

PARECER/2023/3

I. Pedido

1. O Gestor Executivo da Estratégia Nacional para a Integração das Pessoas em Situação de sem-abrigo 2017-2023 (ENIPSSA) solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de parecer sobre a minuta do Protocolo de Colaboração e Gestão da Plataforma para Monitorização e Gestão dos Processos das Pessoas em Situação de sem-abrigo no âmbito da ENIPSSA 2017-2023 (doravante Protocolo).
2. O pedido de parecer veio acompanhado de quatro documentos adicionais à minuta do Protocolo, designados Protocolo de Parceria, Anexo IV - Compromisso de confidencialidade, Consentimento e Avaliação de impacto sobre a proteção de dados pessoais (AIPD).
3. Da análise dos documentos enviados pela ENIPSSA sobrevieram dúvidas e verificou-se que o documento designado Avaliação de impacto sobre a proteção de dados pessoais não consubstanciava verdadeira avaliação de riscos relacionados com a proteção de dados, antes se tratando de um parecer elaborado pelo Setor de Gestão de Risco /GAQGR do ISS, IOP, sobre a AIPD, pelo que foram solicitados esclarecimentos e o envio de documentos.
4. 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.

I. Análise

5. A Estratégia Nacional para a Integração das Pessoas em Situação de Sem-Abrigo (2017-2020), aprovada pela Resolução do Conselho de Ministros n.º 107/2017, de 29 de junho, e alterada pela Resolução de Conselho de Ministros n.º 2/202, 16 de janeiro, visa “[c]onsolidar uma abordagem estratégica e holística de prevenção e intervenção, centrada nas pessoas em situação de sem-abrigo, por forma a que ninguém tenha de permanecer na rua por ausência de alternativas” (Ponto 1 do Anexo I à Resolução de Conselho de Ministros n.º 2/202, 16 de janeiro).
6. Nos termos estabelecidos naqueles diplomas normativos, a ENIPSSA 2017-2023 assenta em três eixos estratégicos: Eixo n.º 1 – Promoção do conhecimento do fenómeno das pessoas em situação de sem-abrigo,

informação, sensibilização e educação; Eixo n.º 2 – Reforço de uma intervenção promotora da integração das pessoas em situação de sem-abrigo; Eixo n.º 3 – Coordenação, monitorização e avaliação da ENIPSSA 2017-2023.

7. O modelo de intervenção a utilizar para implementação da ENIPSSA “aplica-se a todos os casos que sejam encontrados em situação de sem-abrigo, que requeiram intervenção especializada, e durante o tempo necessário até que seja encontrada, e estabilizada, uma solução”, havendo, por conseguinte, que proceder a um diagnóstico da situação e acompanhamento dos casos de pessoas em situação de sem-abrigo (ponto 4 do Anexo I à Resolução de Conselho de Ministros n.º 2/202, 16 de janeiro), através dos órgãos e estruturas legalmente previstas.

8. São órgãos e estruturas da ENIPSSA 2017-2023 a Comissão Interministerial, o Grupo de Implementação, Monitorização e Avaliação da Estratégia (GIMAE) - composto pelas entidades de capital público e pelas entidades privadas constantes do ponto 6.3 do Anexo I à Resolução de Conselho de Ministros n.º 2/202, 16 de janeiro, e outras entidades que venham a ser convidadas -, a Comissão Consultiva e os Núcleos de Planeamento e Intervenção sem-abrigo (NPISA), estes últimos criados no âmbito dos Conselhos Locais de Ação Social (CLAS) quando a situação o justifique.

9. Ainda, integra a ENIPSSA 2017-2023 o gestor executivo que, sob orientação do membro do Governo responsável pela área do Trabalho, Solidariedade e Segurança Social, assegura a gestão e coordenação da ENIPSSA, cabendo-lhe, nomeadamente, a articulação entre os diversos órgãos e estruturas da Estratégia, bem como a coordenação do GIMAE e do núcleo executivo, bem como acompanhar, monitorizar, agilizar a prossecução dos objetivos recursos e estratégias de implementação de medidas e políticas e de intervenção para as pessoas em situação de sem-abrigo (ponto 6.2. do Anexo I à Resolução de Conselho de Ministros n.º 2/202, 16 de janeiro).

10. A Lei n.º 75-B/2020, de 31 de dezembro, que aprova o Orçamento de Estado para 2021, veio prever a interconexão de dados entre unidades, serviços e organismos públicos ou outras instituições públicas e as entidades participantes na ENIPSSA, 2017-2023, para monitorização da situação através de uma plataforma (alínea d) do n.º 1).

11. Na atrás referida lei prevê-se que a “transmissão de dados pessoais entre as referidas entidades deve ser objeto de protocolo que estabeleça as responsabilidades de cada entidade interveniente, quer no ato de transmissão quer em outros tratamentos a efetuar” (n.º 2).

12. Ainda, consagra-se no n.º 3, de forma não exaustiva, o conteúdo dos referidos protocolos, bem como se prevê que são homologados pelos membros do Governo responsáveis pelas respetivas áreas setoriais.

13. O Protocolo em análise, submetido à apreciação da CNPD pelo Diretor Executivo da ENIPSSA, é celebrado entre o Instituto de Informática, I.P., (II, I.P.) e algumas das instituições com representantes no GIMAE – Instituto da Segurança Social, I.P., (ISS, I.P.), Santa Casa da Misericórdia de Lisboa (SCML), Instituto Nacional de Estatística, I.P., (INE), Laboratório Nacional de Engenharia Civil (LNEC), Federação Nacional de Entidades de Reabilitação de Doentes Mentais (FNERDM), REDE DLBC Lisboa – Associação para o Desenvolvimento Local de Base Comunitária de Lisboa (REDE DLBC Lisboa) e European Anti Poverty Network Portugal - Rede Europeia Anti-Pobreza/Associação (EAPN Portugal).

14. 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”, no qual se integra o ENIPSSA.

II. Objecto e finalidades do tratamento

15. Constitui objeto do Protocolo “estabelecer os termos e as condições de acesso de dados entre entidades, serviços e organismos públicos ou outras instituições públicas e as entidades participantes na ENIPSSA 2017-2023 para monitorização da situação de sem-abrigo através de uma plataforma (Plataforma AidHound), tendo em vista a celebração futura de um protocolo de interconexão, conforme o previsto na alínea d) do n.º 1 e n.º 2 do artigo 356.º da Lei do Orçamento do Estado para 2021, aprovado pela Lei n.º 75-B/2020, de 31 de dezembro” (cláusula Primeira).

16. Pretende-se que, no âmbito da ENIPSSA, sejam celebrados Protocolos de Parceria (Anexo III) no âmbito da rede Social dos Conselhos Locais de Ação Social (CLAS), entre os parceiros sociais que se constituem como Núcleo de Planeamento e Intervenção Sem-Abrigo (NPISA), que têm por objeto criar e implementar o respetivo NPISA, definir compromissos a assegurar pelas entidades parceiras (cláusula 1.ª do Protocolo de Parceria).

17. Estes Protocolos de Parceria prevêem as competências dos NPISA, salientando-se, para o que ora importa, a realização do diagnóstico local sobre o fenómeno das pessoas em situação de sem-abrigo, monitorizar os processos individuais de inserção (alíneas a) do n.º 1 e c) do n.º 2 da Cláusula 4.ª).

18. Ainda, estabelece-se que a monitorização e gestão de processos das pessoas em situação de sem-abrigo é realizada, nomeadamente, através do Sistema de Informação (SaaS), o qual é utilizado por diferentes entidades locais, públicas e/ou privadas envolvidas no processo (n.º 1 da Cláusula 6.ª do Protocolo de Parceria).

19. É dito que o tratamento de dados pessoais tem como finalidade apoiar as intervenções técnicas junto das pessoas em situação de sem-abrigo que precisam de receber tratamento diferenciado, no âmbito da monitorização da situação através de uma plataforma, tal como aprovado pela Lei do Orçamento de Estado para 2021, pretendendo-se, com esta aplicação, promover uma atuação essencialmente providente e protetora da população de pessoas em situação de sem-abrigo, de forma a permitir a consolidação da abordagem estratégica de prevenção e integração prosseguida pela ENIPSSA (Cláusulas Terceira e Quarta).

III. Titulares de dados e categorias de dados

20. Os titulares dos dados são pessoas em situação de sem-abrigo no território continental, na área geográfica dos NPISA, sendo a recolha de dados realizada de forma direta, através de entrevista presencial ou contacto telefónico, com recolha de consentimento informado (n.º 4 da Cláusula Segunda).

21. De acordo com a AIPD, é efetuado um tratamento em larga escala de categorias especiais de dados, em concreto, dados de saúde¹. Os dados pessoais tratados constam do Anexo II ao Protocolo e integram as seguintes categorias: Dados de caracterização básicos (nome, data de nascimento, sexo, nacionalidade, contacto telefónico e de email), Dados de identificação (estado civil, naturalidade, números de cartão de cidadão ou bilhete de identidade, de utente do SNS, da carta de condução, caso seja cidadão estrangeiro, ainda, o número de passaporte e indicação do país emissor do mesmo, número de autorização de residência, situação no país e meio de entrada no país); Sinalização, que compreende dados que permitam aferir da situação de sem casa ou sem-abrigo, a georreferenciação do local de pernoita, os as circunstâncias que conduziram à situação de sem-abrigo e a recetividade para a intervenção; são recolhidos igualmente Dados de educação e empregabilidade, Sustentabilidade financeira, Dados de saúde física e mental, incluindo dependências; Dados relativos ao agregado familiar e sobre a existência e caracterização de Rede de suporte informal ou formal / institucional; e Outros registos acerca do utente (atividades desenvolvidas no âmbito da intervenção), referentes ao plano de intervenção, ao encaminhamento de respostas ao acompanhamento dos serviços, entre outros aspetos.

¹ Médico de família atribuído? Sim/Não; Inscrito no centro de saúde? Sim/Não; Doença grave ou crónica diagnosticada? Sim/Não; Lista de doença(s) grave(s) ou crónica(s); Doença mental diagnosticada? Lista de doença(s) mental(ais); Deficiência física diagnosticada? Lista de deficiência(s) física(s); Dependências diagnosticadas? Lista de dependência(s) diagnosticada(s); tem autonomia física? Tem autonomia psíquica? Tem autonomia intelectual?".

IV. O tratamento de dados a realizar e funcionamento do sistema

22. O Protocolo regula a utilização da Plataforma AidHound, “sistema de gestão de caso totalmente digital e online [...], que se enquadra na categoria dos SaaS e é acedido unicamente por browser”.

23. Vêm identificados na Cláusula Terceira do Protocolo e no documento da AIPD, os seguintes objetivos: “Promover a qualidade técnica da intervenção; Maior eficácia e eficiência na intervenção; Garantir qualidade das respostas e dos serviços prestados; Assegurar que ninguém é desinstitucionalizado sem que tenham sido ativadas as medidas e apoios para garantir um lugar adequado para viver, sempre que se justifique; Assegurar que ninguém tenha de permanecer na rua por mais de 24 horas; Assegurar o apoio técnico à saída de um Alojamento Temporário durante o tempo necessário; Assegurar a existência de condições que garantam a promoção de autonomia através da mobilização e contratualização de todos os recursos disponíveis de acordo com o diagnóstico de necessidade; Fomentar o aumento de soluções de alojamento para pessoas em situação de sem-abrigo; Permitir a utilização a nível nacional de um conceito único de pessoa em situação de sem-abrigo; Disponibilizar soluções de capacitação, educação, formação profissional e inserção profissional; Assegurar o acesso a medidas de proteção social; Assegurar o acesso aos cuidados de saúde; Assegurar o acesso a medidas de apoio à integração de migrantes; Garantir o funcionamento articulado dos órgãos e estruturas ENIPSSA.”

24. De acordo com a documentação enviada com o pedido, esta plataforma permitirá proceder ao registo dos dados dos utentes que consentam na intervenção, monitorizar e gerir os processos de pessoas em situação de sem-abrigo, partilhar dados com outros sistemas e transmitir dados entre as entidades, serviços e organismos públicos ou outras instituições públicas e as entidades participantes na ENIPSSA 2017-2023.

25. Ainda de acordo com essa documentação, o tratamento de dados é automatizado, sendo definidos perfis de utilizadores que limitam o acesso em função da área geográfica, abrangência ou tipo de dados. Está igualmente prevista a revisão e atualização pontual ou periódica dos acessos à plataforma.

26. Prevê-se, igualmente, a conservação de registos de auditoria (*log*). Da informação complementar facultada pelo MTSSS resulta que são registados os *log* para todas as operações (data, endereço de IP, ID de utilizador e resultado da operação), que todos os tipos de operações são objeto deste registo e que, no caso de consulta são ainda registados os parâmetros de entrada, sendo esses *log* conservados por dois anos.

27. São definidos na Cláusula Décima Segunda alguns meios e medidas de segurança que os intervenientes no protocolo deverão implementar. No entanto, à lista ali apresentada² haverá ainda que adicionar meios que permitam manter atualizados os sistemas que acedam à plataforma. Idealmente ainda, tendo em conta a natureza dos dados tratados, sugere-se que a utilização da plataforma seja realizada através de ligação dedicada ou VPN.

28. Na Cláusula Décima estabelece-se o envio de informação pseudonimizada ao INE, "por encriptação na fonte através de executável (aplicação de um *hash* com o algoritmo SHAA256) cedido pelo INE, por meio de canais de comunicação seguros, recorrendo à encriptação das comunicações (Protocolo de comunicações HTTPS), sendo utilizada, para o efeito, a *cloud* privada do INE" (n.º 3), não se encontrando, no entanto, especificada a forma como é desencadeado o envio – manual, automático –, a periodicidade, nem quem o desencadeia.

29. E, na verdade, não é clarificado que dados pessoais são objeto do processo de pseudonimização.

30. Da informação recebida parece resultar que ao afirmar-se que o *hash* é aplicado aos "identificadores referidos no anexo 2", se pretenda dizer que se aplica a todos os dados de identificação – em particular, Estado civil, Naturalidade, N.º de CC ou BI (se nacionalidade portuguesa), NIF, NISS, N.º de Utente SNS, N.º de Carta de Condução, N.º de Passaporte, País emissor de passaporte (se cidadão estrangeiro), N.º de Autorização de Residência (se cidadão estrangeiro), Ano de entrada no País (se cidadão estrangeiro), Situação no País (se cidadão estrangeiro), Meio de entrada no País – o que poderá significar que os restantes dados serão transmitidos em claro, isto é, identificados, sobrando desde logo a dúvida se os dados de caracterização básicos estão abrangidos pelo conjunto dos dados identificadores. É importante clarificar quais os dados a remeter, quais os que, destes, serão em claro, isto é, identificados, e quais serão pseudonimizados.

31. De todo o modo, alerta-se para o facto de a suposta irreversibilidade do processo de pseudonimização, que vem invocada na informação complementar transmitida à CNPD, ser facilmente infirmada, porquanto é sobejamente conhecida a forma de construção de dados como o NIF ou o NIC (BI/CC), podendo, dessa forma, chegar-se aos números a que corresponde cada *hash* e, conseqüentemente, à identificação do titular dos dados.

32. É ainda afirmado que "os dados anónimos são armazenados na mesma base de dados [que os demais], mas não estão visíveis, sendo categorizados por forma a filtrar a sua visibilidade". Ora, esta solução, que não

² a) Utilização de equipamento e ligações seguros no acesso à plataforma; b) Atribuição de perfis a utilizadores respeitando o princípio da necessidade de saber; c) Controlo sobre os utilizadores autorizados; d) Controlo ou supressão da produção de cópias ou reproduções, conservando a informação residente na plataforma; e) Garantia do encerramento das sessões na plataforma, na ausência dos utilizadores autorizados; e f) Perfis de acesso protegidos por palavra passe pessoal e intransmissível

segue as práticas recomendadas no RGPD (cf. considerando 29) para o processo de pseudonimização – e que consiste em manter “a conservação em separado das informações adicionais que permitem atribuir os dados pessoais a um titular de dados específico” – e que se aplica, por maioria de razão, a dados anonimizados, deve ser acompanhada da previsão de garantias quanto à forma de pesquisa pelas entidades legitimadas apenas a aceder a dados anonimizados, de modo a não permitir pesquisas livres que conduzam à identificação dos titulares dos dados.

33. No que respeita ao envio de dados para o INE, e de acordo com a resposta às questões colocadas pela CNPD, o ISS, I.P, a SCML e o II, I.P. poderão transmitir dados para a *cloud* privada do INE, manualmente, com uma periodicidade a definir (previsivelmente trimestral). Tratando-se de um sistema único, ao qual o perfil de administrador tem acesso total (alínea i. do ponto 3 da Cláusula Nona), não faz sentido uma remessa tripartida ao INE. Por forma a minimizar o risco, aconselha-se que a remessa ao INE parta de apenas uma das entidades.

34. Como se referiu anteriormente, no protocolo são especificamente identificados os responsáveis pelo tratamento o ISS, I.P e a SCML e Subcontratante o II, I.P.

35. Na Cláusula Décima é expresso que o LNEC, a FNERDM, a REDE DLBC e a EAPN Portugal consideram-se “responsáveis por aceder à informação anonimizada da Plataforma AidHound, através do perfil “análise estatística” concebido para o efeito, que permitirá realizar a avaliação de todo o processo, no âmbito das atividades definidas na Estratégia Nacional, em concreto no eixo de intervenção “E1.OE2 - Garantir a monitorização do fenómeno” (n.º 1) e que são consideradas “responsáveis pelo tratamento de dados pessoais apenas e na medida em que as suas responsabilidades pressuponham o tratamento desses dados” (n.º 2).

36. São ainda individualmente responsáveis por assegurar a integridade e confidencialidade de todos os dados pessoais a que acedem e que são recolhidos, no decurso das suas funções no âmbito dos Núcleos de Planeamento e Intervenção Sem Abrigo (NPISA), tal como previsto no Protocolo de constituição do NPISA e conforme a Minuta que consta do Anexo III.

37. Ora, é o próprio Protocolo a prever, no n.º 1 daquela Cláusula, que a informação a que estas entidades acedem se encontra anonimizada. Ora, ao contrário dos dados pseudonimizados, os dados anonimizados, pela sua natureza, não permitem a identificação direta ou indireta de pessoas, pelo que não são dados pessoais.

38. Esta incongruência é enfatizada pelo texto designado AIPD que acompanhou o pedido, no qual são referidos como destinatários de todos os dados, sem que sejam referidas exceções, todos os outorgantes do protocolo, de acordo com os perfis do acesso, aí se remetendo para a Cláusula Nona do Protocolo. Ora, tendo em conta que os outorgantes LNEC, FNERDM, REDE DLBC Lisboa e EAPN Portugal deverão aceder a dados



anonimizados, não se compreende como podem estas entidades ter acesso a certos dados, por exemplo nome, contactos e números de identificação.

39. Na resposta ao pedido de esclarecimento formulado pela CNPD, é dito que aquelas entidades “são considerados responsáveis por aceder à informação anonimizada da Plataforma AidHound, através do perfil “análise estatística” concebido para o efeito, que permitirá realizar a avaliação de todo o processo, no âmbito das atividades definidas na Estratégia Nacional, em concreto no eixo de intervenção “E1.OE2 - Garantir a monitorização do fenómeno”, o que não é esclarecedor. Assim, sugere-se uma clarificação do texto do protocolo, evitando confusão com a terminologia adotada pelo RGPD.

40. Estabelece-se que o LNEC, a FNERDM, a REDE DLBC e a EAPN Portugal acedam apenas a dados anonimizados, mas nada é dito quanto ao modo de anonimização o que prejudica a possibilidade de avaliação da efetividade da mesma.

V. Fundamentos de licitude

41. Nos termos da Cláusula Quarta, o tratamento de dados pessoais tem, como fundamento de licitude, “o consentimento livre, específico, informado e inequívoco do respetivo titular ou do seu representante legal” [...] nos termos do disposto na alínea a) do n.º 1 do artigo 6.º, no artigo 7.º e artigo 14.º do Regulamento Geral de Proteção de Dados”. Uma vez que alguns dos dados objeto de tratamento são dados de saúde, o consentimento que haja que prestar, a este respeito, deve ser recolhido também nos termos do n.º 2 artigo 9.º do RGPD, por essa a sede legal para o tratamento de categorias especiais de dados, nos quais se incluem, expressamente, os dados relativos à saúde (n.º 1 do artigo 9.º). Recomenda-se, por isso, que se acrescente ainda, na cláusula, a alínea a) do n.º 2 do artigo 9.º do RGPD.

42. Por outro lado, sendo explicitado no Protocolo que os dados serão recolhidos diretamente, há que ter igualmente em consideração o regime previsto no artigo 13.º do RGPD.

43. O consentimento é recolhido através de um documento designado Declaração de Consentimento Informado, cuja minuta constitui o Anexo I ao Protocolo.

44. Ora, é neste documento que aquelas informações devem ser prestadas, o que não acontece. Assim, deve o texto constante nesse documento ser alterado, no sentido de garantir aos titulares o direito à informação dos titulares, nos termos dos artigos 13.º e 14.º do RGPD.

45. Ainda, quando nesse texto se refere o consentimento do declarante para o tratamento de dados relativos ao seu agregado familiar, presume-se estar em causa informação não individualizada dos membros do agregado, sob pena de tal consentimento ser juridicamente irrelevante por não ser proferido pelo respetivo

titular dos dados pessoais. Isto porque o consentimento é sempre um ato pessoal que incide sobre os próprios dados, não podendo consentir-se no tratamento de dados de terceiro exceto nos casos em que haja lugar a representação, como no caso de pessoa maior submetida ao regime de acompanhamento (e na estrita medida do decretado pela sentença judicial), ou no caso dos menores.

46. Por outras palavras, se os dados do agregado familiar a que se refere a declaração de consentimento informado se limita à especificamente enunciada no Anexo II do Protocolo sob a designação de “dados agregado familiar”, tal informação não tem de vir destacada na declaração de consentimento, recomendando-se, até para simplificar o texto da declaração, eliminação da referência a “dados pessoais do meu agregado familiar”.

47. Deve, ainda, corrigir-se o lapso de escrita substituindo a expressão “por meios autorizados ou não”, pela expressão “por meios automatizados ou não, embora, presentemente, esta distinção seja irrelevante.

VI. Responsáveis pelo tratamento de dados

48. São indicados como responsáveis pelo tratamento de dados pessoais o ISS, IP. e a SCML e, como subcontratante, o II.IP. (Cláusula Sétima), e encontram-se especificadas as respetivas responsabilidades neste âmbito (Cláusula Oitava).

49. Invoca-se, aqui, o já referido supra, nos pontos 37 a 39, a propósito da incorreta classificação de outras entidades como responsáveis pelo tratamento.

VII. Riscos

50. O sistema AidHound usa servidores dedicados num *datacenter* em França e, para guardar ficheiros que estejam em campos ficheiros, quando utilizados em formulários ou áreas de perfil, o serviço Amazon S3, usando como região UE (Paris) eu-west-3.

51. A Amazon, porque sediada nos Estados Unidos da América (EUA), encontra-se sujeita ao cumprimento da legislação desse país.

52. Note-se que, em cumprimento do regime das transferências constante do capítulo V do RGPD, tendo em consideração a decisão do Tribunal de Justiça da União Europeia *Schrems II* e as recomendações do Comité Europeu para a Proteção de Dados de novembro de 2020, os responsáveis pelo tratamento devem, nas suas avaliações de risco ou, quando sejam obrigatórias, nas suas AIPD efetuadas ao abrigo do artigo 35.º do RGPD, avaliar se, em concreto, a operação de tratamento de dados projetada põe em causa a proteção dos dados; e,



se for o caso, adotar as medidas suplementares, de natureza técnica e/ou organizativa, necessárias para garantir a proteção adequada exigida pela legislação da União.

53. O documento de análise à AIPD afirma que não existe transferência de dados para fora da União Europeia. O mesmo se afirma na informação complementar. Nesta, acrescenta-se que a Amazon se encontra contratualmente obrigada a respeitar o RGPD e que “O AidHound guarda os ficheiros em buckets cifrados e só são decifráveis pelo próprio AidHound. Pelo que mesmo que algum dado fosse transferido para fora da UE, o que não acontece, estaria cifrado”.

54. O facto de os ficheiros a ser guardados nos serviços da Amazon serem cifrados minimiza o risco associado à utilização desse tipo de serviços. Não obstante, e por tratar-se de empresa sediada nos EUA, é necessário que os responsáveis avaliem e considerem esta questão e adotem as medidas necessárias para garantir a proteção. Assim, a CNPD chama a atenção dos responsáveis para o facto de haver transferências de dados para fora da União Europeia, ao contrário do assinalado no *item* da AIPD “Transferências: cumprimento das obrigações decorrentes da transferência de dados para fora da União Europeia”, recomendando a reponderação das condições em que tais transferências se desenvolvem.

55. No Anexo III ao Parecer AIPD n.º 01/2021 da Secretaria Geral do Ministério do Trabalho, Solidariedade e Segurança Social, de 26 de abril de 2021, é aventada a hipótese de, no futuro, ser “implementada uma API REST que permitirá aceder aos dados no AidHound por outros sistemas das organizações”, cujos requisitos e” maneira de garantir a proteção dos dados que serão transmitidos pela mesma” ainda estão a ser definidos. Tratando-se de uma alteração relevante ao tratamento em apreço, poderá justificar-se a alteração do protocolo e, conseqüentemente, nova consulta à CNPD.

VIII. Prazos de conservação dos dados

56. Prevê-se, nas Cláusula Sexta do Protocolo de Colaboração, que os dados pessoais armazenados no sistema de informação Plataforma AidHound sejam conservados até à extinção da ENIPSSA, “sem prejuízo do previsto na Portaria n.º 182/2020, de 4 de agosto”.

57. A mesma norma é prevista para a conservação dos prazos por parte dos NPSIA (n.º 2 da Cláusula Quarta). No entanto, esta obrigação seria mais bem integrada no Protocolo de Parceria a celebrar entre as entidades que constituirão cada um dos NPSIA; uma vez que, não sendo essas entidades parte do Protocolo de Colaboração, não ficarão obrigadas através deste último instrumento.

58. Já o documento da AIPD, na secção 2.2.1.3, refere diversos prazos, propondo uma cláusula de revisão periódica para eliminação dos dados em uso relativos a titulares que já não estejam a ser acompanhados. Este

documento propõe ainda que os dados em arquivo sejam conservados pelo prazo de 10 anos, fundamentando o prazo na Portaria n.º 182/2020 de 4 de agosto, na qual não foi possível encontrar referência a esta duração.

59. A pedido da CNPD, o MTSSS veio ulteriormente esclarecer que, pese embora o prazo para conservação dos dados relativos a pessoas em situação de sem-abrigo não se encontre especificamente regulado naquela Portaria, deve aplicar-se o prazo aí explicitado para a informação relativa a situações de vulnerabilidade social (Código 650.20) do anexo à Portaria, ou seja, 10 anos.

IX. Encarregado de Proteção de Dados

60. Da documentação junta ressalta que a Avaliação de Impacto foi realizada pelo “Encarregado de Proteção de Dados da Secretaria-Geral do Ministério do Trabalho, Solidariedade e Segurança Social”, com o fundamento na inexistência de EPD da ENIPSSA. No entanto, no n.º 2 da Cláusula Décima Quarta do Protocolo prevê-se que os NPISA designem um Interlocutor para as matérias de proteção de dados, o qual deve colaborar com “o Encarregado de Proteção de Dados” nas matérias nesse número indicadas. Por outro lado, na Declaração de Consentimento é indicada o endereço eletrónico do EPD da Segurança Social. Assim, convirá clarificar também no Protocolo se o EPD é, de facto, o do MTSSS.

X. Direitos dos titulares de dados

61. Os direitos dos titulares dos dados vêm previstos no n.º 3 da Cláusula Quarta do Protocolo de Colaboração, aí se explicitando os direitos de “conhecer, corrigir e, salvo quando a sua conservação seja exigida por requisitos da legislação nacional/europeia, eliminar os dados a si respeitantes, neste tratamento, bem como revogar o consentimento”.

62. No que respeita ao modo de exercício dos direitos por parte dos titulares, verifica-se uma desconformidade entre os textos da Declaração de Consentimento Informado e do clausulado do Protocolo. De facto, embora no Protocolo se encontre previsto que os titulares podem exercer os seus direitos junto do ISS, IP, através de email ou através de formulário disponível na internet (n.º 1 da Cláusula Décima Quarta), tal não ocorre com a Declaração de Consentimento Informado, que apenas indica um destes meios (o envio de requerimento através de *email*).

63. Ora, uma vez que é por via da informação constante no documento em que presta consentimento informado que o titular dos dados tem conhecimento dos seus direitos e de como os exercer, convirá que seja complementada a informação aí disponibilizada, acrescentando o meio de exercício de direitos em falta, sendo facultada cópia desse documento assinado, em conformidade com o n.º 2 do artigo 12.º e do considerando 39 do RGPD.

64. Para efeitos de garantir o exercício dos direitos por parte dos seus titulares, cada NPISA indica o seu “Interlocutor designado para as matérias de proteção de dados, que [deve] colaborar, sem demora injustificada, com o Encarregado de Proteção de Dados” para, entre outras funções, dar “resposta ao exercício de direitos, tratamento de incidentes de violação ou pedidos de esclarecimento, na sua área de competência” (n.º 2 da Cláusula Décima Quarta). A informação complementar de que os pedidos do titular de dados de caráter informativo serão respondidos pelo Gestor do ENIPSSA, com conhecimento do EPD e que a concretização de qualquer dos outros direitos será gerida diretamente pelo EPD do ISS com conhecimento do Gestor do ENIPSSA, não permite compreender qual o fluxo a utilizar aquando do exercício dos direitos por parte dos titulares, o que convirá ser previamente estabelecido.

65. Embora a Cláusula Quarta do Protocolo regule o consentimento e os direitos dos titulares, também neste aspeto se verifica uma desconformidade face aos direitos previstos na Declaração de Consentimento Informado. De facto, no Protocolo prevê-se que o titular dos dados pode a qualquer momento, [...] e salvo quando a sua conservação seja exigida por requisitos da legislação nacional/europeia, eliminar os dados a si respeitantes, neste tratamento”, o que se mostra conforme ao regime previsto no RGPD. No entanto, na informação facultada aos titulares para efeitos de prestação de consentimento – e que, por conseguinte, sustenta a sua decisão de consentir ou não consentir no tratamento dos seus dados –, afirma-se, sem qualquer condição, o seu direito de “[s]olicitar ao responsável pelo tratamento dos meus dados pessoais [...] o respetivo apagamento”.

66. Embora se compreenda que a linguagem a utilizar junto dos titulares deva ser simples, também é verdade que a informação a transmitir deve ser verdadeira e completa, de forma a permitir que o titular dos dados forme a sua vontade. Ora, quando é transmitido ao titular de dados que tem o direito de solicitar ao EPD o apagamento dos seus dados, tal formulação é passível de, com altíssima probabilidade, induzir o titular em erro e de o fazer crer que esse pedido tenha como consequência o efetivo apagamento, o que não ocorrerá necessariamente, pelo deve proceder-se à clarificação e dos direitos dos titulares no documento relativo à prestação do consentimento.

67. Sugere-se, ainda, uniformização da terminologia³ destes documentos e sua adaptação à terminologia do RGPD para maior clareza.

³ Por exemplo, na Declaração de Consentimento refere-se o direito de “retificação dos dados” e de “aceder e consultar” os seus dados, enquanto no Protocolo se prevê o direito de “corrigir” e o direito de “conhecer”, respetivamente.

XI. Dever de confidencialidade sobre os dados pessoais

68. Na Cláusula Décima Primeira do Protocolo prevê-se a que os profissionais, no momento da atribuição de acesso à plataforma, se vinculem a um compromisso de confidencialidade, cuja minuta constitui o anexo IV do Protocolo.

69. Nos termos do referido documento, os profissionais que tenham acesso a informação considerada confidencial, seja por via do acesso à plataforma AidHound ou por outro meio, conquanto seja no exercício das suas funções, obrigam-se a guardar confidencialidade sobre a informação confidencial.

70. Ali se encontra definido o que deve entender-se por “Informação Confidencial” a qual abrange os dados pessoais. Ainda, o mesmo documento estabelece que não se considera informação confidencial, entre outras, “[a] informação que se admita, por autorização expressa e escrita, poder ser divulgada a terceiros”. Ora, presume-se que essa autorização a que se alude corresponda ao consentimento do titular dos dados. Assim sendo, há que ter em consideração que pode acontecer que o consentimento do titular se cinja à transmissão a determinados terceiros, mas não outros, pelo que, nesse caso, a informação continuará a ser confidencial nesta parte.

71. Por outro lado, prevê-se a obrigação de “guardar segredo sobre os códigos de acesso ao sistema informático (user e respetiva password) que me sejam atribuídos”. É possível que se trate de uma imperfeita redação, porém, chama-se a atenção para o facto de a password não poder ser “atribuída”, antes dever ser definida pelo utilizador do sistema, por forma a garantir a segurança e a pessoalidade do acesso.

72. Ainda, sobre os obrigados recai a obrigação de “[c]omunicar às entidades responsáveis pela plataforma qualquer fuga de informação ou incidente de violação de dados pessoais no prazo máximo de 72 (setenta e duas) horas contadas do respetivo conhecimento”. Porventura, pretendeu-se fixar prazo idêntico ao previsto no n.º 1 do artigo 33.º do RGPD para o responsável pelo tratamento notificar à Autoridade Nacional, que o mesmo é dizer à CNPD, qualquer violação de dados pessoais, mas esse prazo viola o n.º 2 do artigo 33.º do RGPD, onde se prevê que o subcontratante notifique o responsável pelo tratamento sem demora injustificada. Recomenda-se, por isso, a correção do prazo indicado no Anexo IV do Protocolo

73. Também em relação às partes é regulado o dever de confidencialidade sobre toda a informação de que tenham conhecimento ao abrigo do Protocolo, ou com relação ao mesmo (n.º 1 da Cláusula Décima Quinta), estabelecendo-se que tal regime se mantém após a cessação do Protocolo (n.º 4).



XII. Conclusão

74. Com os fundamentos supra-expostos, a CNPD entende que o tratamento de dados pessoais objeto do protocolo é legítimo, sendo tratados os dados necessários e não excessivos em relação às finalidades visadas, devendo, no entanto, ter-se em consideração os seguintes aspetos.

i. No que respeita ao Protocolo, recomenda:

- a. A previsão de que o acesso ao sistema se realize através de linha dedicada, ou VPN, de forma a mitigar os riscos para os titulares dos dados;
- b. A inclusão, na lista da Cláusula Décima Segunda, da necessidade de manter atualizados os sistemas que acedam à plataforma e a existência de base distinta para os dados pseudonimizados, anonimizados e para os dados identificados;
- c. Consagração de que a remessa de dados ao INE se efetue a partir de apenas uma das entidades, ao contrário da remessa tripartida prevista, de forma a minimizar os riscos, tendo em consideração que se trata de um sistema único ao qual o perfil de administrador tem acesso total;
- d. A identificação concreta dos dados que são acedidos por cada entidade, com indicação de quais os que se encontram em branco, pseudonimizados e anonimizados;
- e. Alteração da redação da Cláusula Décima, na medida em que se refere a responsabilidades pelo tratamento de dados das entidades aí inscritas, quando se afirma que apenas acedem dados anonimizados;
- f. Sugere-se, adicionalmente, a alteração de redação do n.º 1 da Cláusula Quinta do Protocolo de Parceria, na parte relativa aos instrumentos normativos relativos à proteção de dados, por parecer assimilar a Lei n.º 58/2019, de 8 de agosto e o Regulamento Geral de Proteção de Dados, sugerindo-se que, em alternativa à atual redação, conste nos termos previstos, designadamente, o Regulamento Geral de Proteção de Dados (RGPD) e a *Lei n.º 58/2019, de 8 de agosto*.

ii. No que respeita à documentação técnica:

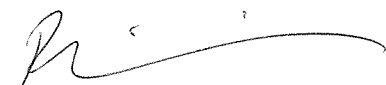
- a. Documentação das características do sistema e de informação sobre o registo de *logs*;
- b. Revisão da nomenclatura utilizada em vários locais da documentação, adaptando-a à nomenclatura do RGPD;

- c. Indicação das específicas medidas de segurança que garantam efetiva proteção de dados, tendo em consideração que o sistema AidHound usa o serviço da Amazon, tal como explicitado no ponto 56;
- d. Previsão da obrigatoriedade de adotar mecanismos para testar e avaliar a eficácia de medidas técnicas e organizativas, de modo a garantir efetiva segurança do tratamento;
- e. A previsão de acesso a dados anonimizados, deve ser acompanhada da especificação de garantias quanto à forma de pesquisa pelas entidades legitimadas para o efeito, de modo a não permitir pesquisas livres que conduzam à identificação dos titulares dos dados.
- f. Previsão de regras de gestão de utilizadores e palavras-passe ou referência para documento autónomo que as contenha.

iii. Quanto ao modelo de Declaração de Consentimento, considera a CNPD que:

- a. Através deste documento, devem transmitir-se ao titular as informações previstas nos artigos 13.º e 14.º do RGPD;
- b. Em virtude do carácter pessoal do consentimento, deve alterar-se o texto do modelo de Declaração de Consentimento, eliminando a referência à autorização do tratamento de dados pessoais do seu agregado familiar;
- c. Ainda neste documento, deve retificar-se o lapso de escrita, substituindo-se a expressão “por meios autorizados ou não”, pela expressão “por meios automatizados ou não”, embora, presentemente, esta distinção seja desnecessária;
- d. Deve ser complementada a informação disponibilizada quando ao meio através do qual podem ser exercidos os direitos, acrescentando a possibilidade de exercício através de formulário disponibilizado na internet, tal como previsto no Protocolo;
- e. Recomenda-se que seja revista a terminologia adotada no documento, adaptando-a à do RGPD e que sejam transmitidos de forma clara os direitos aos titulares, de forma a que fiquem cientes dos mesmos, nomeadamente, revendo a formulação do direito ao apagamento de dados, como explicitado acima.

Aprovado na reunião de 10 de janeiro de 2023



Filipa Calvão (Presidente)