CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2026/23

I. Pedido

1. O Instituto dos Registos e do Notariado, I.P. IRN, I.P.) solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de Parecer sobre um protocolo a celebrar entre este Instituto, a Agência para o Desenvolvimento e Coesão, I.P., (Agência, I.P.), o Instituto de Gestão Financeira e Equipamentos de Justiça, I.P. (IGFEJ, I.P.), e a Agencia para a Reforma Tecnológica do Estado, I.P., (ARTE, I.P.).

2. O Protocolo estabelece as condições de acesso por parte da Agência, I.P., à informação constante da base de dados do Registo Central de Beneficiário Efetivo (RCBE), para a finalidade exclusiva de prossecução das competências que lhe estão legalmente cometidas, nomeadamente pelo Decreto-Lei n.º 140/2013, de 18 de outubro, assim como no âmbito da coordenação dos fundos europeus estruturais e de investimento e de manutenção e desenvolvimento dos sistemas de informação do Portugal 2030 relativos à execução dos fundos, bem como a sua disponibilização, para consulta, às autoridades de gestão e aos organismos intermédios.

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.

4. O pedido é efetuado ao abrigo do disposto abrigo do n.º 3 do artigo 39.º do Regime Jurídico do RCBE, nos termos do qual «o acesso à informação para fins diversos dos estritamente previstos nos artigos 19.º a 21.º, pode ser disponibilizado nos termos e nas condições a fixar em protocolo celebrado com o IRN, I. P., o qual é sujeito a apreciação prévia da Comissão Nacional de Proteção de Dados.

II. Análise

A. As finalidades das entidades intervenientes e a sua base legal

5. Seguindo de perto os considerandos do protocolo em análise, o IRN, I.P. tem por missão executar e acompanhar as políticas relativas aos serviços de registo, tendo em vista assegurar a prestação de serviços aos cidadãos e às empresas no âmbito da identificação civil e da nacionalidade, do registo civil, predial, comercial, de bens móveis e de pessoas coletivas, colaborar com as autoridades competentes na definição e na execução das políticas de prevenção e combate ao branqueamento de capitais e ao financiamento do

terrorismo, bem como assegurar a disponibilização de informação sobre a identificação das pessoas singulares que detêm a propriedade e o controlo de pessoas coletivas e de centros de interesses coletivos sem personalidade jurídica, nos termos previstos na lei (n.º 1 e alínea n) do n.º 2 do artigo 3.º do Decreto-Lei n.º 148/2012, de 12 de julho).

6. Compete ainda ao IRN, I.P. a gestão da base de dados sobre a pessoa ou as pessoas singulares que, ainda que de forma indireta ou através de terceiro, detêm a propriedade ou o controlo efetivo das entidades sujeitas ao Registo Central de Beneficiário Efetivo (RCBE) (artigo 2.º do Regime jurídico aprovado pela Lei n.º 89/2017, de 21 de agosto, alterada pela Lei n.º 58/2020, de 31 de agosto).

7. A Agência, I.P., criada pelo Decreto-Lei n.º 140/2013, de 18 de outubro, é responsável pela coordenação da política de desenvolvimento regional e por assegurar a coordenação geral dos fundos europeus, pelo acompanhamento dos processos de programação, reprogramação e monitorização daqueles fundos em articulação com as autoridades de gestão dos programas, e pelo funcionamento de um sistema de informação relativo à sua execução, que integre os indicadores físicos e financeiros necessários à monitorização, certificação, gestão, avaliação, controlo e auditoria dos apoios concedidos.

8. Cabe à Agência, I.P. assegurar o desenvolvimento, a manutenção e o pleno funcionamento do Balcão dos Fundos, da plataforma de conceção e implementação de formulários, do Sistema de Informação dos Fundos Europeus e da Plataforma de Dados do Portugal 2030 que, nos termos das alíneas a) a d) do n.º 1 do artigo 41.º do Decreto-Lei n.º 5/2023, de 25 de janeiro, e do Decreto-Lei n.º 140/2013, na sua redação em vigor, devem permitir, não só o acesso à informação existente na Administração Pública que seja necessária à instrução dos processos de análise de candidaturas e concessão dos apoios no âmbito dos Fundos Europeus ou outros fundos, designadamente no que diz respeito à caraterização do candidato ou beneficiário, como a centralização de toda a informação necessária ao exercício das funções de gestão, coordenação, incluindo na dimensão da cooperação territorial europeia, monitorização, avaliação, certificação, pagamentos e auditoria, em conformidade com o exigido pelo Regulamento (UE) n.º 2021/1060, do Parlamento Europeu e do Conselho, de 24 de junho de 2021;

9. Nos termos do artigo 51.º do Decreto-Lei n.º 5/2023, de 25 de janeiro, compete também à Agência, I.P. desenvolver, em articulação com a autoridade de gestão do Fundo para o Asilo, a Migração e a Integração (FAMI), um sistema de informação de suporte às atividades do FAMI, o qual obedece a idênticos princípios que regem o funcionamento dos Sistemas de Informação do Portugal 2030;

10. Compete ainda à Agência, I.P., em cumprimento da referida regulamentação europeia, assegurar a proteção dos interesses financeiros da União Europeia, e que a utilização de fundos cumpra o direito da União e o direito nacional aplicáveis, em especial relativamente à prevenção, deteção e correção de fraudes, corrupção e conflitos de interesses;

11. De acordo com o Regulamento (UE) n.º 2021/1060 do Parlamento Europeu e do Conselho, de 24 de junho de 2021, os Estados-Membros encontram-se obrigados a transmitir, por via eletrónica, à Comissão Europeia, os dados referentes às operações financiadas por fundos europeus, nomeadamente os previstos no Anexo XVII do referido Regulamento, que incluem informações sobre os beneficiários efetivos dos apoios.

12. A obrigação de recolha dos dados dos beneficiários, nomeadamente informações sobre os seus beneficiários efetivos, identificados no Anexo XVII do Regulamento (UE) n.º 2021/1060 do Parlamento Europeu e do Conselho, de 24 de junho de 2021, visa, nomeadamente, permitir a análise de risco associado às entidades candidatas e beneficiárias bem como a mitigação do risco de fraude e o combate à fraude na utilização dos fundos europeus;

13. A concessão de apoios financiados pelos fundos europeus depende da verificação de um conjunto de critérios de elegibilidade dos beneficiários previstos na regulamentação geral de aplicação dos programas, entre os quais o da regularidade da sua constituição, incluindo no Registo Central de Beneficiário Efetivo, nos termos da alínea a) do n.º 1 do artigo 14.º do Decreto-Lei n.º 20-A/2023, de 22 de março.

14. O pleno funcionamento dos Sistemas de Informação do Portugal 2030, depende da existência de mecanismos de articulação entre a Agência, I.P. e as autoridades de gestão dos fundos europeus e entre estas e os organismos intermédios a quem foram confiadas funções de gestão nos termos do artigo 19.º do Decreto-Lei n.º 5/2023, de 25 de janeiro, de forma a permitir o acesso à informação existente na Administração Pública que se afigure necessária à instrução do processo de análise de candidatura, concessão e pagamento dos apoios no âmbito dos referidos fundos, onde se inclui a informação relevante residente no IRN, I.P.

15. Nos termos do artigo 37.º, n.º 1, alínea f), do Regime Jurídico do Registo Central do Beneficiário Efetivo, aprovado pela Lei n.º 89/2017, de 21 de agosto, enquanto não se verificar o cumprimento das obrigações declarativas e de retificação previstas no referido regime, é vedado às entidades a elas sujeitas beneficiar dos apoios de fundos europeus e públicos.

16. O IGFEJ, I.P. tem como missão a gestão dos recursos financeiros do Ministério da Justiça (MJ), a gestão do património afeto à área da justiça, das infraestruturas e recursos tecnológicos, bem como a proposta de conceção, a execução e a avaliação dos planos e projetos de informatização, em articulação com os demais serviços e organismos do MJ (nº 1 do artigo 3º do Decreto-Lei n.º 164/2012, de 31 de julho).

17. A ARTE, I.P. é um instituto público de regime especial integrado na administração indireta do Estado, que tem por missão promover a modernização e simplificação da Administração Pública, o desenvolvimento de serviços públicos digitais centrados no cidadão e na empresa, a integração de tecnologias emergentes e o reforço da capacitação da sociedade portuguesa para as oportunidades tecnológicas do futuro, nos termos do disposto no n.º 1 do artigo 3.º do Decreto-Lei n.º 43/2012, de 23 de fevereiro, na sua redação atual.

18. Mais será de referir que nos termos do disposto no ponto 7 da Resolução do Conselho de Ministros n.º 42/2015, de 19 de junho, a ARTE, I.P. é atualmente a entidade responsável pela operação, manutenção e evolução da Plataforma de Interoperabilidade da Administração Pública (iAP), sucedendo à anterior Agência para a Modernização Administrativa, IP (AMA, IP), nos termos do Decreto-Lei n.º 96/2025, de 21 de agosto, e do artigo 2.º do Decreto-Lei n.º 43/2012, de 23 de fevereiro, na sua redação atual.

19. A iAP é uma plataforma central cujo objetivo é dotar os serviços da Administração Pública de soluções partilhadas para a interligação dos sistemas de informação, sob a forma de serviços de interoperabilidade; destaca-se, para o presente âmbito, a disponibilização de serviços como o envio e receção de SMS, realizados através da Gateway de SMS da Administração Pública (GAP), integrando funcionalidades que permitem suportar de forma segura as comunicações eletrónicas entre os organismos públicos e os cidadãos.

B. O desenho do protocolo e questão relevantes em matéria de proteção de dados pessoais

20. Nos termos do n.º 2 da Cláusula 1ª «A informação relativa aos beneficiários efetivos constante da base de dados do RCBE, que sejam candidatos ou beneficiários de fundos destina-se, exclusivamente, à verificação dos critérios de elegibilidade dos beneficiários, referente à sua regular constituição, incluindo no Registo Central de Beneficiário Efetivo, nos termos da alínea a) do n.º 1 do artigo 14.º do Decreto-Lei n.º 20-A/2023, de 22 de março[1], bem como ao exercício das funções de gestão, coordenação, incluindo na dimensão da cooperação territorial europeia, monitorização, avaliação, certificação, pagamentos e auditoria, em conformidade com o exigido pelo Regulamento (UE) n.º 2021/1060, do Parlamento Europeu e do Conselho, de 24 de junho de 2021, e a dar resposta à obrigação de recolha dos dados dos beneficiários nos termos previstos designadamente no Anexo XVII do referido Regulamento (UE) 2021/1060, de modo a permitir a mitigação do risco de fraude e o combate à fraude na utilização dos fundos e ainda as decorrentes das alíneas a) a d) do n.º 1 do artigo 41.º, do artigo 51.º do Decreto-Lei n.º 5/2023, de 25 de janeiro, e do Decreto-Lei n.º 140/2013, de 18 de outubro.

21. O artigo 4.º do referido Regulamento (UE) n.º 2021/1060, do Parlamento Europeu e do Conselho, de 24 de junho de 2021, consagra que «Os Estados-Membros e a Comissão só são autorizados a proceder ao tratamento de dados pessoais quando tal seja necessário para o cumprimento das suas obrigações respetivas previstas no presente regulamento, nomeadamente para fins de acompanhamento, elaboração de relatórios,

[1] 1 - As entidades candidatas e os beneficiários devem reunir, desde a data da apresentação da candidatura, sem prejuízo do disposto nas alíneas b) e c), e até à data da conclusão da respetiva operação, os seguintes requisitos: a) Estar legalmente constituídos e devidamente registados, incluindo no Registo Central de Beneficiário Efetivo (RCBE) relativamente às pessoas que os controlem, quando aplicável;

comunicação, publicação, avaliação, gestão financeira, verificações e auditorias e, se for caso disso, para determinar a elegibilidade dos participantes».

22. Por sua vez, nos termos do artigo 37.º, n.º 1, alínea f), do Regime Jurídico do Registo Central do Beneficiário Efetivo, aprovado pela Lei n.º 89/2017, de 21 de agosto, enquanto não se verificar o cumprimento das obrigações declarativas e de retificação previstas no referido regime, é vedado às entidades a elas sujeitas beneficiar dos apoios de fundos europeus e públicos

23. Assim, das mencionadas disposições legais resulta a obrigação legal da Agência, I.P., tratar dados pessoais dos beneficiários efetivos que sejam candidatos ou beneficiários de fundos, encontrando-se preenchido o fundamento de licitude para o tratamento de dados pessoais, ao abrigo da alínea c) do n.º 1 do artigo 6.º, conjugado com o n.º 3, ambos do Regulamento (UE) 2016/679, do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.[2]

24. Por sua vez, o n.º 1 da cláusula 1.ª consagra que pelo presente protocolo é regulado o acesso por parte da Agência, I.P., à informação constante da base de dados do Registo Central de Beneficiário Efetivo (RCBE), para a finalidade exclusiva de prossecução das competências que lhe estão legalmente cometidas, nomeadamente pelo Decreto-Lei n.º 140/2013, de 18 de outubro, assim como no âmbito da coordenação dos fundos europeus estruturais e de investimento e de manutenção e desenvolvimento dos sistemas de informação do Portugal 2030 relativos à execução dos fundos, bem como a sua disponibilização, para consulta, às autoridades de gestão e aos organismos intermédios.

25. A informação relativa aos beneficiários efetivos constante da base de dados do RCBE, que sejam candidatos ou beneficiários de fundos destina-se, exclusivamente, à verificação dos critérios de elegibilidade dos beneficiários, referente à sua regular constituição, incluindo no Registo Central de Beneficiário Efetivo, nos termos da alínea a) do n.º 1 do artigo 14.º do Decreto-Lei n.º 20-A/2023, de 22 de março, bem como ao exercício das funções de gestão, coordenação, incluindo na dimensão da cooperação territorial europeia, monitorização, avaliação, certificação, pagamentos e auditoria, em conformidade com o exigido pelo

[2] Artigo 7.º do Decreto-Lei n.º 20-A/2023, de 22 de março« 1 - Os órgãos responsáveis pelo exercício das funções de coordenação, gestão, monitorização, avaliação, certificação, pagamentos, auditoria e comunicação, nos termos do Decreto-Lei n.º 5/2023, de 25 de janeiro, procedem ao tratamento de dados pessoais dos candidatos, beneficiários, beneficiários efetivos e subcontratados, de participantes e destinatários dos apoios, quando tal se revele necessário para as finalidades específicas associadas ao exercício das respetivas competências, para efeitos do cumprimento das obrigações decorrentes do Decreto-Lei n.º 5/2023, de 25 de janeiro, do presente decreto-lei e demais legislação conexa, designadamente o Regulamento (UE) 2021/1060, do Parlamento Europeu e do Conselho, de 24 de junho de 2021, e o Regulamento (UE) 2021/1057, do Parlamento Europeu e do Conselho, de 24 de junho de 2021.»

Regulamento (UE) n.º 2021/1060, do Parlamento Europeu e do Conselho, de 24 de junho de 2021, e a dar resposta à obrigação de recolha dos dados dos beneficiários nos termos previstos designadamente no Anexo XVII do referido Regulamento (UE) 2021/1060, de modo a permitir a mitigação do risco de fraude e o combate à fraude na utilização dos fundos e ainda as decorrentes das alíneas a) a d) do n.º 1 do artigo 41.º, do artigo 51.º do Decreto-Lei n.º 5/2023, de 25 de janeiro, e do Decreto-Lei n.º 140/2013, de 18 de outubro.

26. A pesquisa é realizada pelo número de identificação de pessoa coletiva (NIPC) e do país da entidade e são acedidos os seguintes dados pessoais do(s) beneficiário(s) efetivo: nome(s) próprio(s), apelido(s), data de nascimento e número de identificação fiscal (NIF). Tais dados são adequados, pertinentes e limitados ao que é necessário relativamente às finalidades descritas em cumprimento do princípio da minimização dos dados, plasmado na alínea c) do n.º 1 do artigo 5.º do RGPD. Note-se que estes dados correspondem aos indicados no Anexo XVII do Regulamento (UE) n.º 2021/1060, do Parlamento Europeu e do Conselho, de 24 de junho de 2021, relativo a dados a registar e armazenar eletronicamente para cada operação – artigo 72.º n.º 1 alínea e).

27. O acesso à informação é efetuado em tempo real, através de comunicação eletrónica de dados entre os sistemas dos outorgantes, com a utilização de "webservices" (API Web) especificamente implementados de modo a proteger o fornecimento dos dados.

28. O acesso aos dados requer uma prévia autenticação entre a Agência, I.P., a ARTE, I.P. e o IRN, I.P., envolvendo um utilizador aplicacional devidamente credenciado, e a emissão, pelo IRN, I.P, da respetiva API Key.

29. A disponibilização e acesso aos dados é efetuada através de circuito dedicado, implementado sobre tecnologia IP/MPLS, entre a Agencia, I.P., a Arte, I.P., o IGFEJ, I.P. e os servidores onde se encontra o serviço do IRN, I.P.

30. A Agência, I.P., procede ao registo dos utilizadores finais responsáveis pelas consultas e a quem são apresentados os dados provenientes destes "webservices". No caso de processamentos automáticos deverá a Agência, I.P. proceder ao registo com a identificação do processo que acedeu e utilizou os dados. Os registos devem conter a data, hora, minuto e segundo do acesso. Estes registos devem ser conservados pelo prazo de cinco anos, para fins de auditoria.

31. O acesso à informação e a posterior utilização da mesma é da exclusiva responsabilidade da Agência, I.P., e nos fins previstos no presente protocolo, cabendo-lhe estabelecer normas internas de segurança para o efeito, nomeadamente o registo de consumidores finais e obrigando-se a manter uma lista atualizada das

pessoas autorizadas a aceder à base de dados assim como a informação sobre a revogação dos acessos anteriormente atribuídos, efetuando uma comunicação ao IRN, I.P. desses acessos revogados e dos motivos para essa revogação.

32. A Agencia, I.P. é responsável pelo tratamento dos dados pessoais do registo dos utilizadores finais da informação prevista na alínea b) do n.º 2 da Cláusula 3.ª devendo prestar a devida informação aos titulares dos dados sobre a recolha e posterior comunicação ao IRN, I.P. dos dados supra referidos.

33. Porém, o protocolo estabelece no n.º 3 da cláusula 3.ª, que no registo dos utilizadores das consultas ficarão os seguintes dados pessoais: o nome, o número de identificação fiscal, o número de identificação civil.

35. Note-se que o n.º 3 da cláusula 3.ª dispõe que o acesso à informação e a posterior utilização da mesma, nos termos previstos na cláusula 1.ª, é da exclusiva responsabilidade da Agência, I.P., cabendo-lhe estabelecer normas internas de segurança para o efeito, nomeadamente o registo dos utilizadores finais, devendo ficar registado o nome, o NIF, número de identificação civil e a data e hora do acesso efetuado, obrigando-se a manter uma lista atualizada das pessoas autorizadas a aceder à base de dados.

36. Nenhuma justificação é dada para a solicitação do dado NIF e, com efeito, não se vislumbra a pertinência do tratamento deste dado para as finalidades indicadas.

37. De facto, o NIF constitui um número de identificação dos cidadãos para efeitos fiscais, não se compreendendo a recolha desse dado pessoal dos utilizadores, cujos acessos ao RCBE são realizados no exercício de competências legais num contexto profissional, nem a comunicação da Agência, I.P., ao IRN, I.P., do NIF dos utilizadores com acesso à base de dados do RCBE com vista à atribuição de um perfil de acesso.

38. Por conseguinte, considera a CNPD que carece de adequação e necessidade o tratamento do NIF dos utilizadores em violação do princípio da minimização dos dados, reconhecido no artigo 5.º, n.º 1, alínea c), do RGPD.

39. A Agência, I.P. deve promover a revogação do acesso quando se verifique a desnecessidade do mesmo ou quando o utilizador final responsável pelas consultas deixar de ter permissões para aceder à informação.

40. O IRN, I.P. procede ao registo de todas as consultas de informação realizadas no âmbito deste protocolo, devendo estes registos ser conservados pelo prazo de cinco anos, para fins de auditoria.

41. O IGFEJ procede, igualmente, aos registos de acesso no âmbito deste protocolo, para efeitos de auditoria, conservando esses registos pelo prazo de cinco anos.

42. A Cláusula 4ª, com a epígrafe "Preservação de dados" estabelece o princípio de que as entidades devem observar "as disposições legais vigentes em matéria de proteção de dados pessoais constantes do Regulamento (UE) 2016/679, de 27 de abril, e da Lei nº 58/2019, de 8 de agosto, designadamente: a) Respeitar a finalidade para que foi autorizado o tratamento dos dados, que deverá limitar-se ao estritamente necessário, não utilizando a informação para outros fins; b) Não transmitir a informação a terceiros, com exceção da Comissão, para as finalidades de reporte que fundamentam o acesso regulado no presente protocolo; c) Tomar as medidas de segurança necessárias à prevenção de qualquer ato que vise alterar o conteúdo da base de dados ou interferir de qualquer forma no seu bom funcionamento. 2 – É expressamente proibida qualquer forma de interconexão de dados pessoais."

43. Á Agencia, I.P., compete adotar medidas técnicas e organizativas com vista a manter a segurança dos dados contra qualquer acesso ilegal ou tratamento não autorizado e assegurar a confidencialidade da informação.

44. Devem ser efetuados testes de intrusão e avaliação de vulnerabilidades nas comunicações entre os outorgantes devendo o respetivo relatório ser arquivado por 5 anos e disponibilizado ao IRN, I.P. para efeitos de auditoria

45. Casos ocorram incidentes de segurança relativamente aos dados devem ser tomadas as medidas corretivas adequadas e oportunas para cessar esse incidente, devendo ser dado conhecimento do ocorrido no prazo máximo de 24 horas e participar a violação aos titulares dos dados e à CNPD.

46. Constata-se com agrado que o protocolo consagra que caso a Agência, I.P. recorra a subcontratante para dar execução ao protocolo, fique vinculada a garantir a segurança do tratamento, a assegurar que as pessoas envolvidas assumem compromisso de confidencialidade e a dar conhecimento ao IRN de todas as informações necessárias para demonstrar o cumprimento das obrigações previstas no RGPD, incluindo facilitar e contribuir para as auditorias ou inspeções conduzidas pelo IRN ou por outro auditor por este mandatado.

47. Porém, sublinha-se que nos termos do n.º 3 do artigo 28.º do RGPD, o tratamento em subcontratação é regulado por contrato ou outro ato normativo, sob forma escrita, ao abrigo do Direito da União ou dos Estados Membros que vincule o subcontratante ao responsável pelo tratamento, estabeleça objeto e duração do tratamento, a natureza e finalidade do tratamento, o tipo de dados pessoais e as obrigações e direitos dos responsáveis pelo tratamento. O mesmo regime se aplica caso o subcontratante contrate

outro subcontratante ulterior.

48. De entre as obrigações impostas pelo RGPD ao responsável pelo tratamento caso recorra a subcontratante, o n.º 1 do artigo 28.º do RGPD impõe que o responsável recorra apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do RGPD e assegure a defesa dos direitos dos titulares. Recomenda-se a inclusão desta obrigação na Cláusula 5.ª do Protocolo.

49. A transmissão de dados entre as aplicações informáticas de suporte ao RCBE e a aplicação informática de suporte à atividade da Agência, I.P. processa-se via iAP, que se encontra ligada por circuito IP/MPLS à infraestrutura de rede do Ministério da Justiça. A garantia da confidencialidade da informação é assegurada através de mecanismos de encriptação de tráfego por SSL/TLS e VPN IPsec.

50. A Agência, I.P solicita previamente ao IRN, IP a emissão de uma chave de identificação (API Key) para o acesso autorizado à informação do RCBE. Na solicitação deverá ser indicado o nome do utilizador responsável pela configuração do serviço e um endereço de correio eletrónico de contacto, tendo em vista a atribuição da chave de identificação (API Key) para autorização do acesso ao serviço.

51. O Protocolo é celebrado pelo período de um ano, tacitamente prorrogável por iguais períodos.

52. Dá-se nota positiva que a proposta de minuta de protocolo contempla os aspetos técnicos relevantes para o enquadramento numa política responsável de acesso e utilização de dados, nomeadamente a finalidade dos dados, o transporte dos mesmos desde a entidade responsável pelo seu processamento até ao destinatário, o suporte no acesso aos mesmo, o mecanismo de autenticação, a interligação das infraestruturas físicas e atribuição das credenciais de acesso.

53. No entanto, a CNPD recomenda a adoção de medidas adicionais, focando-se na operacionalização e no detalhe processual. Note-se que as medidas organizacionais devem centrar-se na melhoria da responsabilização, na gestão de direitos dos titulares e na supervisão contínua. Assim,

a) Quanto à gestão dos direitos dos titulares dos dados recomenda-se a elaboração de Procedimentos de Exercício de Direitos: A Agência, I.P., e o IRN, I.P., na qualidade de responsáveis pelo tratamento, devem estabelecer e documentar formalmente os procedimentos para que os titulares dos dados possam exercer os seus direitos de acesso, retificação, apagamento, limitação do tratamento e oposição, conforme previsto no RGPD. De facto, o Protocolo exige que a Agência, I.P., preste informação aos titulares dos dados sobre a recolha e comunicação dos dados do registo dos utilizadores finais. Contudo, não detalha a forma como

os titulares dos dados acedidos (os beneficiários efetivos) podem exercer os seus direitos relativamente à informação obtida do RCBE.

b) Criação e manutenção de um registo específico: os responsáveis pelo tratamento (Agência, I.P. e IRN, I.P.) devem manter um registo das atividades de tratamento detalhado, em conformidade com o artigo 30.º do RGPD, abrangendo especificamente as operações de acesso e consulta previstas no Protocolo. Embora exista a obrigação de registo de consultas para fins de auditoria (por Agência, I.P., IRN e IGFEJ), a manutenção de um registo das atividades de tratamento é uma exigência legal organizacional essencial para a demonstração da conformidade.

c) Definição de periodicidade de auditoria: o procedimento interno da Agência, I.P. para avaliação, seleção, controlo e auditoria dos subcontratantes deve incluir uma periodicidade mínima (por exemplo, anual) para a auditoria dos subcontratantes (como o IGFEJ, I.P. e a ARTE, I.P.) e de quaisquer subcontratantes ulteriores. O Protocolo já estabelece a obrigação de manutenção de um procedimento de controlo e auditoria, mas a definição de uma periodicidade garante a sua efetiva implementação e monitorização contínua.

d) Quanto à gestão de incidentes de segurança recomenda-se a elaboração de protocolo de comunicação unificado: estabelecer um fluxo de comunicação formal e testado que detalhe os procedimentos internos da Agência, I.P. e do IRN, I.P. para a notificação de violações, desde a deteção, a comunicação ao IRN (máximo 24h), a participação à CNPD e a comunicação aos titulares dos dados. O Protocolo define a obrigação de notificação, mas o estabelecimento de um procedimento unificado assegura a rapidez e a conformidade da informação fornecida, nomeadamente sobre os riscos emergentes e as medidas tomadas.

e) Relativamente à confidencialidade e formação recomenda-se a elaboração de compromisso de confidencialidade documentado, exigindo que todas as pessoas e entidades envolvidas no tratamento de dados (incluindo utilizadores finais) assinem um compromisso formal de confidencialidade específico ao Protocolo, reforçando a obrigação legal existente. O Protocolo exige que as pessoas envolvidas assumam um compromisso de confidencialidade, mas a sua formalização e arquivamento organizacionais são cruciais para a responsabilização e garantia de que a obrigação subsiste após a cessação do Protocolo.

f) No que respeita ao controlo de acessos e privilégios: definição de perfis de acesso mínimos: o acesso aos dados dos beneficiários efetivos (nome, NIF, data de nascimento) deve ser concedido apenas com base no princípio da necessidade de saber (Need-to-Know). Devem ser definidos perfis de acesso granulares (p. ex., Gestão de Candidaturas vs. Auditoria) para garantir a minimização do acesso aos dados pessoais, conforme exigido pelo RGPD.

g) Pseudonimização para fins analíticos/reporte: para o cumprimento da obrigação de reporte à Comissão Europeia e para as análises de risco, a Agência, I.P. deve implementar tecnicamente a pseudonimização dos dados pessoais sempre que os objetivos de processamento não exijam a identificação direta do titular.

h) Testes de intrusão e vulnerabilidades: definição de plano de remediação obrigatório: após a realização dos testes de intrusão e avaliação de vulnerabilidades anuais, deve ser implementado um plano técnico de remediação obrigatório, com prazos definidos (p. ex., 30 dias para vulnerabilidades críticas), a ser cumprido por Agência, I.P., IGFEJ, I.P. e ARTE, I.P. O Protocolo exige a realização dos testes e a conservação dos relatórios. A conformidade com o RGPD requer não só a identificação das falhas, mas a garantia técnica da sua correção.

i) Implementação de mecanismos de controlo de integridade: Implementação de *checksums* ou outras técnicas criptográficas nos dados transferidos, para além da encriptação de tráfego por SSL/TLS e VPN IPsec, garantindo a integridade dos dados desde o RCBE até ao sistema de informação da Agência, I.P., As entidades subscritoras devem tomar medidas de segurança para prevenir atos que visem alterar o conteúdo da base de dados. Mecanismos de integridade reforçam esta obrigação técnica.

j) Quanto à gestão de chaves de acesso implementação de rotação automática de Chaves (API Keys): além da prerrogativa do IRN, I.P. de renovar a chave de identificação, deve ser estabelecida uma política técnica de rotação obrigatória da API Key com uma periodicidade regular (p. ex., semestral), comunicando a nova chave através de canal seguro.

54. Embora o Protocolo estabeleça uma base sólida de conformidade, incluindo requisitos de autenticação (via API Key), utilização de canais seguros (iAP, IP/MPLS, SSL/TLS, VPN IPsec), regras estritas de finalidade e não transmissão, e mecanismos de auditoria exaustivos (registos de 5 anos por todas as partes) a CNPD entende que a implementação das medidas organizacionais e técnicas propostas, especialmente no que respeita à operacionalização dos direitos dos titulares dos dados e à especificação dos controlos técnicos (perfis e pseudonimização), permitirá elevar o nível de proteção, assegurando o cumprimento integral do RGPD e a salvaguarda dos direitos e liberdades dos cidadãos.

55. Conclusões

56. Considera a CNPD haver legitimidade para o acesso pela Agência, I.P., aos dados pessoais do Registo Central do Beneficiário Efetivo, nos limites e condições preconizados pelo presente protocolo, com as alterações decorrentes do presente parecer. Assim, a CNPD recomenda:

a) O não tratamento do dado NIF dos utilizadores com vista a atribuição de perfis de acesso;

b) A consagração na cláusula 5.ª do Protocolo da obrigação de o responsável recorrer apenas a subcontratantes que apresentem garantias suficientes de execução de medidas técnicas e organizativas adequadas de uma forma que o tratamento satisfaça os requisitos do RGPD e assegure a defesa dos direitos dos titulares; e

c) A adoção de medidas técnicas e organizativas supra referidas.

Aprovado na reunião de 31 de março de 2026

Paula Meira Lourenço (Presidente)

Assinado por: **PAULA CRISTINA MEIRA LOURENÇO**
Data: 2026.03.31 19:38:27+01'00'
Certificado por: **Diário da República**
Atributos certificados: **Presidente - Comissão Nacional de Proteção de Dados**

CARTÃO DE CIDADÃO