CNPD
Comissão Nacional de Proteção de Dados

PARECER/2024/12

I. Pedido

1. A Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) submeteu à Comissão Nacional de Proteção de Dados (CNPD), para parecer, o Protocolo a ser celebrado com a Caixa Geral de Aposentações, I.P., (CGA), regendo os termos da partilha de informação relativa a responsáveis civis por acidentes de viação.

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.

II. Análise

3. Na prossecução das suas atribuições, compete à ASF a gestão do Fundo de Garantia Automóvel (FGA), nos termos da alínea *j)* do n.º 1 do artigo 7.º dos respetivos Estatutos e do n.º 3 do artigo 47.º do Decreto-Lei n.º 291/2007, de 21 de agosto.

4. Nos termos deste decreto-lei, compete ao FGA satisfazer as indemnizações decorrentes de acidentes rodoviários ocorridos em Portugal e noutros países membros da União Europeia, causados por responsável desconhecido ou isento da obrigação de seguro em razão do veículo em si mesmo, ou por responsável incumpridor da obrigação de seguro de responsabilidade civil automóvel. O FGA fica então sub-rogado nos direitos dos lesados, assistindo-lhe o direito a ser reembolsado pelos responsáveis civis e podendo para o efeito solicitar informações a entidades públicas e privadas, ao abrigo do disposto no artigo 56.º do referido Decreto-Lei n.º 291/2007, de 21 de agosto.

5. Assim, no exercício do direito de sub-rogação, o FGA carece do acesso à informação detida pela CGA relativamente à identificação, morada e rendimentos penhoráveis dos responsáveis civis.

6. O presente protocolo tem por objeto definir a natureza da informação a prestar pela CGA ao FGA relativamente a responsáveis civis por acidentes de viação, para efeitos do exercício do direito de sub-rogação deste nos termos dos artigos 54.º e seguintes do Decreto-Lei n.º 291/2007, de 21 de agosto, estabelecer os canais de comunicação para o efeito, identificar os interlocutores das partes e definir as responsabilidades destas no tratamento dos dados pessoais transmitidos. – cf. Cláusula 1.ª

7. O tratamento de dados resultante da execução do presente protocolo encontra fundamento de licitude nas alíneas c) e e) do n.º 1 do artigo 6.º do RGPD.

8. Nos termos da Cláusula 2.ª, nos pedidos de informação a efetuar à CGA relativamente a responsáveis civis por acidentes de viação, o FGA indica o seu número de processo interno e o nome completo do responsável civil. Nas respostas aos pedidos, a CGA comunica ao FGA se o responsável civil é ou não seu beneficiário e, em caso afirmativo, a respetiva morada, o Número de Identificação Fiscal (NIF), o Número de Identificação de Segurança Social (NISS), o valor mensal dos descontos para efeitos de carreira contributiva e o montante das pensões de que o beneficiário seja titular, bem como se as mesmas estão oneradas com penhoras ou outras garantias de crédito de terceiros.

9. Os dados pessoais objeto de tratamento são adequados e limitados ao que é necessário para a finalidade em causa em cumprimento do princípio da necessidade e da minimização dos dados previsto na alínea c) do n.º 1 do artigo 5.º do RGPD.

10. A Cláusula 3.ª é relativa à proteção de dados pessoais. Nela se consagra que cada uma das Partes é responsável pelo tratamento de dados pessoais no âmbito do presente Protocolo, competindo-lhes assegurar o cumprimento dos direitos dos titulares dos dados pessoais.

11. Constata-se que o acesso à informação é circunscrito a colaboradores funcionalmente adstritos à função e, no caso da ASF, autorizados para efeitos da instrução de processos de sinistro automóvel ou de procedimentos de reembolso das quantias pagas com a sua regularização, em obediência ao princípio need to Know.

12. É referido no n.º 1 da cláusula 4.ª que "Nas comunicações entre as partes é exclusivamente utilizado o correio eletrónico". Note-se que, no ofício que acompanha o envio da AIPD, é referido que foram implementadas medidas de mitigação de risco, sendo a que diz respeito ao correio eletrónico a "criação de email dedicado e de utilização exclusiva para troca de informações com a CGA, com acesso restrito aos interlocutores do FGA para o efeito".

13. Porém, o protocolo não refere se os dados pessoais objeto de tratamento constam de ficheiros anexos às mensagens de correio eletrónico ou são colocados diretamente no corpo das mensagens. A CNPD relembra que grande parte de ataques de software malicioso são levados a cabo escondendo o código infetado em ficheiros anexados a mensagens de correio eletrónico. Esses ficheiros aparentemente fidedignos, uma vez abertos, podem executar instruções arbitrárias no computador e enviar vírus informático através da rede local. E chama a atenção para a vertente dos ataques de *Phishing*, em que as mensagens têm hiperligações maliciosas.

14. Acresce que o recurso ao correio eletrónico implica o risco de o ficheiro ser enviado para o destinatário errado, sendo esta, aliás, uma forma dominante nas violações de dados que são notificadas à CNPD. Pode ainda

haver o acesso de terceiros às caixas de correio onde as mensagens ficam guardadas, no destino e na origem. Pelo que, não dispondo o ficheiro de alguma salvaguarda de acesso, não se considera prudente recorrer ao correio eletrónico para o seu envio.

15. Note-se que a AIPD não identifica nem endereça os riscos inerentes ao uso de correio eletrónico para implementação deste protocolo, nomeadamente ataques de software malicioso, *phishing* ou envio para destinatário errado.

16. Por sua vez, a CNPD manifesta a sua discordância com a análise de impacto, quando na coluna "Principais Impactos para os Titulares dos Dados se o Risco ocorrer", se indica "Perda de confidencialidade sobre os dados". De facto, os dados enviados ao FGA podem incluir dados sensíveis sobre situações economicamente vulneráveis, pelo que se circularem fora do sigilo consagrado no protocolo, poderão acarretar consequências negativas para os titulares dos dados.

17. Existe ainda um risco não identificado na AIPD e que, portanto, se encontra pendente de soluções de mitigação: a identificação do titular errado dos dados. Uma vez que os dados enviados à CGA para identificação são única e exclusivamente o nome completo do responsável civil, existe o risco de existir mais que um titular com o mesmo nome.

18. Sublinha-se que tanto a identificação errada como a violação de dados pessoais, neste âmbito, podem trazer consequências indesejadas aos seus titulares, por exemplo, danos de reputação, danos psicológicos, ou constrangimentos financeiros. Assim, a "Perda de confidencialidade sobre os dados" não deve ser considerado um impacto, mas a origem do mesmo.

19. Por sua vez o n.º 4 da Cláusula 3.ª dispõe que perante um incidente de segurança ou violação de dados pessoais que se mostre relevante para a execução do protocolo, cada parte obriga-se a notificar esse facto à outra, sem demora injustificada e, sempre que possível, até 24 (vinte e quatro) horas após ter tido conhecimento do mesmo. Ora tal obrigação existe também relativamente a autoridade de controlo e em relação aos titulares dos dados quando a violação for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares, pelo que se recomenda a sua referência no texto do protocolo (artigos 33.º e 34.º do RGPD).

20. Por último, quanto ao prazo de conservação de dados, o Protocolo limita-se a indicar a «conservação da informação pelo prazo associado às finalidades próprias dos responsáveis» sem, no entanto, o concretizar. Recomenda-se a indicação de um prazo de conservação de dados pessoais em obediência ao principio da limitação da conservação previsto na alínea e) do n.º 1 do artigo 5.º do RGPD.

III. Conclusões

21. Assim, com os fundamentos acima expostos, a CNPD recomenda:

a) A reformulação do n.º 1 da Cláusula 4.ª por forma a esclarecer a forma de envio de dados pessoais;

b) A adoção de medidas de mitigação do risco de identificação do titular errado dos dados identificado no ponto 17;

c) A alteração do n.º 3 da Cláusula 3.ª por forma a contemplar al obrigação de notificação da violação de dados pessoais à autoridade de controlo e aos titulares dos dados quando a violação for suscetível de implicar um elevado risco para os direitos e liberdades das pessoas singulares; e

d) A definição de um prazo de conservação de dados pessoais.

Aprovado na sessão de 23 de abril de 2024

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2024.04.23 19:04:16+01'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

CARTÃO DE CIDADÃO