Parecer do Comité (artigo 64.º)

Parecer 19/2024 sobre os critérios de certificação EuroPriSe 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 16 de julho de 2024

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

Índice

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:

1. RESUMO DOS FACTOS

1. Em conformidade com o artigo 42.º, n.º 5, do RGPD e com as diretrizes, foi elaborado o projeto de «catálogo de critérios EuroPriSe para a certificação das operações de tratamento pelos subcontratantes (âmbito de aplicação: UE) v1.5» (a seguir «projeto de critérios de certificação», «critérios de certificação» ou «critérios») pela EuroPriSe Cert GmbH (a seguir designado «proprietário

do sistema»), uma entidade jurídica na Alemanha, e apresentado à Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen, a autoridade de supervisão alemã competente na Renânia do Norte-Vestefália (a seguir designada «DE-NRW SA»).

2. A autoridade de controlo alemã (a seguir designada por «AC alemã») apresentou o projeto de critérios de certificação ao CEPD para aprovação nos termos do artigo 64.º, n.º 2, do RGPD em 29 de abril de 2024. A decisão sobre a integralidade do processo foi tomada em 29 de maio de 2024.

3. O procedimento de certificação EuroPriSe 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.

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

5. O mecanismo de certificação EuroPriSe contém critérios de certificação de um sistema de certificação a nível da UE para a certificação do tratamento por subcontratantes. O objeto das certificações a que se aplica o catálogo de critérios são as operações de tratamento efetuadas em produtos, processos e serviços ou com a ajuda de (também vários) produtos e serviços e em relação às quais o requerente da certificação atua como subcontratante. Os principais critérios deste mecanismo de certificação estão divididos em três conjuntos de requisitos, a saber: do ponto de vista jurídico (conjunto 1), do ponto de vista das medidas técnicas e organizativas (conjunto 2) e do ponto de vista dos direitos das pessoas em causa (conjunto 3).

6. Os requerentes de certificação no âmbito deste regime devem ser subcontratantes, incluindo os subcontratantes que são diretamente encarregados do tratamento de dados pessoais por um responsável pelo tratamento na aceção do artigo 4.º, n.º 7, do RGPD. No entanto, os requerentes de certificação podem também ser subcontratantes na aceção do artigo 28.º, n.^{os} 2 e 4, do RGPD (subcontratantes ulteriores).

7. Quando um subcontratante, certificado ao abrigo do sistema de certificação EuroPriSe, utiliza um subcontratante ulterior, este não pode alegar que foi certificado ao abrigo do sistema de certificação EuroPriSe. Nesse caso, apenas as operações de tratamento realizadas pelo subcontratante inicial e certificado são abrangidas pela certificação. No entanto, os subcontratantes ulteriores também podem solicitar a certificação, resultando num procedimento autónomo e independente.

8. O Comité observa, na documentação relacionada com o âmbito do procedimento de certificação fornecida pela AC alemã, que o sistema EuroPriSe se aplica aos responsáveis pelo tratamento estabelecidos na União Europeia (UE) ou no Espaço Económico Europeu (EEE).

2.2 Tratamento de dados

9. O âmbito de aplicação destes critérios não se limita a determinados tipos de operações de tratamento. É antes a metodologia subjacente a uma avaliação EuroPriSe que permite a certificação de operações de tratamento por parte dos subcontratantes. Trata-se, por conseguinte, de uma abordagem metodológica universal com base na qual pode ser certificado um grande número de operações de tratamento muito diferentes. Por conseguinte, é de importância fundamental que os requisitos metodológicos sejam respeitados, uma vez que esta é a única forma de garantir uma aplicação uniforme dos critérios de certificação e um nível comparável de testes em diferentes procedimentos de certificação. O objetivo é assegurar a comparabilidade e a reprodutibilidade das certificações emitidas e dos seus resultados.

2.3 Licitude e princípios do tratamento de dados

10. Os critérios exigem a análise da questão de saber se as operações de tratamento a certificar cumprem os princípios da proteção de dados desde a conceção e por defeito (secção 1.5 dos critérios), o que implica a participação do requerente na assistência ao responsável pelo tratamento na aplicação destes princípios. Isto permite avaliar a conformidade com o artigo 25º do RGPD, lido em conjunto com o artigo 5º do RGPD. Embora não existam critérios que visem diretamente o cumprimento do artigo 6.º do RGPD, dado que o responsável pelo tratamento é responsável pela licitude do tratamento, os critérios visam assegurar que os subcontratantes requerentes concebem as operações de tratamento a certificar de forma a facilitar a aplicação pelos responsáveis pelo tratamento dos princípios de proteção de dados do artigo 5.º do RGPD, incluindo o princípio da licitude do tratamento.

2.4 Obrigações gerais dos responsáveis pelo tratamento e dos subcontratantes

11. Os critérios refletem a relação entre o subcontratante e o responsável pelo tratamento. Em particular, os critérios preveem a obrigação de o subcontratante ter em vigor um modelo de acordo de tratamento de dados com o responsável pelo tratamento, que inclua todos os requisitos do artigo 28.º do RGPD (secção 1.2 dos critérios).

12. Os critérios exigem que os requerentes nomeiem um responsável pela proteção de dados (EPD) em conformidade com o artigo 37.º do RGPD e apresentem uma prova da nomeação do EPD (por exemplo, certificado de nomeação). Os critérios verificam se o EPD cumpre os requisitos previstos nos artigos 37.º a 39.º (conjunto 1, secção 1.1, dos critérios).

13. Os critérios verificam o conteúdo dos registos das atividades de tratamento em conformidade com o artigo 30.º do RGPD (conjunto 1, secção 1.1, dos critérios).

2.5 Direitos dos titulares dos dados

14. 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 (conjunto 3 dos critérios).

2.6 Riscos para os direitos e liberdades

15. Os critérios exigem que o subcontratante esteja ciente dos possíveis riscos para os direitos e liberdades das pessoas singulares no que diz respeito ao tratamento de dados envolvidos no ToE. Se

o tratamento de dados pessoais for suscetível de resultar num elevado risco para os direitos e liberdades das pessoas singulares, vários critérios asseguram que o requerente demonstra que os requisitos do artigo 35.º do RGPD estão preenchidos em conformidade com o artigo 35.º do RGPD (secção 1.2.2 dos critérios, requisito n.º 6, secção 1.3.2 dos critérios, secção 1.3.3 dos critérios, secção 2.1.5.1 dos critérios, secção 2.1.5.9 dos critérios).

2.7 Medidas técnicas e organizativas que garantam a proteção

16. 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 aplicação de medidas técnicas para implementar a proteção de dados desde a conceção e por defeito, em conformidade com os artigos 25.º e 32.º do RGPD (secção 1.5 dos critérios, secção 2.1 dos critérios/outros documentos).

17. 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 do RGPD (secção 1.2.2 dos critérios, requisito n.º 6).

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

18. 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 1.4 dos critérios).

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

19. 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 4 dos critérios exige que o requerente cumpra a legislação nacional aplicável e a legislação setorial relevante em matéria de proteção de dados. Além disso, o Comité entende que um «relatório de conformidade com a legislação nacional», o qual avalie, em particular, a conformidade do alvo da avaliação com os requisitos da legislação nacional aplicável em matéria de proteção de dados, deve ser elaborado por peritos jurídicos, desde que estes tenham demonstrado o nível necessário de conhecimentos especializados na legislação nacional aplicável.

CONCLUSÕES/RECOMENDAÇÕES

20. Em conclusão, o CEPD considera que o projeto de critérios de certificação é coerente com o RGPD e aprova-o 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).

21. O CEPD regista o mecanismo de certificação «Catálogo de critérios EuroPriSe para a certificação das operações de tratamento pelos subcontratantes» no registo público dos mecanismos de certificação e dos selos e marcas de proteção de dados, nos termos do artigo 42.º, n.º 8.

OBSERVAÇÕES FINAIS

22. A autoridade de controlo alemã é a destinatária do presente parecer, que 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
Anu Talus