CNPD
Comissão Nacional de Proteção de Dados

PARECER/2024/41

I. Pedido

1. O Instituto da Segurança Social, I.P., submeteu à Comissão Nacional de Proteção de Dados (CNPD), para parecer, um projeto de Acordo sobre Tratamento e Proteção de Dados Pessoais Radar Social (doravante designado por Acordo) a celebrar entre este Instituto, os Municípios e o Instituto de Informática, I.P., (II, I.P.).

2. A CNPD emite o presente parecer no âmbito das suas atribuições e competências, enquanto autoridade nacional de controlo do tratamento de dados pessoais, nos termos do disposto na alínea *c)* do n.º 1 do artigo 57.º do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016 (Regulamento Geral sobre a Proteção de Dados – 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 (a qual tem por objeto assegurar a execução, na ordem jurídica interna, do RGPD).

3. Juntamente com o pedido foi enviada uma Avaliação de Impacto sobre a Proteção de Dados (AIPD).

II. Análise do Acordo em matéria de tratamento de dados pessoais

4. O Acordo visa regular os termos e as condições de acesso e utilização por parte dos serviços do Município do sistema de informação específico disponibilizado pelo ISS, I.P., para identificação de pessoas, famílias e grupos em situação de vulnerabilidade social e/ou risco de pobreza e exclusão social, denominado por RADAR SOCIAL.

5. Os dados pessoais são tratados para as finalidades definidas na Portaria n.º 20/24, de 26 de janeiro, que estabelece as normas aplicáveis à implementação, desenvolvimento e gestão de sistema integrado de georreferenciação social. Nos termos do n.º 2 do artigo 1.º da Portaria as finalidades são: a identificação e caraterização da pessoa sinalizada no sistema de informação do sistema integrado de georreferenciação social; e o tratamento de dados necessários de suporte à gestão, à monitorização, ao acompanhamento, à prestação de contas à Comissão Europeia, aos órgãos de governação e às atividades de avaliação, auditoria e controlo.

6. . São tratados os seguintes dados: NISS, NIF, nome, sexo, data de nascimento, morada país de nacionalidade, verificação da existência de rendimentos, tipologia de rendimentos (trabalho, prestações e pensões), número de processo familiar, data do último atendimento, equipa e técnico de acompanhamento. São ainda tratados dados necessários de suporte à gestão, monotorização e acompanhamento e prestação de contas à Comissão Europeia, aos órgãos de governação e às atividades de avaliação, auditoria e controlo, nos termos da alínea b)

do n.º 2 do artigo 1.º da Portaria n.º 20/24 (código do projeto, NIF, nome, morada código do concelho, código da freguesia, designação da freguesia, código postal, localidade do código postal).

7. Os dados pessoais tratados são necessários, pertinentes e adequados às finalidades enunciadas em cumprimento ao princípio da minimização dos dados consagrado na alínea c) do n.1 do artigo 5.º do RGPD.

8. Quanto ao fundamento de licitude dos tratamentos de dados, o Acordo indica o consentimento informado dos titulares dos dados (Cláusula 4.ª e Anexo II) nos termos da alínea a) do n.º 1 dos artigos 6.º, artigo 7.º e alínea a) do n.º 2 do artigo 9.º do RGPD.

9. Quanto às condições de acesso à informação (Cláusula Quinta) o Acordo refere no ponto 4 que «o acesso aos dados requer uma prévia autenticação e só é permitida a pessoas devidamente credenciadas, que tenham assumido um compromisso de confidencialidade, mediante a atribuição de um utilizador aplicacional e de uma palavra-chave». Indica ainda o «recurso a um sistema de autenticação forte, que permita o bloqueio de contas após várias tentativas inválidas de login e a utilização de palavras-passe preferencialmente com recurso a duplo fator de autenticação». Por sua vez, no ponto 5 da cláusula Quinta surge que «o tratamento de dados pessoais, por cada Equipa, circunscreve-se à área geográfica de atuação da mesma, e efetua-se no âmbito dos serviços do Município responsáveis pela identificação de pessoas e famílias em situação de vulnerabilidade e exclusão social». No entanto não está definido se o acesso aos dados pessoais registados no sistema é permitido pela atribuição de competência geográfica e, consequentemente, se os funcionários podem aceder a dados registados por outros municípios. Relembra-se que deve ser sempre cumprido o princípio de minimização de dados, pelo que é imperativo que a equipa de um Município não consiga aceder aos dados das demais e vice-versa.

10. Note-se que no estudo de impacto, mais precisamente no quadro da página 18 sobre os controlos de acesso, é indicado que «no âmbito do presente protocolo, não é possível apreciar este controlo relativamente aos tratamentos efetuados pelas restantes entidades, nomeadamente no que respeita a postos de trabalho dos elementos dos Municípios». Concluiu-se, pois, que o Instituto de Informática, enquanto subcontratante do Instituto da Segurança Social, não assume responsabilidades sobre os controlos de acesso nos Municípios.

11. Ora, tendo em consideração que o âmbito do tratamento incide sobre categorias especiais de dados pessoais pertencentes a grupos vulneráveis entende-se que os controlos de acesso fora do controlo do Instituto de Informática deveriam ser contratualizados no acordo a celebrar com cada um dos municípios. Propõe-se, assim, que a cláusula quinta do Acordo seja alterada para que o Município, enquanto corresponsável do tratamento, fique responsabilizado por garantir controlos, no mínimo, idênticos aos do II, I.P., Segurança

Operacional, Deteção de software malicioso, Gestão de estações de trabalho, Backups, Manutenção, Controlo de acessos físicos, Prevenção de fontes de risco.

12. Quanto ao prazo de conservação dos dados é indicado o período de 10 anos nos termos da Portaria 182/2020, de 4 de agosto, que aprova o regulamento para a classificação e avaliação da informação produzida no exercício de funções pelos órgãos e entidades integradas no Ministério do Trabalho, Solidariedade e Segurança Social e da Portaria n.º 11/2023 de 27 de abril, que aprova o Regulamento para a Classificação e Avaliação da Informação Arquivística da Administração Local.

13. Nos termos da Cláusula Sétima são considerados responsáveis conjuntos pelo tratamento de dados pessoais o ISS, IP., e o Município. O II, I.P., é considerado subcontratante. As obrigações do ISS, I.P., e do Município vêm reguladas na Cláusula Oitava. No entanto esta Cláusula apenas invoca a responsabilidade pela integridade e confidencialidade dos dados e a obrigação dos responsáveis comunicarem entre si uma violação de dados pessoais. E ainda o n.º 3 desta Cláusula consagra a obrigação do Município comunicar ao ISS, I.P., a identificação de novos utilizadores do sistema de informação específico e a cessação dos utilizadores que por qualquer motivo deixem de ter legitimidade para permissão de acesso ao sistema.

14. Por razões de facilidade de leitura seria aconselhável incluir nesta Cláusula o disposto no n.º 1 da Cláusula Décima Terceira relativa à tutela dos direitos dos titulares dos dados. De facto, o n.º 1 do artigo 26.º do RGPD relativo aos responsáveis conjuntos pelo tratamento dispõe que *estes determinam, por acordo entre si e de modo transparente as respetivas responsabilidades pelo cumprimento do presente regulamento, nomeadamente no que diz respeito ao exercício dos direitos do titular dos dados e aos respetivos deveres de fornecer as informações referidas nos artigos 13.o e 14.o, ...»* .Este acordo reflete devidamente as funções e relações respetivas dos responsáveis conjuntos pelo tratamento em relação aos titulares dos dados devendo a essência do acordo ser disponibilizada ao titular dos dados.

15. Relativamente às obrigações do subcontratante previstas na Cláusula Nona recomenda -se que o Acordo refira ainda as elencadas no artigo 28.º do RGPD, nomeadamente as previstas nos n.ºs 3 e 4 deste artigo.

16. Relativamente aos meios e medidas de segurança importa antes de mais notar que consta na alínea f) dos considerandos do Acordo de tratamento e proteção de dados, a existência de um termo de aceitação pelos Municípios. Esse documento, entre outros aspetos, define na alínea j) do n.º 1 da Cláusula Sexta os termos para a utilização de um sistema de informação específico para este projeto, disponibilizado pelo ISS, IP. Não é possível avaliar completamente a utilização prevista do sistema sem ter conhecimento desse documento.

17. Quanto a medidas técnicas e de segurança refira-se que de acordo com o "Guia de Apoio Técnico à Aplicação do Radar Social", documento disponível publicamente, o acesso ao sistema se realiza através de uma ligação disponível na Internet : https://app.seg-social.pt/sso/. Este endereço é o mesmo que serve serviços como a Segurança Social Direta e está, portanto, sem restrições de acesso.

18. Ora disponibilizar uma aplicação na internet expõe-na a uma série de riscos associados ao acesso indevido e à manipulação de utilizadores. Agentes externos podem explorar vulnerabilidades na aplicação para obter acesso não autorizado a dados sensíveis. Através de técnicas de engenharia social, os atacantes podem induzir os usuários a fornecer informações confidenciais ou a realizar ações que comprometam a segurança da aplicação. Não é demais frisar que para numa aplicação disponível pela Internet, sem recurso a VPN ou circuitos dedicados, é absolutamente crucial existir uma robusta Gestão de Identidades e Acessos (IAM), para controlar o acesso aos sistemas e dados, com base em perfis e autorizações.

19. O mesmo guia de apoio técnico define que o apoio técnico de acessos e do sistema é solicitado recorrendo aos endereços de email ISS-SegurançaDados-RadarSocial@seg-social.pt e ISS-SuporteAplicacional-RadarSocial@seg-social.pt respetivamente. Sublinha-se que enviar e responder a pedidos de suporte técnico por e-mail, especialmente aqueles não solicitados, pode acarretar riscos elevados. Muitas vezes, estes e-mails são disfarçados de mensagens legítimas, com o objetivo de induzir o utilizador a clicar em links maliciosos ou a descarregar ficheiros infetados. Ao fazer isto, pode estar a expor os dados pessoais e senhas a atores mal-intencionados, para além de infetar o posto de trabalho com algum tipo de malware.

20. Assim, entende a CNPD que os canais de comunicação entre o ISS, I.P., e os Municípios, no âmbito desta plataforma, devem ser reponderados sendo de evitar o recurso ao correio eletrónico. O mecanismo de pedidos de suporte, pelo menos os relacionados com a aplicação, deveria ser integrado no sistema e disponível apenas para os utilizadores credenciados. Os pedidos deveriam ser iniciados pelos utilizadores dentro das aplicações. De igual forma, as comunicações que se pretendem enviar aos utilizadores deverão ser apresentadas dentro do sistema, logo após iniciar sessão.

21. Por fim salienta-se que o acesso a esta aplicação, contextualizada no facto de tratar categorias especiais de dados pessoais previstas no artigo 9.º do RGPD, requer salvaguardas de segurança adicionais dada a natureza sensível e confidencial desses dados. Nestes termos, considera-se insuficiente que o recurso ao segundo fator de autenticação seja facultativo. Propõe-se a sua utilização obrigatória.

22. A título de recomendações adicionais elencam-se as seguintes:

a. Seguir as melhores práticas acompanhando as melhores práticas de segurança da informação e as atualizações legislativas; e

b. Realizar testes de intrusão, de modo a simular ataques para identificar vulnerabilidades e avaliar a eficácia das medidas de segurança.

III. Conclusão

23. Nos termos e com os fundamentos expostos a CNPD recomenda:

a. A alteração da cláusula quinta do Acordo por forma a prever que o Município, enquanto corresponsável do tratamento, fique responsabilizado por garantir controlos de acesso nos Municípios;

b. A inclusão na Cláusula sétima do disposto no n.º 1 da Cláusula Décima Terceira relativa à tutela dos direitos dos titulares dos dados;

c. Que na Cláusula Nona do Acordo se refira ainda as obrigações do subcontratante elencadas no artigo 28.º do RGPD, nomeadamente as previstas nos n.ºs 3 e 4 deste artigo;

d. A reponderação dos canais de comunicação entre o ISS, I.P., e os Municípios, no âmbito desta plataforma, por forma a evitar o recurso ao correio eletrónico; e

e. A consagração no texto do Acordo que o recurso ao segundo fator de autenticação seja obrigatório.

Aprovado na sessão de 15 de outubro de 2024

Luís Barroso (Vogal que substitui a Presidente)