CNPD
Comissão Nacional
de Proteção de Dados

PARECER/2021/24

I. Pedido

1. A Direção-Geral de Estatísticas de Educação e Ciência (DGEEC) solicitou à Comissão Nacional de Proteção de Dados (CNPD) a emissão de parecer sobre o projeto de Protocolo relativo ao tratamento automatizado de dados pessoais no âmbito da transferência de dados para efeitos de PASSES DE TRANSPORTES pelo Portal de Matrículas do Ministério de Educação.

2. 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.

O Protocolo em análise visa regular a transferência de dados do Portal de Matrículas do Ministério da Educação para a TIP – Transportes Intermodais do Porto, ACE, para efeitos de emissão de passes de transporte público a todos os alunos que reúnam as condições de idade e pertençam a concelhos abrangidos pela Área Metropolitana do Porto.

3. É ainda outorgante no Protocolo a Direção Geral dos Estabelecimentos Escolares (DGEstE) enquanto entidade responsável pela verificação das colocações dos alunos nas respetivas escolas e agrupamentos através do Portal das Matrículas.

4. Os dados a transferir são comunicados através da Plataforma do Portal das Matrículas, gerida pela DGEEC, através de protocolo via *WebServices*.

5. A condição de licitude para este tratamento assentará no consentimento dos encarregados de educação ou dos alunos quando maiores de idades, que será recolhido pela DGEEC.

6. São indicadas diversas medidas de segurança com vista à proteção efetiva dos dados pessoais.

7. O prazo de conservação dos registos de consentimento é de 60 dias após a conclusão da finalidade. Os *logs* de auditoria, com os registos das consultas via *webservice* serão conservados por um período de 24 meses, conforme consta do n.º 8 da cláusula terceira.

8. Foi efetuada uma Avaliação de Impacto na Proteção de Dados (AIPD), que acompanha o pedido de Parecer. A AIPD descreve as finalidades e condições do tratamento de dados, assim como as categorias de dados envolvidas. São apresentados vários mecanismos preventivos que serão aplicados ao tratamento e que envolvem a pseudonimização dos dados, encriptação e monotorização dos acessos.

9. A apreciação da CNPD cinge-se às normas que preveem ou regulam tratamentos de dados pessoais.

II. Análise

10. O protocolo em apreço visa definir os termos da colaboração entre a DGEEC, a DGEstE e a TIS, com vista à produção de cartões Andante e emissão de passes de transporte público a todas as crianças e jovens a frequentar a escolaridade obrigatória que reúnam as condições de idade e pertençam a concelhos abrangidos pela Área Metropolitana do Porto. Para o efeito, torna-se necessária a transferência de dados pessoais do portal de matrículas para a TIP, sendo que a comunicação de dados configura um tratamento de dados pessoais, na aceção do artigo 4.º, alínea *2)*, do RGPD.

i. Condições de acesso à informação – Cláusula terceira

11. No que respeita às condições de acesso, a cláusula terceira dispõe que o mesmo *é efetuado em tempo real, através de comunicação eletrónica de dados entre sistemas das entidades outorgantes, com a utilização de webServices, especificamente implementados de modo a proteger o fornecimento de dados.* São transferidos os seguintes dados: nome, tipo do documento de identificação, data de validade do documento de identificação, data de nascimento, fotografia do aluno, morada, código postal, localidade, concelho, distrito, nível de ensino, código da unidade orgânica, nome do agrupamento, código da escola, nome da escola, escalão da ação social escolar (se beneficiário), indicador se o processo se encontra terminado, data do consentimento prévio. Atendendo aos critérios da emissão do passe escolar, legalmente previstos considera-se que os dados pessoais que serão transmitidos são os necessários e adequados para cumprir a finalidade, em obediência ao princípio da minimização dos dados, conforme alínea *c)* do n.º 1 do artigo 5.º do RGPD.,

12. O acesso aos dados requer uma autenticação prévia e só é permitido mediante a atribuição de um utilizador aplicacional e de uma palavra-chave. A comunicação da informação é efetuada através de circuito dedicado entre DGEEC e a TIP. As entidades outorgantes procedem ao registo de todas as consultas de informação realizadas neste âmbito, o que se assinala como positivo, sendo os registos conservados por dois anos para efeitos de auditoria.

ii. Consentimento prévio – Cláusula quarta

13. Cabe à DGEEC a obtenção do consentimento inequívoco do encarregado de educação ou do aluno se maior de idade, para o acesso e transmissão dos dados supra referidos, e que constitui fundamento de licitude do tratamento nos termos da alínea *a)* do n.º 1 do artigo 6.º do RGPD. O mecanismo de consentimento será implementado e disponibilizado pela DGEEC no Portal das Matrículas, sendo que o direito de retirar o consentimento poderá ser exercido até ser emitido o respetivo cartão.

14. O Decreto-Lei n.º 186/2008, de 19 de setembro, criou o passe escolar ou «passe 4_18@escola.pt» tendo a Portaria n.º 268-A/2012, de 31 de agosto, alterado as condições de atribuição do passe escolar previstas na Portaria n.º 138/2009, de 3 de fevereiro, alterada pelas Portarias n.º 982-A/2009, de 2 de setembro, e 34-A/2012, de 1 de fevereiro, Portaria 249-A/2018, de 6 de setembro, e 353/2019, de 7 de outubro. Por sua vez, o Decreto-Lei n.º 21/2019, de 30 de janeiro, na sua redação atual, veio concretizar o quadro de transferência de competências para os órgãos municipais e para as entidades intermunicipais no domínio do planeamento da oferta de serviço público de transporte escolar[1]. No entanto, estas disposições legais limitam-se a prever como pressupostos de atribuição do passe4-18@escola.pt as condições que os alunos têm de preencher, cuja prova se pretende agora agilizar.

15. Assim, e na ausência de uma lei que expressamente determine as formas de agilização da prova e da verificação do preenchimento dos pressupostos legais no caso concreto para atribuição e manutenção de passe escolar, apenas o consentimento dos encarregados de educação ou dos titulares dos dados se forem maiores, legitima este tratamento de dados pessoais.

16. Por sua vez, o n.º 5 da Cláusula quarta prevê que, *em caso de necessidade de alteração do consentimento de acordo com a vontade do encarregado de educação do aluno, ou do aluno se maior, após o envio da informação por parte da DGEEC para a TIP, deverá ser requerida junto da TIP*. A CNPD relembra que nos termos do n.º 3 do artigo 26.º do RGPD o titular dos dados pode exercer os seus direitos em relação a cada um dos responsáveis pelo tratamento, independentemente do acordado pelas entidades outorgantes.

iii. Obrigações dos responsáveis pelo tratamento – Cláusula sexta

17. Nos termos da cláusula primeira do Protocolo, a DGEC e a TIP são responsáveis conjuntos pelo tratamento, sendo a TIP a entidade coordenadora e operadora do Sistema ANDANTE, e responsável pela emissão, gestão e aprovisionamento dos Cartões ANDANTE personalizados e ainda «responsável pelo Sistema Intermodal Andante,

[1] A alínea *b)* do artigo 36.º dispõe que é da competência das câmaras municipais «*Requisitar às entidades concessionárias dos serviços de transporte coletivo os bilhetes de assinatura (passes) para os alunos abrangidos, nos termos a fixar por portaria dos membros do Governo com competência na matéria*».

o sistema central que reúne os dados pessoais e informações sobre clientes, vendas e validações dos operadores de transporte público».

18. Operacionalmente a DGEEC tem a atribuição de *gerir o sistema integrado de informação e gestão da oferta educativa e formativa,* enquanto a DGEstE é *responsável pela verificação das colocações dos alunos nas respetivas escolas e agrupamentos*. Assim, o n.º 3 da Cláusula primeira estipula que a DGEstE é também considerada responsável conjunta pelo tratamento, na relação com a DGEEC.

19. Assim, estamos perante um caso de responsabilidade conjunta, que pressupõe a existência de um acordo que reflita devidamente as funções e relações respetivas dos responsáveis conjuntos pelo tratamento em relação aos titulares dos dados. Deste modo, este deverá definir *as respetivas responsabilidades pelo cumprimento do RGPD, nomeadamente no que diz respeito ao exercício dos direitos dos titulares dos dados e aos respetivos deveres de fornecer as informações referidas nos artigos 13.º e 14.º*, e refletir *as funções e relações respetivas dos responsáveis conjuntos pelo tratamento em relação aos titulares dos dados* (cf. n.º 2 do artigo 26.º do RGPD).Além disso, a repartição de responsabilidades deve cobrir outras obrigações dos responsáveis tais como as relativas ao cumprimento dos princípios de proteção de dados, fundamento de licitude, medidas de segurança, obrigação de notificação de violação de dados pessoais, o uso de subcontratantes, contactos com os titulares dos dados e com a Autoridade de Controlo[2]. A CNPD sugere, assim, que seja alterado o conteúdo da cláusula por forma a conter uma referência expressa à existência de um acordo entre os dois responsáveis pelo tratamento que consagre as respetivas responsabilidades pelo cumprimento do RGPD.

iv. Subcontratação

20. Note-se que a Cláusula sétima, relativa à subcontratação, se limita a consagrar a necessidade de autorização prévia para subcontratação e a observar o disposto no artigo 29.º do RGPD. Entende-se que a cláusula é demasiado vaga pelo que se recomenda que sejam incluídas referências às obrigações dos subcontratantes plasmadas nos n.ºs 2 a 4 do artigo 28.º do RGPD.

v. Direito de acesso e informação dos titulares dos dados – Cláusula oitava

21. Aqui constata-se que o corpo da Cláusula é mais abrangente do que a sua epígrafe, uma vez que consagra a responsabilidade de cada responsável em assegurar o efetivo exercício *dos direitos dos titulares dos dados*, bem como os deveres de informação referidos nos artigos 13.º e 14.º do RGPD. Ora, efetivamente, os direitos dos

[2] Vide Diretrizes sobre Responsáveis e subcontratantes disponível em https://edpb.europa.eu/guidelines-relevant-controllers-and-processors_en.

titulares dos dados não se esgotam no direito de acesso, abrangendo o direito de retificação e apagamento, limitação do tratamento, portabilidade e direito de oposição. Sugere-se assim a alteração da epígrafe para «direitos dos titulares dos dados»

vi. Medidas de segurança e privacidade – Cláusula nona

22. Quanto às medidas de segurança, o ponto 3 da Cláusula nona do Protocolo consagra, que no âmbito da recolha, os outorgantes elaborem uma lista nominativa de colaboradores autorizados a aceder aos dados pessoais de acordo com a sua função, em cumprimento do princípio da minimização dos dados e do princípio da necessidade de conhecer (*need to know*) consagrado na alínea *c)* do n.º 1 do artigo 5.º, do RGPD.

23. Prevê-se a utilização de um identificador único, distinto e exclusivo de utilização neste *webservice* que garanta a identificação de um único processo de matrícula, permitindo à TIS efetuar mais tarde novamente a invocação para reprocessamento de registo anteriormente transferidos, indicando no pedido esse mesmo identificador.

24. A DGGE fornece à TIS uma conta de serviço, específica para autenticação no sistema. O envio da palavra-chave dessa conta para a TIS será efetuado em separado da informação sobre o utilizador para a pessoa e número de telefone previamente estabelecido. A transferência da informação será efetuada em circuito dedicado e seguro, comprometendo-se as duas entidades a registar todas as consultas e outros acessos à informação em ficheiros *log*, também esses encriptados.

25. Foi efetuada uma Avaliação de Impacto na Proteção de Dados, que acompanha o pedido de Parecer, tendo a mesma classificado o conjunto de operações efetuadas sobre dados pessoais objeto do presente Protocolo como de nível médio de risco. Quanto ao efeito prejudicial, este foi considerado significativo por força do tratamento do Escalão Social Escolar, dado pessoal considerado de natureza altamente pessoal, tendo em conta o risco significativo de estigmatização e discriminação em crianças e jovens.

26. Adicionalmente, o risco de identificação do titular, através do nome, número e tipo de documento de identificação foi considerado como máximo. Para mitigar estes riscos que colocam em causa os direitos e liberdades dos titulares (pertencendo a categorias de titulares especialmente vulneráveis) serão implementadas várias medidas técnicas e organizativas, descritas na AIPD, destacando-se, entre elas, a geração de números aleatórios na variável que contém o identificador único a partir do número do processo de matrícula; a pseudonimização dos dados de testes utilizados nos vários ambientes de desenvolvimento; a encriptação na comunicação dos dados utilizando o protocolo TLS 1.25 ; a encriptação no armazenamento da informação em

produção e na tabela de *logs* de auditoria; a elaboração de lista de acessos (mecanismos ACL) nominal; ações de sensibilização sobre a proteção de dados e RGPD, quer na DGEEC, quer na TIS.

27. Note-se, que na seção "Avaliação global para uma AIPD aceitável", página 13, é referido que *a informação, encontra-se de forma genericamente anonimizada, através de técnicas de encriptação na base de dados, onde residirão os logs e de encriptação do canal de comunicação, tal como proposto incluindo o armazenamento dos logs e os canais de transmissão (i.e., encriptação na comunicação e no armazenamento)*. Ora, a referência à anonimização da informação não está correta, pois, por um lado, a técnica de pseudonimização, listada na AIPD como uma das medidas mitigadoras do risco para os titulares, não é considerada uma técnica de anonimização, visto que «apenas dificulta a possibilidade de correspondência de um conjunto de dados à identidade original de um titular de dados[3]». Por outro lado, se a informação estivesse de facto anonimizada, tornava-se impossível a sua utilização para o tratamento de dados descrito no protocolo.

28. Após a análise do Protocolo e da AIPD, considera-se que as medidas técnicas e organizativas propostas para mitigar os riscos identificados na AIPD, a implementar no âmbito do Protocolo, são aceitáveis e adequadas para assegurar a segurança dos dados pessoais e a privacidade.

III. Conclusão

29. Com a introdução das alterações acima identificadas, a CNPD entende não haver impedimentos à celebração do Protocolo para o intercâmbio de dados pessoais entre a Direção Geral de Estatísticas da Educação e Ciência (DGEEC) e a Transportes Intermodais do Porto, ACE (TIP).

Aprovado na sessão plenária de 23 de fevereiro de 2021

Filipa Calvão (Presidente)

[3] Conforme disposto no Parecer 05/2014 sobre técnicas de anonimização, do Grupo de trabalho de Proteção de Dados do Artigo 29, acessível em https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp216_en.pdf