

## PARECER/2021/120

### I. Pedido

1. A Caixa Geral de Aposentações 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 do Sistema de Informação do Ministério da Educação e do Sistema de Informação da Caixa Geral de Aposentações, a celebrar entre a Caixa Geral de Aposentações (CGA), a Direção-Geral de Estatísticas da Educação e Ciência (DGEEC) e a Agência para a Modernidade Administrativa (AMA), bem como do correspondente Estudo de Impacto.

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.

### II. Análise

#### i. Objecto e operações de tratamento

3. O Protocolo em análise visa regular os procedimentos relativos à troca de informações entre a DGCEE e a CGA, relativas “à prova de situação escolar em estabelecimento de ensino, para efeitos de reconhecimento e manutenção do direito para efeitos de atribuição de prestações familiares e de pensões de sobrevivência e de preço de sangue por parte da CGA”.

4. A referida troca de informação é realizada através da plataforma de Interoperabilidade da Administração Pública (iAP), gerida pela AMA.

5. Para cumprimento das finalidades do Protocolo, a DGEE transmite à CGA os seguintes dados dos alunos: NISS PS Titular / Estudante; ano Letivo da Prova Escolar / Matrícula; ano de Escolaridade da Matrícula (prova); nível de Ensino da Prova Escolar / Matrícula; aproveitamento Escolar do Ano Letivo Anterior; situação da Matrícula; data da Situação da Matrícula, dados que, atendendo às finalidades visadas, parecem adequados e não excessivos.

6. Uma vez que o n.º 3 da Cláusula Segunda se refere a estes dados como as “respostas possíveis da DGEEC”, deduz-se que tais informações sejam facultadas a solicitação da CGA.

7. Das Cláusulas Segunda<sup>1</sup> e Terceira resulta que a "CGA, através da AMA, I.P. não disponibiliza à DGEEC qualquer informação adicional ao que esta já detém nos seus sistemas de informação, para além das mensagens de controlo e de pedido de informação do titular de dados, previstas no protocolo de comunicações, para que a CGA obtenha os dados de que necessita".

8. Esta redação carece de clarificação. Senão vejamos: é dito que, através da AMA, não será transmitida pela CGA à DGEEC nenhuma informação além da que esta entidade já disponha. Ora, não fica claro se se pretendeu excluir a transmissão de qualquer outra informação da CGA para a DGEEC, seja qual for a via, ou se existirá a transmissão de outra informação, mas não por esta via. Nesse caso, haveria que indicar qual a informação em causa. Ademais, é referido um "protocolo de comunicações" onde se encontrarão previstas as informações a transmitir, o qual não foi junto ao requerimento de parecer, o que impede a CNPD de se pronunciar sobre todos os aspetos relevantes.

## **ii. Responsabilidade conjunta e direitos dos titulares dos dados**

9. Nos termos do artigo 2.º do Decreto Regulamentar n.º 13/2012, de 20 de janeiro, na sua redação atual, cabe à DGEEC criar e assegurar o bom funcionamento do Sistema Integrado de Informação da Educação e Ciência, bem como observar e avaliar globalmente os resultados obtidos pelos sistemas educativo e tecnológico, em articulação com os demais serviços da Educação e Ciência. Para tal, prossegue, nomeadamente, as seguintes atribuições: garantir a recolha, monitorização, tratamento, produção e divulgação de informação adequada, no quadro do Sistema Estatístico Nacional; gerir o sistema integrado de informação e gestão da oferta educativa e formativa; conceber e implementar as aplicações informáticas de gestão do sistema de informação, nomeadamente as que assegurem a consistência dos dados e certificar as aplicações escolares e, em particular para o que ora importa, o sistema MISI, o Escola 360 e o Portal das Matrículas, através dos quais se faz a recolha e tratamento da informação relevante para a execução do presente Protocolo.

10. Por seu turno, A CGA é um Instituto Público que "tem por missão gerir o regime da segurança social público em matéria de pensões e aposentação, de reforma, de sobrevivência e de outra natureza especial" (n.º 1 do artigo 3.º do Decreto-Lei n.º 131/2012, de 25 de junho).

11. Por seu turno, a AMA é o Instituto Público responsável por assegurar a operacionalização do iAP que, nos termos do n.º 2 do artigo 6.º do Decreto-Lei n.º 73/2014, 13 de maio, se constitui como o meio preferencial de comunicação entre os serviços e organismos da Administração Pública.

---

<sup>1</sup> O número 1 da Cláusula Segunda remete para "a situação definida na alínea a) da cláusula primeira", que, no entanto, não existe.

12. Nos termos da Cláusula Sexta, a CGA e a DGEEC assumem-se como “responsáveis conjuntos nos termos do artigo 26.º do RGPD”, cabendo ao terceiro contraente, a AMA, a posição de subcontratante.
13. No que respeita à proteção de dados, refira-se que a epígrafe da Cláusula Quinta se presta a equívocos. De facto, sob a designação *Direitos dos Titulares* não se regula o exercício de quaisquer direitos, antes se consagra o acordo das Partes de “comunicar de forma expedita, designadamente através de correio eletrónico”, os pedidos dos titulares dos dados que pretendam exercer os seus direitos. Assim, do que se trata, verdadeiramente, é de estabelecer um dever de colaboração entre os responsáveis pelo tratamento e a AMA.
14. No que tange às obrigações específicas dos outorgantes quanto ao tratamento de dados e, mais precisamente, quanto à salvaguarda dos direitos dos titulares, rege a Cláusula Décima<sup>2</sup>.
15. Assim, no n.º 1 é dito que compete à AMA colaborar com os responsáveis na garantia dos do exercício dos direitos dos titulares, informar os responsáveis pelo tratamento de eventuais retificações ou situações de apagamento de dados pessoais solicitados pelo titular e garantir que exista fundamento de licitude para a realização do tratamento dos dados.
16. Por sua vez, o número 2 identifica as responsabilidades dos responsáveis pelo tratamento. Assim, vêm indicados dois endereços de correio eletrónico, um da DGEEC e outro da CGA através dos quais os titulares ou seus encarregados de educação podem solicitar esclarecimentos consoante o tipo de informação que pretendam. Assim, através do endereço [dpo@dgeec.mec.pt](mailto:dpo@dgeec.mec.pt) os titulares dos dados podem solicitar “esclarecimentos sobre questões de privacidade dos sistemas de tratamento de dados”. O endereço [epd@cga.pt](mailto:epd@cga.pt) será usado para solicitar “esclarecimentos sobre questões de privacidade dos sistemas de tratamento de dados”, sem embargo de nos termos da mesma cláusula, qualquer um dos outorgantes possa receber esses pedidos.
17. Não se compreende, no entanto, a razão pela qual se estabelece na alínea h) do número 2 que o pedido de retificação de dados tenha de ser formulado por escrito para a Direção-Geral da Educação e Ciência ou a Caixa Geral de Aposentações – de acordo com as respetivas competências –, sem se explicitar que o correio eletrónico pode ser o meio a utilizar para o efeito, permitindo a interpretação de que não poderá ser efetuado, também, através de tal meio.
18. Nada se diz quanto ao exercício do direito de apagamento de dados, informação que deve ser disponibilizada ao titular.

---

<sup>2</sup> Crê-se haver um lapso na epígrafe *Direito de Acesso Tutela de Direitos dos Titulares dos Dados Pessoais*, devendo ser suprimida a primeira parte uma vez que a categoria *direitos dos titulares* engloba, necessariamente, o direito de acesso.

19. Caso exista suspensão ou resolução do Protocolo tal implica, por força do disposto na Cláusula Décima-Terceira, a imediata cessação da autorização de acesso aos dados pessoais.

20. Encontra-se preceituado o dever de confidencialidade durante a vigência do Protocolo e mesmo após a sua cessação.

### iii. Tratamento de dados

21. A “forma, extensão e limites da interconexão de dados entre os diversos serviços e organismos da Administração Pública” necessários ao cumprimento da sua missão encontram previsão no Decreto-Lei n.º 309/2007, de 7 de setembro, que, no uso de uma autorização legislativa, elenca no artigo 2.º as bases de dados das quais constam os dados a relacionar para que a CGA cumpra a sua missão.

22. Diga-se desde, já que, das bases de dados que a Cláusula Segunda menciona como sendo as que fornecerão os dados no âmbito do presente Protocolo - Portal das Matrículas, Escola 360 e MISI (Gabinete Coordenador do Sistema de Informação do Ministério da Educação) -, apenas a terceira consta da lista do decreto-lei (alínea j). De facto, esta alínea estabelece o acesso pela CGA apenas aos dados referentes à matrícula, frequência e aproveitamento escolar constantes da base de dados MISI.

23. Assim, quanto às demais, não se encontra previsto o tratamento de dados, pelo que havendo fundamento de licitude para a recolha e tratamento de dados nos termos do respetivo regime, parece não existir para a transmissão à CGA.

24. O n.º 4 do artigo 4.º do referido decreto-lei consagra que “[o] acesso da CGA aos dados sobre a situação escolar dos alunos constantes das bases de dados do MISI tem por exclusiva finalidade permitir a ponderação de informações pertinentes às específicas decisões de atribuição de prestações sociais e à prevenção e combate à fraude e evasão contributiva, designadamente para efeitos de atribuição de prestações familiares e de pensões de sobrevivência e de preço de sangue”. De onde a referência exclusiva também à mesma base de dados, com exclusão das demais.

25. As categorias de dados objeto de interconexão são, nos termos da alínea g) do n.º 1 do artigo 3.º, a “situação escolar dos alunos, relativamente à frequência e aproveitamento, e teor do registo dos estabelecimentos de ensino não públicos legalizados, das bases de dados do MISI.

26. Por conseguinte, caso se trate de um tratamento novo realizado a partir das bases de dados Escola 360 e Portal das Matrículas, haverá que encontrar fundamento legal para essa transferência.

27. Não está excluída, no entanto, a hipótese de uma interpretação atualizada das condições definidas no referido diploma legal, caso as demais bases de dados ou sistemas de informação indicadas no presente protocolo tenham sido criadas após a entrada em vigor deste diploma legal, que permita estender a fórmula «Matrícula, frequência e aproveitamento escolar e de estabelecimentos de ensino não públicos legalizados, sedeadas no Gabinete Coordenador do Sistema de Informação do Ministério da Educação (MIS), a outros sistemas de informação que contenham os dados pessoais relevantes e necessários para a finalidade legalmente delimitada.

28. De todo o modo, uma vez que a informação transmitida pela DGEEC à CGA já se encontra nos sistemas Portal das Matrículas, Escola 360 e MISI, estando assegurado o fundamento de licitude desta recolha, haverá, agora que garantir a informação aos titulares ou seus representantes em relação a este novo tratamento.

#### **iv. Condições de acesso à informação e Garantias de Segurança e Privacidade**

29. Explicita-se na Cláusula Quarta que a partilha de dados é efetivada com recurso a *WebServices* capazes de garantir a protecção de dados e efetuada através de um circuito dedicado entre as entidades.

30. Como condições de acesso à informação prevêem-se mecanismos de autenticação prévia perante as entidades outorgantes. Ainda, que a credenciação dos utilizadores é efetuada através da atribuição de um utilizador aplicacional e de uma palavra-chave. Será elaborada lista nominativa de colaboradores autorizados a aceder aos dados pessoais de acordo com a sua função.

31. Todas as consultas efetuadas são objeto de registos conservados pelo prazo de dois anos para fins de auditoria.

32. Quanto às medidas de Segurança, prevê-se na Cláusula Décima-Primeira que os dados comunicados ao abrigo do Protocolo apenas possam ser utilizados para os fins nele previstos, sendo conservados pelo período estritamente necessário à prossecução da finalidade prevista no presente protocolo, que não se indica.

33. Determina-se de forma genérica que devem ser “adotados padrões de segurança organizacional e tecnológica que garantam a proteção da confidencialidade e integridade dos dados.

34. Como exemplo das medidas técnicas a adotar, indicam-se, com especial relevância:

- a. quanto ao meio de comunicação entre as entidades - proteção da comunicação por *Virtual Private Network* (VPN) e encriptação de dados através do protocolo de segurança TLS v1.2.

- b. quanto ao controlo de acessos – controlo de acesso nominal tanto no acesso à rede corporativa dos outorgantes como ao conteúdo da base de dados com o conteúdo da *WebService*, bem como restrições de acesso por competência funcional.

35. A Avaliação de Impacto sobre a Proteção de Dados elaborada e que foi igualmente submetida à apreciação da CNPD, considerou que o nível de risco para os dados pessoais dos titulares é baixo, conquanto sejam cumpridas as medidas de segurança e mitigação previstas.

36. De facto, de uma forma geral, o Projeto de Protocolo consagra boas práticas na implementação de sistemas de partilha de informação. A utilização de um protocolo criptográfico confere proteção à informação em trânsito entre entidades e o mecanismo de autenticação e respetivas credenciais nominais robustecem o sistema, promovendo a capacidade de mitigação de incidentes de segurança.

37. É garantida a monitorização necessária, através de estabelecimento de restrições de acesso por competência funcional e de um sistema de registos de eventos, fortalecido por uma política de conservação desses registos por um período aceitável de 2 anos.

38. No entanto, não será demais recomendar que seja enfatizado o carácter pessoal e intransmissível das credenciais de acesso a atribuir aos utilizadores indicados pelos outorgantes, bem como o reforço das políticas de gestão de privilégios de acesso a dados pessoais, no sentido de garantir que a informação veiculada entre outorgantes encontra enquadramento no protocolo a celebrar.

39. Ainda, recomenda-se que se proceda à definição cuidadosa dos eventos de acesso à informação a registar, por forma a garantir uma mais eficaz prevenção de incidentes, bem com a mitigação dos seus efeitos, caso se verifiquem.

40. De igual forma, sugere-se a realização de ações de formação no sentido de capacitar os interlocutores indicados pelos outorgantes a operar os mecanismos de partilha previstos, de acordo com o Protocolo e demais políticas e procedimentos internos eventualmente existentes, bem como a sensibilização para os erros mais comuns e potencialmente suscetíveis de originar violação de dados pessoais.

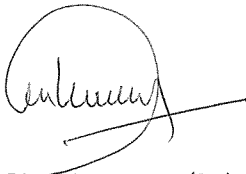
41. Por outro lado seria desejável a implementação de procedimentos de auditoria com o objetivo de rever, confirmar e manter o cumprimento das políticas e dos procedimentos instituídos à luz do Protocolo e a revisão regular as medidas e políticas de segurança da informação, de forma a imprimir melhorias sempre que se afigure necessário.

### III. Conclusão

42. Com os fundamentos acima expostos entende a CNPD que deverá ser verificada a existência de um fundamento de licitude para a transferência de dados da plataforma Escola 360 e Plataforma de Matrículas para a CGA.

43. Salvaguardada que seja essa questão, a CNPD considera que, no geral, o Protocolo consagra medidas de segurança dos sistemas e de mitigação de riscos adequados e recomenda que sejam consideradas as medidas referidas os pontos 38 a 41.

Lisboa, 10 de setembro de 2021



Ana Paula Pinto Lourenço (Relatora)