CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2023/102

I. Pedido

1. O Instituto de Gestão Financeira da Segurança Social, IP. (IGFSS), o Instituto da Segurança Social dos Açores, I.P.R.A. (ISSA, IPRA), o Instituto de Segurança Social da Madeira, IP-RAM, (ISSM, IP-RAM), o Instituto de Informática, IP (II, I.P.) e a Caixa de Previdência dos Advogados e dos Solicitadores (CPAS) submeteram à Comissão Nacional de Proteção de Dados (doravante CNPD), para parecer, a minuta de Protocolo que tem por objetivo definir os termos e condições da comunicação e interoperabilidade entre as instituições envolvidas para efeitos de participação e execução de dívida da Caixa de Previdência dos Advogados e dos Solicitadores (CPAS).

2. São parte no presente Protocolo o Instituto de Gestão Financeira da Segurança Social, IP. (IGFSS), Instituto da Segurança Social dos Açores, I.P.R.A. (ISSA, IPRA), Instituto de Segurança Social da Madeira, IP-RAM, (ISSM, IP-RAM), Instituto de Informática, IP (II, I.P.) e a Caixa de Previdência dos Advogados e dos Solicitadores (CPAS).

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, 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

1. O Decreto-Lei nº 42/2001, de 9 de fevereiro, relativo à cobrança coerciva de dívidas à Segurança Social, aplica-se igualmente a todos os montantes devidos à Caixa de Previdência dos Advogados e Solicitadores (CPAS), sendo que, para efeitos do referido diploma, a CPAS é equiparada a instituição da segurança social.

2. O nº 1 do artigo 18º-A do Decreto-Lei nº 42/2001, de 9 de fevereiro, aditado pelo artigo 416º da Lei nº 2/2020, de 31 de março, determina que para efeitos de participação da dívida relativa à CPAS são estabelecidos canais específicos de comunicação e interoperabilidade entre as instituições envolvidas.

3. Por sua vez, o nº 2 do mencionado artigo 18º-A prevê que os termos e condições da comunicação e interoperabilidade são estabelecidos por protocolo a celebrar entre o IGFSS, I. P., o ISSA, IPRA, o ISSM, IP-RAM e a CPAS. O Despacho 6542/2023, publicado em 16 de junho de 2023 procedeu à definição dos procedimentos necessários à aplicação do nº 1 do artigo 18º-A do Decreto-Lei nº 42/2001, de 9 de fevereiro.

4. Nestes termos, os tratamentos de dados efetuados no âmbito do presente protocolo têm como fundamento de licitude o disposto na alínea c) do n.º 1 e no n.º 3 do artigo 6.º do RGPD.
5. Importa, assim, regular a partilha de dados pessoais entre o ISS, I.P., a SCML e a ACSS, I.P para efeitos de participação e execução de dívida da CPAS, o que agora se concretiza.
6. Nos termos da Cláusula 2.ª do Protocolo a comunicação eletrónica de dados entre os sistemas das entidades outorgantes é efetuada por webservices, especificamente implementados de modo a proteger o fornecimento dos dados, e por canal seguro, acordando as partes a concretização deste processo de interoperabilidade.
7. Os dados a trocar entre as partes são: Número Beneficiário da CPAS; Número Identificação Fiscal; Identificador da dívida; Período apuramento da dívida; Montante da dívida; Natureza da dívida; Indicação para exigência de juros; Data limite pagamento; Data início prescrição; Data início exigência de juros; Motivo anulação; Data anulação; Data participação; Motivos de erros; Estado da dívida; Informação de dívida prescrita; Valor pagamento de dívida e juros; Valor pagamento anulado de dívida e juros; Valor prescrição de dívida e juros; Valor anulação prescrição dívida e juros; Valor restituído de dívida e juros; Data valor de pagamento; Data valor da prescrição; Data valor de pagamento de anulação; Identificação da certidão / processo de execução fiscal; Valor a ressarcir; Motivo do pedido de ressarcimento; IBAN para onde deve ser efetuado o pagamento.
8. Os dados pessoais passíveis de tratamento são adequados, pertinentes e necessários às finalidades em causa, em obediência ao princípio da minimização de dados previsto na alínea c) do n.º 1 do artigo 5.º do RGPD.
9. Quanto às condições de comunicação eletrónica dos dados, a Cláusula 3.ª estabelece que a comunicação entre sistemas requer uma prévia autenticação entre o II, I.P. e a CPAS, mediante a atribuição de um utilizador aplicacional e de uma palavra-chave utilizados exclusivamente para comunicação eletrónica. Sobre esta vertente da autenticação cumpre fazer as seguintes recomendações: i - deve existir uma política de utilização de credenciais fortes com passwords longas, únicas, complexas e com números, símbolos, letras maiúsculas e minúsculas; ii - bloquear as contas após várias tentativas inválidas de login e iii - se viável, o uso de palavra-passe, preferencialmente em combinação com outro fator (2FA).
10. A CPAS procede ao registo de todas as consultas de informação realizadas e da informação enviada no âmbito deste protocolo. O II, I.P. procede, igualmente, aos registos de acesso e da informação enviada no âmbito deste Protocolo, nos termos da sua política de auditoria, conservando os mesmos por um período de 5 anos, findo os quais são eliminados. Ora, sobre este prazo de conservação recomenda-se a densificação da Cláusula 3.ª, com a indicação do perfil de utilizador que terá acesso a esses registos de auditoria e com a

indicação das salvaguardas para que os mesmos sejam de acesso restrito. Propõe-se ainda a inclusão da previsão de um processo de eliminação automática dos dados após o período de retenção previsto.

14. Por sua vez a Cláusula 4ª regula a participação e anulação de dívidas com origem na CPAS que será efetuada de modo automático recorrendo ao subsistema SID com vista a articular a comunicação entre ambos os sistemas. Note-se que a instauração só ocorrerá se verificadas as regras previstas no n.º 2 desta Cláusula.

15. A informação relevante relativa à dívida participada pela CPAS constará da Certidão de Dívida, cuja materialização em formato digital pode ser efetuada pelo Sistema de Informação da Segurança Social com base nos dados transmitidos eletronicamente, constando deste documento *a imagem digitalizada da assinatura do representante da entidade da proveniência da dívida* (CPAS). Note-se que este dado não consta do elenco da Cláusula 2.ª pelo que se sugere a sua inclusão.

16. Nos termos da Cláusula 13.ª da minuta de Protocolo em análise, que ora se transcreve, são responsáveis pelo tratamento de dados pessoais o IGFSS, ISSA, IP-RA, ISSM, IP-RAM e a CPAS *que determinam de forma isolada as finalidades e os meios de tratamento dos dados pessoais a que acedem no âmbito do presente Protocolo e são isoladamente responsáveis pelo cumprimento do RGPD.*

17. *A responsabilidade pelos dados pessoais tratados pelo IGFSS, ISSA, IPRA, ISSM, IP-RAM e pela CPAS é repartida considerando os seguintes momentos:*

a) *Num primeiro momento, a CPAS, enquanto responsável autónoma pelo tratamento de dados dos seus Beneficiários, irá transmitir ao IGFSS os dados pessoais indicados na Cláusula 2ª com vista a permitir a cobrança coerciva pelo IGFSS, ISSA,IPRA, ISSM, IP-RAM como determinado pelo Decreto-Lei nº 42/2001, de 9 de fevereiro, correspondendo esta transmissão, para efeitos de RGPD, uma transmissão de dados entre entidades responsáveis autónomas, a qual será feita mediante a inserção pela CPAS dos dados na plataforma e comunicada via webservices, enquanto medida técnica organizativa adotada pelas Partes para o efeito, nos termos das Cláusulas 2ª e 3ª;*
b) *num segundo momento, o IGFSS, ISSA, IPRA, ISSM, IP-RAM, cada uma enquanto responsável autónoma e isolada pelo tratamento de dados dos Beneficiários da CPAS que lhe respeitem, irá tratar os dados pessoais indicados na Cláusula 2ª com vista a assegurar a cobrança coerciva pelo IGFSS, ISSA, IPRA e ISSM, IP-RAM sendo, para este efeito, subcontratado o II.*

18. Assim, sendo cada uma destas entidades considerada responsável pelo tratamento de dados que efetua, cabe a cada uma delas o cumprimento das obrigações previstas na Cláusula 14.ª. Note-se que entre essas obrigações consta a realização das respetivas Avaliações de Impacto sobre a proteção de dados. Ora, nos termos do artigo 35.º do RGPD tais avaliações devem ser realizadas *antes do início do tratamento* por forma a

permitir a adoção de medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao risco identificado.

19. Do exposto resulta que a definição das medidas de segurança a adotar ocorrerá em momento posterior à celebração do presente Protocolo, não sendo assim possível à CNPD a pronúncia sobre a valia das mesmas.

20. Quanto à Cláusula 15.ª, relativa às obrigações do subcontratante, dispõe no seu n.º 3 que se considera «*delegada no subcontratante a escolha de subcontratantes ulteriores, sem prejuízo da disponibilização de uma lista atualizada com a identificação destes, acompanhada das condições contratuais aplicáveis e do direito de oposição*». Note-se que o n.º 2 do artigo 28.º do RGPD prevê a possibilidade de um subcontratante contratar outro subcontratante, sob autorização "específica ou geral" prévia do responsável, mas obriga o subcontratante a informar o responsável do tratamento "*de quaisquer alterações pretendidas quanto ao aumento do número ou à substituição de outros subcontratantes, dando assim ao responsável pelo tratamento a oportunidade de se opor a tais alterações*".

21. Entende-se, pois, que a redação da Cláusula 15.ª n.º 3 é demasiado genérica e permissiva, não cumprindo os requisitos legais da subcontratação previstos nos n.ºs 2 e n.º 4 do artigo 28.º do RGPD, uma vez que o subcontratante só pode proceder a ulteriores subcontratações se esses subcontratantes apresentarem as «*garantias suficientes de execução de medidas técnicas e organizativas adequadas…*». Sugere-se ainda a substituição da referência ao *direito de oposição* por possibilidade de se opor, uma vez que aquela expressão é atribuída no RGPD aos titulares dos dados, nos termos do seu artigo 21.º.

22. Por último, importa uma referência à Clausula 18.ª, relativa a medidas de segurança a adotar no âmbito do presente Protocolo, reafirmando o referido nos pontos 18 e 19 supra quanto ao facto das AIPD serem efetuadas posteriormente à celebração deste Protocolo.

23. Para além das medidas enunciadas nesta Cláusula, a CNPD relembra que nas comunicações entre o II, I.P. e os responsáveis pelo tratamento deve haver capacidade para garantir a identidade correta do remetente e destinatário da transmissão dos dados pessoais. Nomeadamente e de acordo com os requisitos técnicos da Resolução do Conselho de Ministros n.º 41/2018, recomenda-se a utilização de tecnologia de comunicação segura (por exemplo VPN), com sistema de autenticação forte (preferencialmente através de certificados), para que a transmissão de dados entre entidades de ambientes tecnológicos distintos seja efetuada em segurança.

24. Sugere-se ainda que o II, I.P. realize uma verificação periódica de que as medidas de segurança definidas estão em prática, garantindo que são eficazes e atualizando-as regularmente especialmente quando o processamento ou as circunstâncias se alteram, incluindo as que são implementadas pelos responsáveis nos tratamentos de dados.

CNPD
Comissão Nacional
de Proteção de Dados

III. Conclusão

25. Com os fundamentos acima expostos a CNPD recomenda:

a) A reformulação da Cláusula 3.ª relativamente à prévia autenticação entre o II, I.P. e a CPAS por forma a compreender uma política de utilização de credenciais fortes com passwords longas, únicas, complexas e com números, símbolos, letras maiúsculas e minúsculas; o bloqueamento das contas após várias tentativas inválidas de login e o uso de palavra-passe, preferencialmente em combinação com outro fator (2FA);

b) a densificação da Cláusula 3.ª, com a indicação do perfil de utilizador que terá acesso aos registos de auditoria e ainda a inclusão da previsão de um processo de eliminação automática dos dados após o período de retenção de 5 anos;

c) A inclusão no n.º 3 da Cláusula 15.ª de que o subcontratante só pode proceder a ulteriores subcontratações se esses subcontratantes apresentarem as garantias suficientes de execução de medidas técnicas e organizativas adequadas. Sugere-se ainda a substituição da referência ao direito de oposição por possibilidade de se opor; e

d) A inclusão na Cláusula 18.ª das medidas de segurança indicadas no ponto 23.

Lisboa, 5 de dezembro de 2023

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2023.12.05 17:20:14+00'00'
Certificado por: **Diário da República Eletrónico**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

CARTÃO DE CIDADÃO