

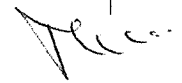
PARECER/2022/46

I. Pedido

1. A Direção-Geral de Estatísticas da Educação e Ciência (DGEEC), submeteu à Comissão Nacional de Proteção de Dados (doravante CNPD), para parecer, o Protocolo de colaboração para acesso a informação relativa à situação contributiva dos cidadãos perante a segurança social para verificação e comprovação da inexistência de dívidas, para o processamento e pagamento do "Incentivo Qualifica". São outorgantes neste Protocolo a DGEEC, a Agência Nacional para a Qualificação e o Ensino Profissional, I.P., (ANQEP, I.P.), a Agência para a Modernização Administrativa, I.P., (AMA), o Instituto da Segurança Social, I.P., (ISS) e o Instituto de Informática, I.P., (II, I.P.).
2. O pedido é acompanhado pela Avaliação de Impacto sobre a Proteção de Dados (AIPD).
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

4. O Decreto-Lei n.º 29-B/202, de 4 de maio, estabelece o modelo de governação dos fundos europeus atribuídos a Portugal através do Plano de Recuperação e Resiliência, no qual se inscreve o subinvestimento Acelerador Qualifica, sendo a ANQEP, I.P. a entidade designada para a sua execução.
5. O Acelerador Qualifica determina a atribuição de um incentivo pecuniário aos formandos que concluírem uma qualificação escolar de nível 3 ou nível 4 do Quadro Nacional de Qualificações (QNQ), ou sendo detentores do 12.º ano, a conclusão de uma qualificação profissional de nível 4 do QNQ (vide artigo 17.º da Portaria n.º 61/2022, de 31 de janeiro).
6. Para o cumprimento da atribuição do incentivo pecuniário no âmbito do "Acelerador Qualifica" torna-se necessário que a DGEEC, através do sistema SIGO, confirme que o beneficiário desse incentivo possui a sua situação tributária e contributiva regularizada.
7. O acesso a esta plataforma SIGO que se encontra livremente acessível na Internet pública, através do URL: <https://www.sigo.pt/Login.jsp>, permite verificar que o mecanismo de autenticação apresentado é de



utilizador e senha e permite várias tentativas. Por forma a evitar ataques de força-bruta e prevenir a intrusão no sistema, deveriam ser equacionados mecanismos complementares de proteção (v.g., autenticação de dois fatores (tal como referido nos alertas do EPD no documento da AIPD) ou um teste CAPTCHA).

8. O n.º 1 da Cláusula 2.ª do Protocolo estabelece que «a consulta dos dados pessoais é *efetuada em tempo real, através de comunicação eletrónica de dados entre sistemas dos outorgantes, com a utilização de "webservices" especificamente implementados de modo a proteger o fornecimento dos dados*». Deste modo, recomenda-se que todas as comunicações sejam cifradas, no protocolo HTTPS, com uso de *Transport Layer Security* (TLS), na sua versão mais recente.

9. Por sua vez, o número 3 da cláusula 2.ª do Protocolo faz referência à credenciação nos respetivos sistemas, nomeadamente a atribuição de um utilizador aplicacional e de uma palavra-chave. Na AIPD vem identificado, nos alertas do EPD, que «no caso da autenticação dos utilizadores deve ser implementada com a maior brevidade possível o mecanismo de 2FA, para os acessos a dados de um conjunto de alunos, incluindo a realização de autenticação de forma nominal por parte destes de forma a ser possível conhecer quem utilizou/acedeu os dados pessoais». Este alerta revela que o SIGO não identifica nominalmente os utilizadores e poderá haver partilha de credenciais. Transparece também que não haverá mecanismos de auditoria que permita identificar quem acedeu a que dados no sistema, ao longo da utilização.

10. Constata-se que tanto o Protocolo como a AIPD são omissos quanto à existência de uma política de gestão de credenciais e manutenção de lista atualizada de utilizadores, por parte de cada um dos outorgantes nos respetivos sistemas. Assim, a CNPD recomenda a introdução de um inciso que proceda à definição da atribuição das credenciais de acesso de forma controlada através de um processo formal de gestão do respetivo ciclo de vida, assim como a revisão de direitos de acesso de utilizadores em intervalos regulares.

11. Refira-se que o n.º 4 da Cláusula 2.ª dispõe que *a consulta de dados pessoais é efetuada através de circuito dedicado entre a DGEEC e a AMA, I.P., e entre esta última entidade e o II, IP*. A CNPD recomenda que no Protocolo conste como é feita a comunicação segura que suporta os *Web Services*, concretamente, aspetos como a configuração de uma VPN, encriptação segura dos dados e protocolos de comunicação.

12. Nos termos da Cláusula 7.ª é da exclusiva responsabilidade da DGEEC a obtenção de consentimento prévio por parte dos titulares dos dados para acesso e transmissão dos dados objeto de tratamento. O consentimento dos beneficiários está previsto através de uma declaração de autorização de consulta, nos termos previstos no artigo 4.º do Decreto-Lei n.º 114/2007, de 19 de abril. A declaração de autorização de consulta encontra-se expressamente prevista no Termo de Aceitação, que consta em anexo à Orientação



Técnica elaborada pela ANQEP, I.P. e refere a autorização da transmissão eletrónica de dados alusivos que permite à DGEEC aferir a situação de não-dívida junto da Autoridade Tributária e da Segurança Social.

13. Por sua vez, o Protocolo dispõe que são considerados responsáveis pelo tratamento dos dados pessoais o ISS, I.P., a DGEEC e a ANQEP, I.P., sendo subcontratantes o II, I.P., e a AMA, I.P. (cf. Cláusula 8.^a).

14. Da análise do Protocolo resulta que estamos perante um caso de responsabilidade conjunta, nos termos do artigo 26.º do RGPD, que pressupõe a existência de um acordo que reflita devidamente as funções e relações respetivas dos responsáveis conjuntos pelo tratamento em relação aos titulares dos dados. A CNPD sugere assim que seja alterado o conteúdo da Cláusula por forma a conter uma referência expressa à existência de um acordo entre os dois responsáveis pelo tratamento que consagre as respetivas responsabilidades pelo cumprimento do RGPD.

15. Quanto à Cláusula 11.^a, relativa a subcontratação, consagra que «Considera-se delegada no subcontratante e 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"*.

16. Entende-se, pois, que a redação da Cláusula 11.^a 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 tem um significado próprio no RGPD, correspondendo a um direito dos titulares dos dados nos termos do seu artigo 21.º.

17. Assim, recomenda-se a correção da Cláusula 11.^a e que aí sejam inseridas referências concretizadas às obrigações dos subcontratantes plasmadas nos n.ºs 2 e 4 do artigo 28.º do RGPD.

18. A Cláusula 12.^a prevê, na alínea b) do n.º 1, que compete aos subcontratantes informar os responsáveis pelo tratamento de eventuais retificações ou situações de apagamento de dados pessoais que ocorram em virtude de uma solicitação dos titulares dos dados *apresentada perante aqueles Responsáveis*. Ora, os artigos 16.º e 17.º do RGPD atribuem ao titular dos dados o direito de obter junto do responsável pelo tratamento a

retificação e o apagamento dos seus dados pessoais, cabendo ao subcontratante prestar assistência ao responsável pelo tratamento para permitir que este cumpra a sua obrigação de dar resposta aos pedidos dos titulares dos dados. Tal decorre da alínea e) do n.º 3 do artigo 28.º do RGPD e consta da alínea a) do n.º 1 da Cláusula 12.º do Protocolo, pelo que não se compreende a autonomização desta alínea.

19. Por último uma referência ao prazo de 10 anos para conservação dos dados previsto na cláusula 14.º do Protocolo. Na AIPD não é apresentada qualquer justificação para este prazo, pelo que a CNPD não está em condições de se pronunciar sobre o cumprimento do princípio da limitação da conservação previsto na alínea e) do n.º 1 do artigo 5.º do RGPD

III. Conclusão

20. Com os fundamentos acima expostos a CNPD assinala a necessidade de serem equacionados mecanismos complementares de proteção de acesso ao SIGO, bem como a alteração das disposições citadas.

21. Destaca-se, em especial, a necessidade de revisão:

- i. Da cláusula 8.ª por forma a conter uma referência expressa à existência de um acordo entre os dois responsáveis pelo tratamento que delimite as respetivas responsabilidades pelo cumprimento do RGPD;
- ii. Da cláusula 11.ª por forma a serem inseridas referências concretizadas às obrigações dos subcontratantes plasmadas nos n.ºs 2 e 4 do artigo 28.º do RGPD.

Lisboa, 31 de maio de 2022



Maria Cândida Guedes de Oliveira (Relatora)