CNPD
Comissão Nacional
de Proteção de Dados

DELIBERAÇÃO/2021/1566

I. Relatório

1. Em 7 de maio de 2018, deu entrada na Comissão Nacional de Proteção de Dados (doravante "CNPD") uma participação contra a Agência para a Modernização Administrativa, I.P. (doravante "AMA"), NIPC 508184509, com sede na Rua de Santa Marta, 55, 1150-294 Lisboa.

2. Nesta participação, foi reportado que os trabalhadores da AMA, afetos ao Espaço do Cidadão da Loja do Cidadão de Braga, para atribuírem uma Chave Móvel Digital (doravante "CMD") aos cidadãos, em *back-office*, teriam que se autenticar, ou com o seu Cartão de Cidadão (doravante "CC"), ou com a sua própria CMD pessoal.

3. Em 14 de maio de 2018, a Arguida – AMA – foi notificada para se pronunciar sobre os termos da participação, no sentido de esclarecer qual o certificado digital que disponibiliza aos seus trabalhadores quando estes optem por não utilizar o seu CC, para efeitos de autenticação.

4. Por ofício datado de 21 de maio de 2018, a Arguida veio pronunciar-se sobre a referida notificação.

5. Posteriormente, em 22 de julho de 2021, a CNPD proferiu o Projeto de Deliberação n.º 18/2021.

6. Neste, ordenou à AMA, para que disponibilizasse um meio alternativo para autenticação dos seus trabalhadores que cumprisse as exigências constantes do Regulamento Geral de Proteção de Dados[1] (doravante "RGPD"), e da Lei n.º 7/2007, de 5 de fevereiro.

7. A Arguida foi notificada do teor do referido Projeto de Deliberação e convidada, querendo, a exercer o direito de audiência prévia de interessados, no prazo de 10 (dez) dias (cf. artigos 121.º e 122.º do Código de Procedimento Administrativo, doravante "CPA").

8. A Arguida apresentou a sua resposta, tendo alegado, em suma, que:

a. Analisadas as atribuições e poderes da CNPD, esta não tem competência para ordenar que a AMA proceda à emissão de certificados profissionais para os seus trabalhadores, por forma a que estes constituam uma alternativa à utilização do CC e da CMD na sua autenticação (identificação) nas plataformas eletrónicas, necessária ao exercício das suas funções;

b. A utilização do CC ou da CMD nos sistemas eletrónicos da Administração Pública decorre da lei quando esta determina o CC como um documento autêntico que contém os dados de cada cidadão

[1] 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 e que revoga a Diretiva 95/46/CE.

relevantes para a sua identificação, sendo a sua obtenção obrigatória para todos os cidadãos nacionais. Estes serão, na perspetiva da AMA, os meios mais adequados de autenticação nos sistemas eletrónicos da Administração Pública;

c. A AMA já providencia um meio de autenticação alternativo à autenticação eletrónica através do CC, sendo este a CMD. Por sua vez, a autenticação do trabalhador via CMD assenta num duplo fator de segurança e permite que o código numérico gerado para o efeito seja recebido no e-mail profissional do trabalhador, ao invés do seu telemóvel pessoal;

d. Os meios de autenticação atualmente utilizados – CC e CMD – são os mais seguros e adequados;

e. Os organismos públicos estão obrigados à otimização e desmaterialização de processos no âmbito da redução do consumo de papel;

f. Os procedimentos de autenticação teriam sempre de utilizar dados pessoais dos trabalhadores. Neste contexto, a AMA não compreende de que forma a emissão de certificados profissionais para os seus trabalhadores contribuiria para a salvaguarda do direito fundamental à proteção de dados pessoais. Esta emissão implicaria, sim, um tratamento adicional de dados pessoais e meios adicionais, o que se traduziria num inevitável aumento do risco de segurança.

II. Apreciação

9. A CNPD, enquanto autoridade nacional de controlo dos tratamentos de dados pessoais, é competente, na medida do necessário, para receber participações e para as investigar [cf. artigo 3.º da Lei n.º 58/2019, de 8 de agosto (doravante "LERGPD"), lei que executa o RGPD, cf. ainda, a alínea f) do n.º 1 do artigo 57.º do RGPD].

10. Compete, ainda, à CNPD, fiscalizar o cumprimento das disposições do RGPD e demais disposições legais relativas à proteção de dados pessoais, corrigir e sancionar o seu cumprimento (cf. n.ºs 1 e 2 do artigo 58.º do RGPD e alínea b) do n.º 1 do artigo 6.º da LERGPD).

11. Atenta a resposta apresentada pela Arguida, cumpre fazer a apreciação dos argumentos de facto e de direito ali apresentados.

Assim:

i. Sobre a competência da CNPD como autoridade de controlo nacional

12. Alega a Arguida que, analisados as atribuições e os poderes da CNPD, esta não tem competência para ordenar à AMA que proceda à emissão de certificados profissionais para os seus trabalhadores, que constituam

uma alternativa à utilização do CC ou CMD aquando da sua autenticação nas plataformas eletrónicas da Administração Pública, necessária ao exercício das suas funções.

13. Tal entendimento não tem acolhimento.

Vejamos:

14. A CNPD dispõe de poderes de investigação, de correção, consultivos e de autorização em relação aos tratamentos de dados pessoais (cf. n.ºs 1, 2 e 3 do artigo 58.º do RGPD e alínea b) do n.º 1 do artigo 6.º e n.º 2 da LERGPD).

15. Dentro dos seus poderes de correção, a CNPD dispõe da faculdade de *"[o]rdenar ao responsável pelo tratamento ou ao subcontratante que tome medidas para que as operações de tratamento cumpram as disposições do presente regulamento e, se necessário, de uma forma específica e dentro de um prazo determinado"* (cf. alínea d) do n.º 2 do artigo 58.º do RGPD).

16. Pode, ainda, impor ao responsável pelo tratamento uma limitação ou proibição, temporária ou definitiva, ao tratamento de dados pessoais (cf. alínea f) do n.º 2 do artigo 58.º do RGPD).

17. Sendo certo que a utilização de CC ou de CMD para certificação com atributos profissionais implica o tratamento de dados pessoais dos respetivos titulares, a CNPD é competente para exercer todos os poderes acima indicados.

18. No presente caso, veio a CNPD exercer um poder de correção, ordenando que o responsável pelo tratamento – *in casu*, a AMA – disponibilizasse aos seus trabalhadores um meio alternativo de autenticação no exercício das suas funções, que satisfaça as exigências do RGPD, quando o mesmo seja necessário ao exercício das funções por parte daqueles.

19. Frisa-se que as entidades públicas, como é o caso da Arguida, não são exceção, estando sujeitas aos poderes de correção da CNPD, tal como previstos no RGPD e na LERGPD (cf. n.º 3 do artigo 44.º da LERGPD).

20. Assim, não pode o argumento da Arguida, relativo à incompetência da CNPD, vingar. Sendo claro que esta pode exercer os seus poderes corretivos para ordenar ao responsável pelo tratamento a adoção de medidas para que as operações de tratamento que efetua sejam conformes ao RGPD.

ii. Sobre os argumentos da adequação do meio de autenticação utilizado e da disponibilização de um meio de autenticação alternativo

21. Alega a Arguida que a utilização do CC ou da CMD para autenticação dos trabalhadores nos sistemas eletrónicos da Administração Pública, no exercício das suas funções, é o meio mais adequado de autenticação.

22. Sustenta-se no facto de o CC representar um documento autêntico, sendo a sua obtenção obrigatória para todos os cidadãos nacionais (cf. n.º 1 do artigo 3.º e artigo 2.º da Lei 7/2007, de 5 de fevereiro).

23. Conclui, assim, serem estes os meios idóneos a garantir a autoria dos atos praticados por trabalhadores da Administração Pública.

Vejamos,

24. O CC é, efetivamente, um documento autêntico e de obtenção obrigatória para cidadãos nacionais, que tem como função provar a identidade do titular perante terceiros (cf. n.º 1 do artigo 3.º, artigo 2.º e n.º 2 do artigo 6.º da Lei 7/2007, de 5 de fevereiro).

25. A CMD consiste num "*sistema alternativo e voluntário de autenticação dos cidadãos nos portais e sítios na Internet da Administração Pública*", sendo a gestão e segurança da infraestrutura tecnológica que a suporta responsabilidade da AMA (cf. artigo 1.º e n.º 8 do artigo 2.º da Lei n.º 37/2014, de 26 de junho).

26. Já o atendimento digital assistido é "*o complemento indispensável da prestação digital de serviços públicos*" e vem regulado no Decreto-Lei n.º 74/2014, de 13 de maio.

27. Este diploma legal estabelece o "digital como regra", mas prevê um sistema de "*auxílio ao cidadão ou agente económico no acesso e interação com os portais e sítios na Internet da Administração Pública*", auxílio este "*prestado por um trabalhador de uma entidade parceira devidamente credenciada pela AMA, I. P.*" (cf. n.º 1 do artigo 6.º do Decreto-Lei n.º 74/2014, de 13 de maio).

28. Ora, se por um lado a entidade empregadora pode, num primeiro momento, solicitar a identificação pessoal dos seus trabalhadores, para se certificar da mesma e até para gerar credenciais que permitam identificar com rigor os seus trabalhadores; não pode, por outro lado, exigir que estes utilizem o seu documento de identificação pessoal como instrumento profissional, diariamente.

29. Na realidade, não existe qualquer disposição, no Decreto-Lei n.º 74/2014, de 13 de maio, que estabeleça a obrigatoriedade de utilização do CC ou da CMD para efeitos de autenticação de trabalhadores da Administração Pública, nem tampouco que defina o CC como um instrumento necessário para o exercício da atividade profissional.

30. Aliás, a letra da lei é clara quando estabelece que o titular do CC só utiliza as suas funcionalidades de certificação eletrónica "*[q]uando pretenda*" (cf. n.º 5 do artigo 18.º da Lei n.º 7/2007, de 5 de fevereiro).

31. Não obstante, é possível a certificação de atributos profissionais, empresariais e públicos através do CC e da CMD, mediante o Sistema de Certificação de Atributos Profissionais ("SCAP").

32. Ainda que isto seja verdade, note-se que, mais uma vez, esta certificação é puramente opcional, dependendo integralmente da vontade do cidadão em questão, quer seja utilizado o CC, quer seja utilizada a CMD para o efeito (cf. n.ºs 1 e n.º 3 do artigo 18.º-A da Lei n.º 7/2007, de 5 de fevereiro, e artigo 3.º-A da Lei n.º 37/2014, de 26 de junho, bem como n.º 1 do artigo 3.º da Portaria n.º 73/2018, de 12 de março).

33. No presente caso, a autenticação mediante utilização do CC ou da CMD do trabalhador não depende da sua vontade, sendo necessária ao exercício das suas funções, visto não existir qualquer meio alternativo (como veremos), que permita a autenticação do trabalhador sem recorrer aos dados constantes do seu documento pessoal de identificação.

34. Na verdade, o argumento apresentado pela AMA, segundo o qual os trabalhadores disporiam de alternativa de meios, por terem à sua disposição para o efeito de certificação com atributos profissionais o CC ou a CMD, empeça na circunstância da lei prever o caráter voluntário da utilização de ambos os meios para esse efeito (cf. supra, pontos 27, 31 e 33).

35. É bom de ver que a exigência, que a AMA faz aos seus trabalhadores para atribuírem uma CMD em *back-office*, de utilização de um dos meios, em alternativa, para certificação com atributos profissionais subverte as normas legais já citadas – máxime n.ºs 1 e n.º 3 do artigo 18.º-A da Lei n.º 7/2007, de 5 de fevereiro, e artigo 3.º-A da Lei n.º 37/2014, de 26 de junho –, na medida em que implica que os mesmos sejam obrigados a autenticarem-se com atributos profissionais com o seu CC ou com a CMD.

36. Com efeito, se a utilização de qualquer destes meios para esta finalidade (certificação com atributos profissionais) é, nos termos da lei, voluntária, a imposição da utilização de um desses meios altera a natureza voluntária que a lei manifesta e expressamente fixa.

37. Ora, sendo certo que a utilização do CC ou da CMD digital implica um tratamento de dados pessoais, se a lei faz depender a realização do tratamento da manifestação de vontade do respetivo titular dos dados, então têm de estar preenchidas em concreto as condições exigidas pelo ordenamento jurídico nacional para a manifestação dessa vontade, para que se possa ter por verificado o fundamento de licitude do tratamento de dados pessoais.

38. No caso, essa manifestação de vontade (ou consentimento) para o tratamento dos dados pessoais tem de preencher os requisitos previstos na alínea 11) do artigo 4.º do RGPD, disposição de aplicação direta no ordenamento jurídico nacional. Assim, a manifestação de vontade tem de ser: *livre, específica, informada e inequívoca*.

39. Ora, no caso concreto, não foi demonstrada a manifestação de vontade dos trabalhadores afetos ao Espaço do Cidadão da Loja do Cidadão de Braga quanto à utilização de CC ou CMD para o efeito da sua certificação com atributos profissionais; aliás, as participações que deram origem a este processo são disso demonstração.

40. Mas, sobretudo, não foi demonstrada a existência de condições de liberdade para a manifestação dessa vontade, que dependem de haver uma alternativa à utilização daqueles meios, porque qualquer deles supõe a utilização voluntária e livre pelos trabalhadores.

41. Na verdade, se não for garantida uma alternativa à utilização daqueles meios, o tratamento de dados pessoais é ilícito, como de seguida se demonstra. E, portanto, torna-se irrelevante avaliar da adequação do meio para atingir a finalidade.

iii. Sobre a ilicitude do tratamento

42. A Arguida, apesar de tal ser mencionado no Projeto de Deliberação, não se pronunciou quanto ao fundamento de licitude que utiliza para o tratamento dos dados pessoais dos seus trabalhadores quanto estes têm de proceder à autenticação mediante CC ou CMD.

43. Contudo, e para efeitos da presente Deliberação, a questão é de importância significativa, não podendo ser olvidada.

Assim:

44. Como se referiu supra, a utilização do CC ou da CMD por parte dos trabalhadores da AMA constitui uma operação de tratamento de dados pessoais, sendo a Arguida a responsável pelo tratamento (cf. n.ºs 2 e 7 do artigo 4.º do RGPD).

45. Isto porque, como é evidente, a Arguida providencia os meios e define a finalidade destas operações de tratamento, ao impô-las aos seus trabalhadores.

46. Ora, para que uma operação de tratamento de dados se figure lícita, deve ser legitimada por um fundamento de licitude, constante do artigo 6.º do RGPD.

47. Não tendo a Arguida indicado o fundamento de licitude que legitima este tratamento de dados pessoais, é relevante proceder a uma análise sucinta das possibilidades, com o objetivo de averiguar se o tratamento em causa tem por base um fundamento de licitude válido.

48. Uma leitura atenta do artigo 6.º do RGPD permite facilmente concluir que não existe qualquer norma legal que imponha, ou possibilite, que o empregador exija aos seus trabalhadores a utilização do seu CC ou CMD como

instrumentos de trabalho (cf. Lei n.º 7/2007, de 5 de fevereiro, Decreto-Lei n.º 74/2014, Lei n.º 37/2014 de 26 de junho).

49. Assim, não é possível enquadrar o tratamento dos dados pessoais na necessidade de cumprimento de uma obrigação legal nos termos da alínea c) do n.º 1 do artigo 6.º do RGPD.

50. Tão pouco se vislumbra como se poderia alegar ser a utilização do CC ou da CMD *necessária* para a satisfação de um interesse público [cf. alínea e) do n.º 1 do artigo 6.º do RGPD], nem a prossecução do interesse público poderia prevalecer, sem mais, sobre os direitos fundamentais à proteção de dados pessoais e reserva da vida privada (cf. artigos 266.º, 35.º e n.º 1 do artigo 26.º, todos da Constituição da República Portuguesa), já que o tratamento de dados pessoais em causa – a autenticação mediante CC ou CMD no exercício de certas funções profissionais, pelos trabalhadores – ainda que seja feito pelos titulares de dados, não deixa de representar um risco para os direitos, liberdades e garantias dos mesmos.

51. O fundamento de licitude que poderia ser mais plausível de fundamentar, neste particular, o tratamento de dados pessoais seria o interesse legítimo do responsável pelo tratamento [cf. alínea f) do n.º 1 do artigo 6.º do RGPD]. Acontece que é o próprio RGPD a afastar essa possibilidade, ao ditar, expressamente, que o interesse legítimo *"não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrónica"* (cf. segundo parágrafo do n.º 1 do artigo 6.º do RGPD).

52. A obtenção do consentimento do trabalhador constituiria a alternativa derradeira para fundamentar a licitude do tratamento dos dados. Mas, como se explicou supra, o consentimento, para poder ser válido, depende do preenchimento de requisitos muito exigentes, que visam pautar os direitos, liberdades e garantias dos titulares de dados pessoais [cf. alínea a) do n.º 1 do artigo 6.º do RGPD].

53. Assim, o consentimento, para ser válido, deve resultar de uma manifestação de vontade livre (cf. Considerando 32 do RGPD).

54. Ora, como já foi analisado, no presente caso, não existe a possibilidade de o consentimento resultar de qualquer manifestação de vontade livre, já que os trabalhadores se encontram condicionados pela necessidade de, para executar as suas funções profissionais, utilizarem obrigatoriamente o CC ou CMD.

55. Na verdade, o consentimento, no contexto das relações jurídico-laborais, dificilmente constitui um fundamento de licitude adequado, devido à posição contratual de desequilíbrio em que o trabalhador se encontra face ao empregador (cf. Considerando 43 do RGPD).

56. Perante este desequilíbrio, não é possível defender a existência de um consentimento livre, pois o trabalhador estará sempre condicionado pela relação laboral, tendo presente que, por regra, a subsistência do trabalhador depende do rendimento obtido com o seu trabalho.

57. O que dependeria de haver um meio alternativo que permitisse uma escolha livre do trabalhador.

58. Conclui-se, assim, que o tratamento de dados pessoais aqui em causa carece de fundamento de licitude válido.

59. Pelo que, é forçoso concluir que o tratamento de dados pessoais é ilícito.

iv. Sobre o argumento de que o projeto de deliberação da CNPD implica a utilização de meios burocráticos e menos seguros

60. Em relação ao argumento da Arguida, que defende que os organismos públicos estão obrigados à otimização e desmaterialização de processos no âmbito da redução do consumo de papel, cabe aqui referir que a CNPD não sugeriu uma alternativa burocrática, que exclui os meios digitais e tecnológicos.

61. A exigência de um meio alternativo à autenticação mediante CC ou CMD não implica uma materialização, em papel, havendo múltiplas alternativas à disposição da Arguida, inovadoras, que não implicam a utilização obrigatória dos meios de autenticação pessoais dos trabalhadores.

62. A Arguida alega que a utilização de serviços eletrónicos requer mecanismos seguros de autenticação, que atestem, com segurança, a identidade dos utilizadores.

63. Considera, neste contexto, que o CC ou a CMD são os mecanismos mais seguros para autenticação, visto que serem utilizados nos sítios eletrónicos públicos de maior adesão, bem como nos sítios de diversas entidades privadas.

64. Alega ainda que, caso não fosse utilizada a autenticação mediante CC ou CMD, o trabalhador autenticar-se-ia no sistema mediante nome de utilizador e palavra chave, que por natureza são dados transmissíveis que não garantem os níveis de segurança necessários.

65. Argumenta, também, que a CMD *"(...) assenta num duplo fator de segurança:*

a) Em primeiro lugar, um código pessoal único (de 4 a 6 dígitos) e intransmissível, escolhido pelo utilizador e que apenas ele conhece;

b) Em segundo lugar, um código numérico gerado de forma aleatória, que o utilizador recebe no seu telemóvel, ou endereço de correio eletrónico selecionado, e que é utilizado por uma única vez para a conclusão da autenticação e/ou assinatura, com apenas 5 minutos de duração".

66. A Arguida considera, ainda, que não seria satisfatório, em termos de segurança da informação, que um trabalhador pudesse aceder ao *back-office*, necessário para atribuir uma CMD, através de um mecanismo de autenticação menos seguro do que aquele que vai atribuir.

67. Finalmente, argumenta que não compreende de que forma a emissão de certificados profissionais para os seus trabalhadores contribuiria para a salvaguarda do direito fundamental à proteção de dados pessoais, pois esta implicaria um tratamento adicional de dados pessoais e meios adicionais, que se traduziriam num inevitável aumento do risco de segurança.

68. Não podem estes argumentos ter provimento.

Vejamos:

69. É verdade que a segurança da informação é um fator de extrema importância no âmbito do tratamento de dados pessoais.

70. Aliás, os dados devem ser "*tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas*" [cf. princípio da integridade e confidencialidade, disposto na alínea f) do n.º 1 do artigo 5.º do RGPD].

71. É exatamente por esta razão que o RGPD vem estabelecer obrigações, na esfera do responsável pelo tratamento, que visam garantir a segurança do tratamento.

72. O responsável pelo tratamento deve aplicar medidas técnicas e organizativas, bem como políticas, adequadas a assegurar o cumprimento do RGPD e a salvaguardar os direitos, liberdades e garantias dos titulares de dados pessoais (cf. n.º 1 do artigo 24 do RGPD).

73. As medidas adotadas devem ter em conta diversos fatores e, imperativamente, garantir um nível de segurança adequado ao risco do tratamento de dados em causa (cf. n.º 1 do artigo 32.º do RGPD).

74. É importante ter em consideração que estas medidas não podem ser implementadas de forma genérica, devendo ter em conta o tratamento de dados em causa e a relação entre o responsável pelo tratamento, o titular dos dados e a finalidade do tratamento.

75. Por estas razões, o RGPD estatui também que estas medidas devem ser aplicadas tanto no momento de definição dos meios de tratamento, como no momento do próprio tratamento (cf. n.º 1 do artigo 25.º do RGPD).

76. Isto porque deve existir proteção de dados desde a conceção e por defeito.

77. *"Desde a conceção"* ou *"by design"* significa que todo o tratamento de dados deve ser pensado, e desenhado, tendo como objetivo a salvaguarda dos direitos, liberdades e garantias dos seus titulares. Ou seja, a proteção dos dados pessoais deve ser garantida, ainda antes do próprio tratamento, aquando do seu planeamento.

78. *"Por defeito"* ou *"by default"*, por sua vez, significa que o responsável pelo tratamento deve implementar medidas que garantam, apenas, o tratamento dos dados pessoais *"(...) que forem necessários para cada finalidade especifica do tratamento"*, privilegiando a defesa dos interesses, liberdades e garantias do titular dos dados pessoais, em relação aos interesses do responsável pelo tratamento (cf. n.º 2 do artigo 25 do RGPD).

79. Não se nega que a autenticação segura é um fator crucial para a segurança da informação. Porém, não se pode conceder aos argumentos da Arguida.

80. Desde logo, existem mecanismos de autenticação capazes de garantir, pelo menos, o mesmo nível de segurança que a autenticação do trabalhador mediante CC ou CMD.

81. E que recorrem, também, ao duplo fator de autenticação.

82. Permitindo aos trabalhadores autenticar a sua identidade e realizar as suas funções, sem recorrer ao seu próprio CC ou CMD.

83. Prática, aliás, utilizada em outras profissões, onde a identidade do profissional é igualmente relevante, como médicos, advogados, forças da autoridade, forças militares, entre outras.

84. Acrescente-se que o facto de os mecanismos de autenticação, utilizados pela Arguida, serem amplamente disponibilizados para utilização pelos cidadãos em sítios eletrónicos públicos de maior adesão e sítios de diversas entidades privadas não permite deduzir, sem mais, que são os mecanismos mais seguros de autenticação.

III. Conclusão

85. Ao abrigo da alínea d) do n.º 2 do artigo 58.º do RGPD e da alínea b) do n.º 1 do artigo 6.º da LERGPD, com os fundamentos acima desenvolvidos, por manifesta falta de licitude do tratamento de dados pessoais decorrente da imposição de utilização de CC ou CMD aos trabalhadores da Agência para a Modernização Administrativa, I.P., para o efeito da sua certificação com atributos profissionais para atribuírem uma CMD em *back-office*, a CNPD ordena que a Agência para a Modernização Administrativa, I.P., disponibilize um meio alternativo para certificação dos trabalhadores quando o mesmo seja necessário ao exercício de funções por parte daqueles, no prazo de seis meses.

CNPD
Comissão Nacional
de Proteção de Dados

Aprovado na reunião de 21 de dezembro de 2021

Filipa Calvão (Presidente)

Av. D. Carlos I, 134, 1º
1200-651 Lisboa
T (+351) 213 928 400
F (+351) 213 976 832
geral@cnpd.pt
www.cnpd.pt