PARECER/2022/73

I. Pedido

1. O Instituto da Segurança Social, I.P., submeteu à Comissão Nacional de Proteção de Dados (doravante CNPD), para parecer, a minuta de Protocolo que visa definir os termos da colaboração entre os outorgantes, com vista à comunicação de dados pessoais, por via eletrónica entre o ISS, I.P., a Santa Casa de Misericórdia de Lisboa (SCML) e a Administração Central do Sistema de Saúde, I.P., (ACSS, I.P.), e as entidades competentes do Ministério da Saúde, no âmbito da Lei n.º 100/2019, de 6 de setembro, do ECI e do Decreto Regulamentar n.º 1/2022, 10 de janeiro.

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. A Lei n.º 100/2019, de 6 de setembro, que aprovou o Estatuto do Cuidador Informal, regula os direitos e os deveres do cuidador e da pessoa cuidada e estabelece as respetivas medidas de apoio.

5. Nos termos do n.º 1 do artigo 8.º deste diploma legal são desenvolvidos projetos-piloto experimentais destinados a pessoas que se enquadrem nas condições previstas no Estatuto de Cuidador Informal.

6. Os termos e condições de implementação dos referidos projetos-piloto foram, por sua vez, regulados pela Portaria n.º 64/2020, de 10 de março, tendo sido criado um programa de enquadramento e acompanhamento, bem como as medidas de apoio ao cuidador informal.

7. Para efeitos de aplicação da referida Lei, podem ser estabelecidos protocolos entre os serviços da segurança social e as entidades de diversos setores, designadamente da saúde, justiça, educação, emprego e formação profissional e forças de segurança – cfr. n.º 1 do artigo 13.º.

8. Importa, assim, regular a partilha de dados pessoais entre o ISS, I.P., a SCML e a ACSS, I.P no âmbito do apoio ao Cuidador Informal, e em particular no que respeita aos fluxos de tratamento de informação determinante para a identificação do profissional de referência de saúde (PRS), e do profissional de

referência da segurança social (PRSS), a definição do Plano de Intervenção Específico ao Cuidador (PIE) e a manutenção ou cessação do ECI e demais medidas de apoio, o que agora se concretiza.

9. Os dados que são registados e partilhados são aqueles que constam do Anexo I na proposta de Protocolo, estando feita a distinção entre os atributos que são obtidos automaticamente a partir dos sistemas de informação da Segurança Social e os atributos que são introduzidos manualmente pelos diversos intervenientes, responsáveis pelo tratamento dos dados. Os dados elencados são relativos ao processo, ao cuidador informal, às pessoas cuidadas, aos profissionais, ao Plano de Intervenção Específico, à articulação institucional e à gestão de processos.

10. 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.

11. Contudo, e acompanhando a recomendação feita na AIPD, sugere-se a delimitação do acesso aos dados por área geográfica, de forma a assegurar que os técnicos de determinada área apenas podem aceder aos processos dessa mesma área geográfica. Do mesmo modo se concorda com a necessidade de identificar no Protocolo quais as entidades que terão acesso a cada dado alvo de tratamento. Esta medida visa reforçar o cumprimento do princípio da minimização dos dados e do princípio da necessidade de conhecer (*need to know*), limitando o acesso aos dados estritamente necessários.

12. Quanto ao fundamento de licitude, a Cláusula Quarta dispõe que o tratamento de dados pessoais previsto no presente Protocolo é necessário ao exercício das atribuições públicas do ISS, IP e da SCML, no âmbito da ação social, e das atribuições públicas da ACSS, I.P. e dos demais serviços do Ministério da Saúde envolvidos no âmbito da prestação de cuidados de saúde e da gestão do sistema de saúde, nos termos previstos na Lei n.º 100/2019, de 6 de setembro, e na respetiva regulamentação. Nessa medida, o tratamento de dados efetuados no âmbito do presente protocolo tem como fundamento de licitude o disposto na alínea e) do n.º 1 e no n.º 3 do artigo 6.º do RGPD e alínea b) do n.º 2 do artigo 9.º do mesmo diploma legal.

13. No que respeita aos prazos de conservação dos dados rege a Cláusula Quinta do Protocolo. Porém, o Protocolo remete para a Circular Normativa Conjunta n.º 8/2020/ACSS/ISS quanto à definição do modelo de articulação entre as entidades e estruturas que compõem as áreas da Segurança Social e da Saúde no âmbito do Estatuto de Cuidador Informal. No ponto 10 da circular, estabelece-se que a cessação do Estatuto de Cuidador Informal determina a cessação do PIE (Plano de Intervenção Específico) ao cuidador. Na Cláusula Quinta do Protocolo, indica-se que os dados são mantidos enquanto estiverem em uso e, após a cessação do ECI, ainda ficam retidos 2 anos para efeitos de auditoria.

14. Ora, sobre este prazo de conservação recomenda-se a densificação da Cláusula Quinta com a indicação do perfil de utilizador que terá acesso aos dados quando passam de «Dados em uso» para «Dados em arquivo». Propõe-se ainda a inclusão da previsão de um processo de eliminação automática dos dados após o período de retenção previsto.

15. Nos termos da Cláusula Sexta da minuta de Protocolo em análise são responsáveis pelo tratamento de dados pessoais o ISS, I.P., a SCML, a ACSS, I.P. e os demais serviços do Ministério da Saúde que intervêm nas operações de tratamento de dados pessoais reguladas no Protocolo, sendo o II, I.P subcontratante. 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 Sexta por forma a conter uma referência expressa à existência de um acordo entre os responsáveis pelo tratamento que consagre as respetivas responsabilidades pelo cumprimento do RGPD ou, em alternativa, que essa delimitação seja aqui expressamente regulada.

16. Quanto à Cláusula Oitava, relativa às obrigações do subcontratante, consagra no n.º 2 que «Considera-se 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*".

17. Entende-se, pois, que a redação da Cláusula Oitava 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.

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

19. Constata-se que no Protocolo nada consta quanto aos direitos dos titulares dos dados, pelo que se recomenda a introdução de um inciso que expressamente os contemple e regule a forma de exercício desses direitos.

20. Os dados são registados e partilhados através da Plataforma Colaborativa de Gestão de Conteúdos, acessível na extranet da Segurança Social, cuja responsabilidade de gestão e manutenção compete ao ISS, I.P. De acordo com a Cláusula Nona do Protocolo, a solução informática que permite o acesso partilhado assenta numa infraestrutura de servidores fisicamente no centro de processamento de dados do II, I.P., e localizados na rede informática do MTSSS, sendo disponibilizada às entidades externas através da Extranet desta mesma rede.

21. Note-se que não resulta claro qual o mecanismo que esta Extranet possui para controlo de acessos na rede, pelo que se propõe a interconexão com as redes privadas do Ministério da Saúde e da SCML, através de VPN, ou, em alternativa, a implementação de um sistema de autenticação forte (preferencialmente através de certificados).

22. Por sua vez, a alínea e) da Cláusula Décima afirma que «a autenticidade da plataforma é garantida por Certificado Digital, através da encriptação de dados entre o navegador (cliente) e a plataforma (servidor) web». Salvaguarda-se que esta encriptação deve recorrer ao uso de *Transport Layer Security* (TLS), na sua versão mais recente.

23. Por último, as Cláusulas Décima Primeira e Décima Segunda do Protocolo regulam a adesão pelos serviços da Ministério da Saúde e da Santa Casa da Misericórdia de Lisboa através do fornecimento de uma lista atualizada com a identificação dos utilizadores, obrigando-se a comunicar qualquer alteração. Recomenda-se a utilização de credenciais fortes com *passwords* longas, únicas, complexas e com números, símbolos, letras maiúsculas e minúsculas, bem como a implementação de mecanismos de autenticação de duplo fator.

III. Conclusão

24. Com os fundamentos acima expostos a CNPD recomenda:

a) A alteração da Cláusula Terceira por forma a consagrar a delimitação do acesso aos dados por área geográfica, bem como identificar no Protocolo quais as entidades que terão acesso a cada dado alvo de tratamento;

b) A densificação da Cláusula Quinta com a indicação do perfil de utilizador que terá acesso aos dados quando passam de «Dados em uso» para «Dados em arquivo» e ainda a inclusão da previsão de um processo de eliminação automática dos dados após o período de retenção previsto;

c) A reformulação da Cláusula Sexta por forma a conter uma referência expressa à existência de um acordo a celebrar entre os responsáveis pelo tratamento que consagre as respetivas responsabilidades

pelo cumprimento do RGPD ou, em alternativa, que a delimitação das responsabilidades seja aqui expressamente regulada;

d) A correção do n.º 2 da Cláusula Oitava e que aí sejam inseridas referências às obrigações dos subcontratantes plasmadas nos n.ºs 2 e 4 do artigo 28.º do RGPD;

e) A introdução de um inciso que expressamente contemple os direitos dos titulares dos dados e regule a forma de exercício desses direitos; e

f) A reformulação da Cláusula Nona prevendo que a interconexão com as redes privadas do Ministério da Saúde e da SCML, ocorra através de VPN, ou, em alternativa, a implementação de um sistema de autenticação forte (preferencialmente através de certificados).

Lisboa, 10 de agosto de 2022

Maria Cândida Guedes de Oliveira (Relatora)