Parecer do Comité (artigo 64.º)

Parecer 28/2022 sobre os critérios de certificação Europrivacy no que diz respeito à sua aprovação pelo Comité como Selo Europeu de Proteção de Dados nos termos do artigo 42.º, n.º 5 (RGPD)

Adotado em 10 de outubro de 2022

Translations proofread by EDPB Members.
This language version has not been proofread yet.

O Comité Europeu para a Proteção de Dados

Tendo em conta o artigo 63.º, o artigo 64.º, n.º 2, e o artigo 42.º 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 e que revoga a Diretiva 95/46/CE (a seguir designado por «RGPD»),

Tendo em conta o Acordo sobre o Espaço Económico Europeu (a seguir designado por «Acordo EEE») e, nomeadamente, o seu anexo XI e Protocolo n.º 37, com a redação que lhe foi dada pela Decisão n.º 154/2018 do Comité Misto do EEE, de 6 de julho de 2018[1],

Tendo em conta os artigos 10.º e 22.º do seu regulamento interno,

(1) Os Estados-Membros, as autoridades de controlo, o Comité Europeu para a Proteção de Dados (a seguir designado por «CEPD» ou «Comité») e a Comissão Europeia devem promover, em especial a nível da União, a criação de procedimentos de certificação em matéria de proteção de dados (a seguir designados por «procedimentos de certificação»), bem como selos e marcas de proteção de dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o RGPD, tendo em conta as necessidades específicas das micro, pequenas e médias empresas[2]. Além disso, a criação de procedimentos de certificação pode reforçar a transparência e permitir aos titulares dos dados avaliar o nível de proteção de dados proporcionado pelos produtos e serviços em causa[3].

(2) Os critérios de certificação fazem parte integrante de um procedimento de certificação. Por conseguinte, o RGPD exige a aprovação dos critérios de um procedimento nacional de certificação pela autoridade de controlo competente [artigo 42.º, n.º 5, e artigo 43.º, n.º 2, alínea b), do RGPD] ou, no caso de um Selo Europeu de Proteção de Dados, pelo CEPD [artigo 42.º, n.º 5, e artigo 70.º, n.º 1, alínea o), do RGPD].

(3) Sempre que uma autoridade de controlo (a seguir designada por «AC») tencione propor a aprovação pelo CEPD de um Selo Europeu de Proteção de Dados nos termos do artigo 42.º, n.º 5, do RGPD, a AC deve declarar a intenção do proprietário do sistema de oferecer o procedimento de certificação em todos os Estados-Membros. Neste caso, o principal papel do CEPD consiste em assegurar a aplicação coerente do RGPD, através do procedimento de controlo da coerência referido nos artigos 63.º, 64.º e 65.º do RGPD. Neste contexto, em conformidade com o artigo 64.º, n.º 2, do RGPD, o CEPD está a aprovar os critérios de certificação.

(4) O presente parecer visa assegurar a aplicação coerente do RGPD, nomeadamente por parte das AC, dos responsáveis pelo tratamento e dos subcontratantes, à luz dos elementos essenciais que os procedimentos de certificação têm de desenvolver. Em especial, a avaliação do CEPD é realizada com base nas «Diretrizes 1/2018 relativas à certificação e à definição dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento» (a seguir designadas por «diretrizes») e na

[1] As referências a «Estados-Membros» no presente parecer devem ser entendidas como referências a «Estados-Membros do EEE».
[2] Artigo 42.º, n.º 1, do RGPD.
[3] Considerando 100 do RGPD.

respetiva adenda que fornece «Orientações sobre a avaliação dos critérios de certificação» (a seguir designada por «adenda»), cujo período de consulta pública expirou em 26 de maio de 2021.

(5) Por conseguinte, o CEPD reconhece que cada procedimento de certificação deve ser tratado individualmente e não prejudica a avaliação de qualquer outro procedimento de certificação.

(6) Os procedimentos de certificação devem permitir aos responsáveis pelo tratamento e aos subcontratantes demonstrar a conformidade com o RGPD. Assim, os seus critérios devem refletir adequadamente os requisitos e princípios relativos à proteção dos dados pessoais estabelecidos no RGPD e contribuir para a sua aplicação coerente.

(7) Ao mesmo tempo, o proprietário do sistema deve assegurar a harmonização e a conformidade do procedimento de certificação com quaisquer normas ISO e práticas de certificação incluídas ou valorizadas.

(8) Consequentemente, as certificações devem acrescentar valor aos responsáveis pelo tratamento e aos subcontratantes, ajudando a aplicar medidas organizativas e técnicas normalizadas e especificadas que, comprovadamente, facilitem e reforcem a conformidade das operações de tratamento com o RGPD, tendo em conta os requisitos setoriais específicos.

(9) O CEPD congratula-se com os esforços envidados pelos proprietários de sistemas para elaborar procedimentos de certificação, que são instrumentos práticos e potencialmente eficazes em termos de custos para assegurar uma maior coerência com o RGPD e promover o direito à privacidade e à proteção de dados dos titulares dos dados, aumentando a transparência.

(10) O CEPD recorda que as certificações são instrumentos de responsabilização voluntária e que a adesão a um procedimento de certificação não reduz a responsabilidade dos responsáveis pelo tratamento ou dos subcontratantes pelo cumprimento do RGPD nem impede as autoridades de controlo de exercerem as suas funções e os seus poderes nos termos do RGPD e da legislação nacional aplicável.

(11) No presente parecer, o CEPD aborda questões como o âmbito dos critérios, a aplicabilidade e a pertinência dos critérios em todos os Estados-Membros.

(12) O presente parecer centra-se nos critérios de certificação. Caso o CEPD exija informações de alto nível sobre os métodos de avaliação para poder avaliar exaustivamente a auditabilidade dos critérios no contexto do seu parecer, este último não inclui qualquer tipo de aprovação desses métodos de avaliação.

(13) O parecer do CEPD deve ser adotado, nos termos do artigo 64.º, n.º 2, do RGPD, em conjugação com o artigo 10.º, n.º 2, do Regulamento Interno do CEPD, no prazo de oito semanas a contar do primeiro dia útil após a presidente e a autoridade de controlo competente terem decidido que o processo está completo. Por decisão da presidente, este prazo pode ser prorrogado por mais seis semanas, tendo em conta a complexidade do tema. Se o parecer do CEPD concluir que os critérios em causa não podem ser aprovados, a AC pode voltar a apresentar os critérios para aprovação quando forem abordadas as preocupações expressas no parecer inicial do CEPD.

ADOTOU O PRESENTE PARECER:

RESUMO DOS FACTOS

1. Em conformidade com o artigo 42.º, n.º 5, do RGPD e com as diretrizes, os critérios Europrivacy v.60 (a seguir designados por «projeto de critérios de certificação», «critérios de certificação» ou «critérios») foram elaborados pelo Centro Europeu para a Certificação e a Privacidade (a seguir designado por «proprietário do sistema»).

2. A autoridade de controlo luxemburguesa (a seguir designada por «AC luxemburguesa») apresentou os critérios de certificação Europrivacy ao CEPD para aprovação nos termos do artigo 64.º, n.º 2, do RGPD em 28 de setembro de 2022. A decisão de que o processo está completo foi tomada em 28 de setembro de 2022.

3. O procedimento de certificação Europrivacy não é uma certificação nos termos do artigo 46.º, n.º 2, alínea f), do RGPD destinada a transferências internacionais de dados pessoais e, por conseguinte, não prevê garantias adequadas no quadro das transferências de dados pessoais para países terceiros ou organizações internacionais nos termos do artigo 46.º, n.º 2, alínea f). Com efeito, qualquer transferência de dados pessoais para um país terceiro ou para uma organização internacional só pode ser efetuada se forem respeitadas as disposições do capítulo V do RGPD.

2 AVALIAÇÃO

4. O CEPD realizou a avaliação dos critérios de certificação para a sua aprovação nos termos do artigo 42.º, n.º 5, do RGPD, em conformidade com a estrutura prevista no anexo 2 das diretrizes (a seguir designado por «anexo») e respetiva adenda.

5. O CEPD observa que as orientações de execução e os meios sugeridos de verificação do procedimento de certificação fornecidos pelo proprietário do sistema nem sempre são coerentes em todo o catálogo de critérios. Por exemplo, a secção T.2.3.2 exige que existam regras, políticas, procedimentos ou mecanismos para detetar e comunicar intrusões (por exemplo, um sistema de deteção de intrusões que monitorize o tráfego de rede para atividades suspeitas e emita um alerta quando for detetada tal atividade), ao passo que os meios de verificação sugeridos se referem ao teste de inspeção e penetração (exigido na secção T.2.3.1). Embora tais incoerências não sejam abrangidas pelo âmbito da sua avaliação, o CEPD sublinha que podem constituir um obstáculo à acreditação do organismo de certificação, a menos que sejam retificadas pelo proprietário do sistema.

2.1 Âmbito do procedimento de certificação e alvo da avaliação («target of evaluation» - ToE)

6. O procedimento de certificação Europrivacy é um sistema geral, na medida em que visa uma vasta gama de diferentes operações de tratamento realizadas por responsáveis pelo tratamento e subcontratantes de vários setores de atividade. Os principais critérios deste procedimento de certificação são compostos pelos «critérios fundamentais» e pelos «controlos e verificações das medidas técnicas e organizativas» relativos às medidas tecnológicas e organizativas estabelecidas para garantir a segurança dos dados pessoais tratados. Um conjunto de critérios de «controlos e verificações das medidas técnicas e organizativas» só é aplicável se o alvo de avaliação (a seguir designado por «ToE», do inglês «target of evaluation») tratar categorias especiais de dados, dados relacionados com infrações penais ou dados pessoais de uma criança.

7. Além disso, os critérios incluem igualmente «verificações e controlos contextuais complementares» que visam assegurar que o tratamento de dados envolvido no ToE cumpre os requisitos específicos em termos de domínio e tecnologia. Uma matriz informativa fornecida pelo proprietário do sistema descreve a que categorias de operações de tratamento de dados se aplica cada conjunto de critérios de «verificações e controlos contextuais complementares».

8. O CEPD congratula-se com os sistemas gerais que incluem critérios específicos para os tornar moduláveis e aplicáveis a operações de tratamento ou a setores de atividade específicos. No entanto, o CEPD pretende igualmente clarificar que, no contexto de um sistema geral, a exaustividade dos critérios relativos a operações de tratamento específicas não é necessária e, por conseguinte, não foi avaliada no contexto do presente parecer. Além disso, o CEPD recorda que, ao publicar documentos relacionados com atividades de tratamento específicas, tais documentos devem ser tidos em conta pelo proprietário do sistema e pelos organismos de certificação acreditados.

9. Os critérios aplicáveis à especificação do ToE são definidos nos requisitos constantes da secção A.2.1.1. As regras específicas aplicáveis ao processo a seguir pelo requerente e pelo organismo de certificação para definir o ToE são especificadas pelo sistema Europrivacy (10.2 – Atividades de pré-certificação).

10. O Comité observa, na documentação relacionada com o âmbito do procedimento de certificação fornecida pela AC luxemburguesa, que o sistema Europrivacy se aplica aos responsáveis pelo tratamento e aos subcontratantes estabelecidos na União Europeia (UE) ou no Espaço Económico Europeu (EEE). A aplicabilidade dos critérios é definida em função do papel e das responsabilidades do requerente.

11. O Comité observa que um responsável pelo tratamento pode submeter ao processo de certificação Europrivacy um ToE sujeito a responsabilidade conjunta pelo tratamento (secção A.2.7.1 dos critérios). Caso o ToE seja objeto de responsabilidade conjunta pelo tratamento, o Comité pretende sublinhar que o organismo de certificação acreditado terá de conduzir cuidadosamente o processo de candidatura para assegurar que o ToE é significativo e que o requerente é plenamente responsável pela conformidade do ToE com todas as obrigações previstas no RGPD que o procedimento de certificação visa demonstrar. Consequentemente, o acordo celebrado entre o requerente e os outros responsáveis conjuntos pelo tratamento envolvidos no ToE no que diz respeito às respetivas responsabilidades pela conformidade com as obrigações decorrentes do RGPD[4] pode – dependendo do contexto das atividades de tratamento do ToE – impedir o requerente de cumprir os critérios de certificação.

12. O Comité observa que o tratamento de dados genéticos está excluído do âmbito de aplicação do procedimento de certificação Europrivacy. Por conseguinte, a avaliação dos critérios realizada pelo Comité não abrange a adequação dos critérios para os ToE que incluiriam o tratamento de dados em causa.

2.2 Operações de tratamento

13. Os critérios abordam os componentes pertinentes das operações de tratamento (dados, sistemas e tratamento) no que diz respeito ao âmbito geral do procedimento de certificação. Em especial, os

[4] *A determinação das suas respetivas responsabilidades deve ter especialmente em consideração o exercício dos direitos dos titulares dos dados e os deveres de fornecer informações. Além do que precede, a repartição de responsabilidades deve abranger outras obrigações do responsável pelo tratamento, tais como no que se refere aos princípios gerais de proteção de dados, à base jurídica, às medidas de segurança, à obrigação de notificação de violação de dados, às avaliações do impacto sobre a proteção de dados, à utilização de subcontratantes, às transferências para países terceiros e aos contactos com titulares de dados e autoridades de controlo* (Orientações 07/2020 sobre os conceitos de responsável pelo tratamento e subcontratante no RGPD).

critérios permitem identificar categorias especiais de dados, tal como definidas no artigo 9.º do RGPD (secção G.2 dos critérios – Tratamento de dados especiais).

2.3 Licitude do tratamento

14. Os critérios exigem a verificação da licitude do tratamento de dados para cada uma das operações de tratamento do ToE, bem como exigem a verificação dos requisitos de um fundamento jurídico, tal como definida no artigo 6.º do RGPD (secção G.1 dos critérios – Licitude do tratamento de dados).

2.4 Princípios do tratamento de dados

15. Os critérios abordam adequadamente os princípios de proteção de dados nos termos do artigo 5.º do RGPD. Em especial, os critérios exigem que o requerente demonstre que os dados pessoais são adequados, pertinentes e limitados ao que é necessário relativamente às finalidades para as quais são tratados (minimização dos dados).

2.5 Obrigações gerais dos responsáveis pelo tratamento e dos subcontratantes

16. Os critérios refletem as obrigações do responsável pelo tratamento nos termos do artigo 24.º do RGPD (secção G.4 – Responsabilidade do responsável pelo tratamento), bem como exigem a avaliação dos acordos contratuais entre o subcontratante e o responsável pelo tratamento em conformidade com o artigo 28.º do RGPD (secção G.5 dos critérios – Subcontratantes ou subcontratantes ulteriores).

17. Os critérios exigem que todos os requerentes nomeiem um encarregado da proteção de dados (EPD), mesmo no caso de o requerente não ser obrigado a designar um EPD nos termos do artigo 37.º do RGPD. Os critérios verificam se o EPD cumpre os requisitos previstos nos artigos 37.º a 39.º (secção G.9 dos critérios – Encarregado da proteção de dados).

18. Os critérios verificam o conteúdo dos registos das atividades de tratamento em conformidade com o artigo 30.º do RGPD (secção G.5.3 dos critérios – Registos das atividades de tratamento).

2.6 Direitos dos titulares dos dados

19. Os critérios abordam adequadamente o direito à informação do titular dos dados, em conformidade com o capítulo III do RGPD, bem como exigem a adoção das respetivas medidas. Os critérios exigem igualmente a adoção de medidas que prevejam a possibilidade de intervir na operação de tratamento, a fim de garantir os direitos dos titulares dos dados e permitir a retificação, o apagamento ou a limitação (secção G.3 dos critérios – Direitos dos titulares dos dados).

2.7 Riscos para os direitos e liberdades

20. Os critérios exigem a avaliação do risco para os direitos e liberdades das pessoas singulares decorrente do tratamento de dados envolvido no ToE, em conformidade com o artigo 35.º do RGPD (secção G.8 dos critérios – Avaliação de impacto sobre a proteção de dados).

2.8 Medidas técnicas e organizativas que garantam a proteção

21. Os critérios exigem a aplicação de medidas técnicas e organizativas que prevejam a confidencialidade, a integridade e a disponibilidade das operações de tratamento. Os critérios exigem igualmente a utilização de medidas técnicas para aplicar a proteção de dados desde a conceção e por defeito, em conformidade com os artigos 25.º e 32.º do RGPD (secção G.6 dos critérios – Segurança do tratamento e proteção de dados desde a conceção, secção T.1/T.2 dos critérios – Requisitos de segurança fundamentais/Requisitos de segurança alargados).

22. Os critérios exigem a aplicação de medidas para assegurar que as obrigações de notificação de violações de dados pessoais são cumpridas em tempo útil e no âmbito de aplicação, em conformidade com os artigos 33.º e 34.º do RGPD (secção G.7 dos critérios – Gestão de violações de dados).

2.9 Critérios para demonstrar a existência de garantias adequadas para a transferência de dados pessoais

23. Os critérios exigem a identificação de todas as transferências de dados pessoais para países terceiros e organizações internacionais envolvidas no ToE, bem como a fundamentação da escolha feita relativamente ao mecanismo de transferência de dados que prevê garantias adequadas, nos termos do capítulo V do RGPD (secção G.10 dos critérios – Transferências de dados pessoais para países terceiros ou organizações internacionais).

3. CRITÉRIOS ADICIONAIS PARA UM SELO EUROPEU DE PROTEÇÃO DE DADOS

24. De acordo com as diretrizes, a avaliação deve incluir a questão de saber se os critérios podem ter em conta a legislação ou os cenários em matéria de proteção de dados dos Estados-Membros. A secção G.1.1.3 dos critérios exige que o requerente apresente a avaliação em causa num relatório de avaliação do cumprimento das obrigações nacionais (NOCAR). O Comité observa que tal relatório deve incluir uma avaliação das obrigações nacionais aplicáveis ao ToE, bem como documentar as medidas tomadas pelo requerente para cumprir as regras aplicáveis e, eventualmente, as medidas corretivas em curso. O requerente não deve utilizar a lista de requisitos nacionais complementares essenciais fornecida pelo proprietário do sistema para cada país como uma lista exaustiva de obrigações nacionais pertinentes para o ToE. A lista indicativa de requisitos mínimos de verificações e controlos complementares fornecida pelo proprietário do sistema não constitui um critério de certificação no âmbito do presente parecer.

CONCLUSÕES/RECOMENDAÇÕES

25. Em conclusão, o CEPD considera que os critérios de certificação Europrivacy são coerentes com o RGPD e aprova-os no âmbito da atribuição do Comité definida no artigo 70.º, n.º 1, alínea o), do RGPD, resultando numa certificação comum (Selo Europeu de Proteção de Dados).

26. O CEPD regista o procedimento de certificação Europrivacy no registo público dos procedimentos de certificação e dos selos e marcas de proteção de dados, nos termos do artigo 42.º, n.º 8.

OBSERVAÇÕES FINAIS

27. O presente parecer é dirigido à AC luxemburguesa e será tornado público nos termos do artigo 64.º, n.º 5, alínea b), do RGPD.

Pelo Comité Europeu para a Proteção de Dados

A Presidente