CNPD
Comissão Nacional
de Proteção de Dados

# PARECER/2023/9

## I. Pedido

1. A Encarregada de Proteção de Dados do Instituto de Segurança Social, I.P. solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de parecer sobre a minuta do Protocolo de Colaboração para Integração de Atributos Profissionais do Instituto da Segurança Social, IP, no Sistema de Certificação de Atributos Profissionais (doravante Protocolo), celebrado entre a Agência para a Modernização Administrativa (AMA, IP), o Instituto da Segurança Social, IP (ISS, IP) e o Instituto de Informática, IP (II, IP).

2. O pedido de parecer não veio acompanhado da Avaliação de impacto sobre a proteção de dados pessoais (AIPD), que foi solicitada e entretanto remetida.

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, 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

### a. Objeto e âmbito do Protocolo

4. A Lei n.º 7/2007, de 5 de fevereiro, que estabelece o regime de emissão e utilização do cartão de cidadão prevê no artigo 18.º-A, na redação introduzida pela Lei n.º 61/2021, de 19 de agosto, a possibilidade de a assinatura eletrónica promovida através do cartão de cidadão conter a certificação de determinado atributo profissional, a pedido do seu titular (n.º 1), certificação que, nos termos do n.º 2 do mesmo artigo, é efetuada através do Sistema de Certificação de Atributos Profissionais.

5. Por sua vez, a Lei n.º 37/2014, de 26 de junho, prevê um sistema de autenticação segura nos sítios da internet, através de Chave Móvel Digital (CMD), que consiste num *"sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na Internet da Administração Pública"*, sendo a gestão e segurança da infraestrutura tecnológica que a suporta responsabilidade da AMA (cf. artigo 1.º e n.º 8 do artigo 2.º da Lei n.º 37/2014, de 26 de junho).

6. Nos termos do artigo 11.º da Portaria n.º 73/2018, de 12 de março, os trabalhadores em funções públicas e dirigentes podem livremente solicitar que seja certificado o seu atributo público para posterior assinatura com

cartão de cidadão ou chave móvel digital (n.º 1), podendo ser definidos por protocolo com a AMA outras formas de adesão aos atributos públicos (n.º 3).

7. Neste contexto, o Protocolo em análise tem por objeto proceder à "definição das regras de cooperação entre a AMA e o ISS, IP. no âmbito do projeto de implementação do Sistema de Certificação de Atributos Profissionais (SCAP) nas operações de assinatura eletrónica sobre documentos e transações digitais e autenticação eletrónica, no âmbito dos cargos e funções associadas à estrutura orgânica do ISS, IP".

### b. Responsáveis pelo tratamento de dados pessoais e subcontratante

8. Nos termos da Cláusula Segunda, são consideradas responsáveis pelo tratamento de dados pessoais, a AMA, IP e o ISS, IP. O II, IP intervém na qualidade de subcontratante.

9. De facto, nos termos do n.º 5 do artigo 18.º-A da Lei n.º 7/2007, de 5 de fevereiro, a AMA é a entidade responsável pelo procedimento de atribuição de atributos profissionais e, por conseguinte, pelo tratamento de dados que haja necessidade de fazer para cumprimento dessa finalidade.

10. O ISS intervém no presente Protocolo por ser o Instituto Público no qual exercem funções os trabalhadores cujos atributos profissionais pretende certificar-se.

11. O II, IP. intervém no presente Protocolo por ser a "pessoa coletiva pública que assegura a construção, gestão e operação de sistemas aplicacionais e de infraestruturas tecnológicas nas áreas de tecnologias de informação e comunicação dos serviços e organismos dependentes do Ministério do Trabalho, Solidariedade e Segurança Social.

12. As obrigações dos responsáveis e do subcontratante vêm indicadas nas cláusulas Sétima e Oitava, respetivamente.

13. Além das observações que, a respeito de algumas das obrigações se farão, infra, não se compreende o preceituado na alínea g) da Cláusula Oitava, quando se afirma que constitui obrigação do subcontratante "[c]umprir as regras definidas pelos Responsáveis pelo tratamento no quadro do RGPD, para proceder à transferência de dados para países terceiros ou organizações internacionais, dentro dos limites impostos pelo n.º 3 do artigo 28.º do RGPD". Ora, o número 3 do referido artigo estabelece as obrigações às quais os subcontratantes estão obrigados em todo e qualquer contexto no âmbito da relação com os responsáveis, apenas convocando as transferências internacionais como exemplo ilustrativo de uma dessas obrigações, qual seja, a documentação das instruções do responsável (alínea a) do n.º 3 do artigo 28.º), pelo que não se compreende o teor daquela alínea g).

14. De resto, o Protocolo não refere qualquer necessidade de transferência de dados para países terceiros ou organizações internacionais, nem se compreende em que medida estas são necessárias para a execução do Protocolo, pelo que aquela norma, constante na alínea g) da Cláusula Oitava do Protocolo deve ser revista, eliminando-se a referência às transferências as quais, nos termos do RGPD apenas podem ocorrer quando e se estiverem reunidos os pressupostos e nos termos dos artigos 44.º a 46.º.

15. Uma vez que existe apenas um subcontratante, sugere-se que, formalmente, a referência a subcontratante seja inscrita no singular.

### c. Dados pessoais objeto de tratamento

16. Segundo consta do Anexo I ao Protocolo, os dados a transmitir pelo ISS, IP à AMA, IP são os seguintes: nome do trabalhador, categoria ou função, designação do serviço a que pertence o trabalhador e situação perante o organismo (A- Ativo; B- Não Ativo; C – irregular).

17. Tendo em consideração esta informação e o facto de o Protocolo nada indicar a este respeito, conclui-se que a identificação do funcionário é, aparentemente, efetuada através do seu nome. Ora, esta identificação não constitui, claramente, um identificador único e livre de equívocos, pelo que se deve transmitir um identificador seguro. Do ponto de vista operacional, a omissão de um identificador seguro constitui uma fragilidade, que deve ser suprida através da consideração de que também o número de cartão de cidadão constitui um elemento a transmitir pelo ISS, IP à AMA, IP, para efeitos de identificação inequívoca do trabalhador.

### d. Fundamento de licitude

18. A utilização do CC ou da CMD por parte dos trabalhadores do ISS.IP constitui uma operação de tratamento de dados pessoais, pela qual são responsáveis o ISS.IP e a AMA, IP.

19. Ora, para que uma operação de tratamento de dados se figure lícita, tem de ser legitimada por um dos fundamentos de licitude previsto no artigo 6.º do RGPD.

20. Uma leitura atenta do artigo 6.º do RGPD permite facilmente concluir que não existe qualquer norma legal que imponha, ou possibilite, que o empregador exija aos seus trabalhadores a utilização do seu CC ou CMD como instrumentos de trabalho (cf. Lei n.º 7/2007, de 5 de fevereiro, Decreto-Lei n.º 74/2014, Lei n.º 37/2014 de 26 de junho).

21. Desde logo, também não é possível enquadrar o tratamento dos dados pessoais na necessidade de cumprimento de uma obrigação jurídica, nem no interesse legítimo do responsável por este corresponder a uma entidade pública [cf. alíneas c) e f) e parte final do n.º 1 do artigo 6.º do RGPD].

22. Por isso, e bem, prevê-se no n.º 1 da Cláusula Sexta, que «[a] adesão à assinatura eletrónica promovida através de Cartão de Cidadão ou Chave Móvel Digital estará sujeita à manifestação de vontade livre dos trabalhadores em funções públicas e dirigentes do ISS. IP, a qual será efetuada através do Sistema de Certificação de Atributos Profissionais, nos termos do artigo 18.º-A da Lei n.º 7/2007, na sua redação atual, e n.º 3 artigo 11.º da Portaria n.º 73/2018, na sua redação atual».

23. A este respeito, mantêm-se atuais as reservas manifestadas pela CNPD relativamente à utilização de mecanismos de autenticação individuais com base no CC ou CMD como instrumento para o desempenho de funções profissionais.

24. Recorda-se, a este respeito, o que foi dito a este respeito no Parecer n.º 66/2017, de 19 de dezembro, da CNPD a propósito da Portaria n.º 73/2018, de 12 de março.

25. O consentimento, para poder ser válido, depende do preenchimento de requisitos muito exigentes, que visam pautar os direitos, liberdades e garantias dos titulares de dados pessoais [cf. alínea a) do n.º 1 do artigo 6.º e alínea 11) do artigo 4.º do RGPD].

26. No caso, essa manifestação de vontade (ou consentimento) para o tratamento dos dados pessoais tem de preencher os requisitos previstos na alínea 11) do artigo 4.º do RGPD, disposição de aplicação direta no ordenamento jurídico nacional. Assim, a manifestação de vontade tem de ser: *livre, específica, informada e inequívoca*. O que implica que fique demonstrada a existência de condições de liberdade para a manifestação dessa vontade. Ora, no contexto das relações laborais, o trabalhador encontra-se numa situação de dependência que não permite, à partida, a formação livre da vontade.

27. A letra da lei é clara quando estabelece que o titular do CC só utiliza as suas funcionalidades de certificação eletrónica "[q]uando pretenda" (cf. n.º 5 do artigo 18.º da Lei n.º 7/2007, de 5 de fevereiro). Assim, para que a adesão a estes meios seja efetivamente livre, os responsáveis devem poder garantir ao trabalhador um meio alternativo que permita a autenticação do trabalhador sem utilização do seu documento pessoal de identificação civil.

28. Ora, sendo certo que a utilização do CC ou da CMD digital implica um tratamento de dados pessoais, se a lei faz depender a realização do tratamento da manifestação de vontade do respetivo titular dos dados, então têm de estar preenchidas, em concreto, as condições exigidas pelo RGPD e pelo ordenamento jurídico nacional para a manifestação dessa vontade, para que se possa ter por verificado o fundamento de licitude do tratamento de dados pessoais. Dito de outro modo, a alternativa não pode ser entre a autenticação e assinatura com ou sem atributos profissionais, através de CC ou CMD, mas entre estes meios e um meio que garanta que o trabalhador não tem de utilizar o seu CC ou a CMD.

29. Uma vez que a formação livre da vontade depende da existência de alternativa à utilização daqueles meios, porque qualquer deles supõe a utilização voluntária e livre pelos trabalhadores, se não for garantida uma alternativa à utilização daqueles meios, o tratamento de dados pessoais será ilícito.

30. Além deste aspeto, refira-se que o Protocolo é completamente omisso quanto aos termos do consentimento a prestar, não tendo sido enviado à CNPD qualquer informação sobre o modo como vai ser obtido esse consentimento, nem se é o titular quem insere todos os dados pessoais ou se estes são transmitidos pelo ISS, IP, na sequência de um pedido do titular, nem ainda quanto à informação a transmitir ao titular dos dados. Assim, no que respeita a este particular aspeto, a CNPD apenas enfatiza a necessidade de cumprir o preceituado nos artigos 13.º e 14.º consoante a informação seja obtida junto do titular ou não, respetivamente.

31. Por outro lado, sendo o tratamento de dados pessoais sustentado no consentimento, deve o titular dos dados poder revogá-lo a todo o momento, pelo que o Protocolo deve prever de que modo pode aquela revogação ser formalizada pelos titulares dos dados e qual o seguimento a dar ao seu pedido de revogação.

32. O protocolo é igualmente omisso no que respeita às obrigações dos responsáveis quanto ao exercício dos demais direitos por parte dos titulares.

33. Nomeadamente, não é indicado por que meio pode o titular dos dados exercer, nomeadamente, o direito de acesso, de retificação ou apagamento de dados, devendo haver previsão, no Protocolo, junto de quem e por que meio os exercitará.

34. Ora, o artigo 5.º do RGPD consagra os princípios que devem ser respeitados aquando do tratamento de dados pessoais. Nos termos da alínea d) do n.º 1 daquele artigo, os dados pessoais são "[e]xatos e atualizados sempre que necessário; devem ser adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são tratados, sejam apagados ou retificados sem demora». Assim, recomenda-se que o Protocolo concretize o modo como serão geridos o envio, a retificação e a eliminação dos dados, de forma a que, a cada momento, seja garantia de exatidão dos dados.

35. A este propósito se refira que as únicas normas relativas à obrigação de garantir a atualidade das informações acometem ao ISS, IP, em exclusivo, a responsabilidade de "garantir a atualidade da informação disponibilizada nos termos do disposto nas alíneas e) e f) anteriores". Porém, essas alíneas referem-se, tão só, às obrigações da AMA, IP, de "monitorizar o desenvolvimento dos trabalhos" e de "garantir existência de um período de testes, de duração não inferior a 30 dias, para a correção de anomalias e realização das alterações necessárias à plena operacionalidade do software da plataforma".

36. Assim sendo, deve o Protocolo ser densificado no sentido de concretizar de que modo é gerido o processo de envio de dados, de retificação e eliminação dos mesmos.

37. Embora o artigo 5.º da Portaria n.º 73/2018, de 12 de março, estabeleça a proibição de os utilizadores do SCAP utilizarem a autenticação e assinatura qualificada relativa a atributos profissionais, empresariais ou públicos quando já não sejam detentores do mesmo, devem prever-se mecanismos que vedem à partida essa utilização, assumindo-se que o SCPA reflete, a cada momento, a realidade atual e que os mecanismos de comunicação entre o SCAP e os organismos aderentes, no caso o ISS, IP, permitem uma atualização constante da informação, uma vez que a garantia de atualização dos dados é elemento essencial para o bom funcionamento de um sistema com as características do SCAP e que é da maior importância que se definam as responsabilidades da atualização da informação dos utilizadores, em particular das informações relativas ao cargo.

e. Prazo de conservação

38. O Protocolo é ainda vago quanto ao prazo de conservação dos dados pessoais. De facto, ali apenas se afirma que constituem obrigações dos responsáveis pelo tratamento "[d]efinir os prazos de conservação dos dados pessoais ou, quando tal não seja possível, indicar as circunstâncias que ditam o fim da conservação" [alínea d) da Cláusula Sétima).

39. Ora, encontrando-se igualmente previsto no Protocolo que os dados "são conservados pelo período estritamente necessário à prossecução da finalidade prevista no presente protocolo" (n.º 1 da Cláusula Nona) não se compreende a razão pela qual se remete para um momento ulterior a determinação de um prazo que pode ser definido desde já, porque não depende da vontade dos contraentes. Assim, deve o texto do Protocolo clarificar esta norma, explicitando o prazo, ou o acontecimento que determina o prazo de conservação e o apagamento dos mesmos.

40. O Protocolo nada diz quanto ao prazo de conservação de dados de arquivo, bem como dos *Logs* de Acesso, seja por parte do ISS, IP, por intermédio do subcontratante, II, IP, como por parte da AMA, tal como se reconhece na própria AIPD (ponto 2.2.1.3). Uma vez que o estabelecimento de medidas de segurança e de mecanismos de auditoria constitui uma obrigação dos responsáveis, o Protocolo deve ser revisto e densificado, em obediência às obrigações vertidas nos n.ºs 1 e 2 do artigo 5.º do RGPD.

41. Importa ainda salientar que faltam elementos que permitam uma pronúncia cabal por parte da CNPD em relação a determinados aspetos técnicos. Nomeadamente, não é possível a CNPD pronunciar-se sobre os aspetos que exigem a materialização dos trabalhos previstos na Cláusula Terceira do Protocolo, mas que ainda não estão implementados, como sejam as características técnicas da Plataforma de Interoperabilidade da

Administração Pública e posterior integração com SCAP; a solução tecnológica para garantir a certificação de atributos profissionais com cartão de cidadão através do SCAP ou solução tecnológica das interfaces que permitam a interligação dos dados disponibilizados pelo ISS, IP destinados a garantir a certificação de atributos profissionais com cartão de cidadão.

42. A única descrição da implementação técnica, no Protocolo, encontra-se na Cláusula Quarta e alude a boas práticas e acessos HTTPS. Nessa mesma cláusula deve acautelar-se que as comunicações entre o II, IP e a AMA, IP são realizadas através de um canal de ligação exclusivo para esta transmissão de dados, em obediência aos requisitos técnicos da Resolução do Conselho de Ministros n.º 41/2018.

## III. Conclusão

43. Com os fundamentos acima expostos a CNPD recomenda que o Protocolo seja revisto no sentido de prever:

a. a adição do número de cartão de cidadão ao elenco de dados a transmitir pelo ISS, IP à AMA, IP, para efeitos de identificação segura dos trabalhadores, para efeitos de certificação de atributo profissional;

b. a previsão do modo como os titulares dos dados podem exercer os seus direitos, incluindo a revogação do consentimento;

c. a referência ao modo como são geridos o envio, a retificação e a eliminação dos dados, de forma a que, a cada momento, seja garantida a exatidão dos dados;

d. a identificação clara dos prazos de conservação dos dados ou das situações que conduzem ao seu apagamento;

e. a previsão do prazo de conservação dos dados de arquivo e dos *logs* de acesso;

f. acautelar que as comunicações entre o II, IP e a AMA, IP são realizadas através de um canal de ligação exclusivo para a transmissão de dados.

44. Recomenda-se, ainda, que sejam garantidos aos trabalhadores meios alternativos de autenticação do trabalhador nos sistemas e assinatura digital que não exija o recurso ao Cartão de Cidadão ou à Chave Móvel Digital, por exemplo, a criação de um cartão de trabalhador.

Aprovado na reunião de 19 de janeiro de 2023

Filipa Calvão (Presidente)