamento de reclamações por esta entidade em obediência ao princípio da proporcionalidade e da minimização dos dados previsto na alínea c) do n.º 1 do artigo 5.º do RGPD.

11. Assinala-se, contudo, a aparente incongruência entre o elenco dos dados pessoais do cliente a tratar pela empresa de seguros ou pela entidade gestora, no contexto de uma reclamação, e o elenco dos dados pessoais do reclamante no contexto de uma relação apresentada à ASF: no primeiro caso, indica-se o número do documento de identificação civil (cf. alínea d) do n.º 2 do artigo 11.º do Projeto), enquanto no segundo caso, se exige o número de identificação fiscal (cf. alínea b) do n.º 3 do artigo 35.º do Projeto). Uma vez que não se encontra qualquer justificação para esta diferença quanto aos dados pessoais de identificação do reclamante e, especialmente, não se alcançar a razão por que um cidadão é identificado através do NIF e não do seu

18. Importa, por isso, assegurar que a informação sobre o tratamento de dados pessoais prestada nos sítios da Internet e na plataforma de gestão das reclamações não faça referência ao consentimento do reclamante, tão-pouco dependa de um qualquer ato de aceitação da referida informação. O que pode haver, se tal se demonstrar necessário para o efeito de prova de prestação da informação, é a exigência de uma declaração (ou confirmação) de que *se tomou conhecimento* da informação.

19. No que respeita à avaliação do risco, a maioria dos riscos identificados são apresentados com um impacto “Não significativo” após a implementação das medidas mitigadoras, ponderados a probabilidade e o impacto do mesmo.

20. Um dos riscos identificado pelo responsável prende-se com a recolha de dados através da integração com a plataforma do Livro de Reclamações Eletrónico. Porém, a documentação fornecida não detalha em que moldes essa integração é feita, não tornando possível averiguar dos eventuais riscos associados, da sua probabilidade e impacto, nem das medidas necessárias para a sua mitigação.

21. Por sua vez, os documentos em análise não detalham as atividades do tratamento associado à recolha presencial ou por *email* das reclamações. A AIPD apenas refere a recolha eletrónica via Portal do Consumidor ou Livro de Reclamações Eletrónico sendo omissa quanto à forma como essa recolha é feita e como esses dados são armazenados, se serão incluídos na plataforma interna para seguirem os trâmites processuais, bem quanto ao modo como essa informação é eliminada findo o tratamento.

22. Note-se que os documentos em análise pouco especificam sobre os detalhes técnicos da infraestrutura, sistemas e aplicações da solução, não permitindo avaliar se a mesma assegura um nível adequado para a segurança dos dados e privacidade. Pouco ou nada é dito sobre a política de gestão de acessos, sobre a política de gestão dos *backups*, sobre a proteção das máquinas com *software* de segurança (*e.g.*, antivírus), sobre a política de acessos às bases de dados e pastas de partilhas de ficheiros, sobre a criação e gestão dos registos de auditoria ao sistema que permita cadastrar os acessos e respetivas operações, sobre a segurança no transporte da informação e sobre a interligação entre os diversos sistemas.

23. Nessa medida, a CNPD não pode aferir com exatidão se todos os riscos foram identificados na AIPD, ou se outros deveriam estar incluídos, juntamente com as respetivas medidas de mitigação.

24. De todo o modo, tendo em conta que parte da infraestrutura residirá em máquinas com sistema operativo datado (Windows Server 2007, com Service Pack 2), o que pode implicar eventuais vulnerabilidades identificadas e passíveis de ser exploradas por terceiros, sempre se recomenda que as soluções implementadas sejam instaladas com as últimas versões (ou, ao menos, com versões recentes) do *software*,

número de identificação civil, a CNPD recomenda a reponderação daquelas normas, máxime, da alínea b) do n.º 3 do artigo 35.º do Projeto.

12. Considerando o número médio de reclamações analisadas constata-se que o número de titulares de dados envolvidos ronda os 9000 por ano. Assim, o elevado número de titulares e a natureza dos dados tratados reclamam a AIPD, ao abrigo do artigo n.º 35, n.º 3, alínea b) do RGPD, que se encontra anexa ao Projeto e que é considerada na presente análise.

13. A recolha de dados, embora se privilegie os meios eletrónicos, pode também ser realizada presencialmente. Pelos meios eletrónicos prevê-se a recolha por *email*, pelo *site* do Portal do Consumidor, e através da integração com a plataforma digital do Livro de Reclamações Eletrónico.

14. Prevê-se que os dados pessoais recolhidos possam ser comunicados a terceiros. Nos termos da AIPD apresentada, a ASF pode remeter os dados para as entidades reclamadas, uma vez que “o tratamento da reclamação implica contacto com a entidade para exercício do contraditório e prestação dos esclarecimentos devidos”. Essa divulgação é feita através da plataforma informática da ASF, o Portal ASF Operadores, disponível na internet no endereço <https://portaldasf.asf.com.pt/>, que permite o acesso restrito para tratamento das reclamações.

15. O acesso às aplicações internas na rede da ASF é feito mediante autenticação. Os computadores clientes estão no mesmo domínio e os utilizadores autenticam-se com as respetivas credenciais. Uma vez autenticados no domínio, o uso das aplicações não requer nova autenticação, sendo que o acesso é facultado mediante a definição e atribuição prévia de perfis de autorização.

16. O sítio do Portal do Consumidor permite ao reclamante submeter um pedido de esclarecimento, e submeter ou consultar o estado de uma reclamação.

17. Note-se que na submissão de uma reclamação o formulário abre uma janela com informação relativa ao tratamento de dados pessoais, consubstanciando o disposto no artigo 13.º do RGPD, onde se encontra identificado o responsável, a finalidade e fundamento de licitude do tratamento, os direitos do titular, e o contacto do Encarregado de Proteção de Dados (EPD). Todavia, parece decorrer da AIPD (ponto 14) que o fundamento de licitude do tratamento é o consentimento do reclamante, quando, em rigor, não é (cf., de resto, o ponto 18 da AIPD, onde se faz referência ao cumprimento de obrigação legal). Na verdade, o tratamento de reclamações pelas empresas de seguros ou entidades gestoras assenta em obrigação legal, sendo para a ASF necessário ao cumprimento da sua função pública de supervisão.

para pleno cumprimento do dever de aplicar as “medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco [...]”, nos termos do artigo 32.º, n.º 1, do RGPD.

25. Relativamente aos riscos identificados pelo responsável, a CNPD considera aceitáveis as medidas de mitigação propostas. Em concreto, as políticas de gestão de perfis de acesso e a implementação periódica dos respetivos procedimentos de revisão, é considerada adequada para os fins em vista, mantendo atualizado o conjunto de operadores capazes de aceder aos dados.

26. Por último, relativamente aos prazos de conservação dos dados, assinala-se que o n.º 3 do artigo do artigo 40.º do Projeto de Norma Regulamentar fixa o prazo de 5 anos, sem para o mesmo ser apresentado qualquer fundamento justificativo. Assim, não estando a CNPD em condições de concluir pelo cumprimento do princípio da limitação da conservação de dados pessoais consagrado na alínea e) do n.º 1 do artigo 5.º do RGPD, recomenda a reponderação deste aspeto do tratamento.

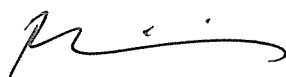
III. Conclusão

27. A análise do Projeto de norma regulamentar fica prejudicada pela omissão ou incompletude da informação prestada quanto a alguns elementos relativos ao tratamento de dados pessoais nele regulado, não permitindo avaliar plenamente o risco decorrente do referido tratamento.

28. De todo o modo, a CNPD recorda a importância de se adotarem medidas organizativas e técnicas que garantam o cumprimento dos princípios de proteção de dados e as regras previstas no RGPD, em especial no artigo 25.º e na alínea b) do n.º 1 do artigo 32.º do RGPD, relativa à segurança da informação, recomendando que sejam tidas em conta as observações acima expostas (em especial, nos pontos 18 e 24).

29. A CNPD recomenda ainda a reponderação da exigência do dado NIF para identificação do reclamante, na alínea b) do n.º 3 do artigo 35.º do Projeto (cf. supra, pontos 10 e 11), bem como do prazo de conservação dos dados, fixado no n.º 3 do artigo 40.º do Projeto (cf. supra, ponto 26).

Aprovado na sessão de 18 de maio de 2022



Filipa Calvão (Presidente)