Parecer 14/2026 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, do RGPD

Adotado em 15 abril 2026

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 «EEE»), nomeadamente o anexo XI e o Protocolo n.º 37, com a redação que lhe foi dada pela Decisão do Comité Misto do EEE n.º 154/2018, de 6 de julho de 2018[1],

Tendo em conta os artigos 10.º e 22.º do seu Regulamento Interno,

Considerando o seguinte:

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 promovem, 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») e de 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. Além disso, a criação de procedimentos de certificação pode reforçar a transparência e permitir que os titulares dos dados avaliem o nível de proteção de dados dos produtos e serviços pertinentes.
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. Caso 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 disponibilizar o procedimento de certificação em todos os Estados-Membros. Neste caso, a principal função do CEPD consiste em assegurar a aplicação coerente do RGPD, através do procedimento de controlo da coerência a que se referem os artigos 63.º, 64.º e 65.º do RGPD. Neste contexto, nos termos do artigo 64.º, n.º 2, do RGPD, o CEPD aprova os critérios de certificação.
4. O presente parecer visa assegurar a aplicação coerente do RGPD, nomeadamente pelas AC, pelos responsáveis pelo tratamento e pelos subcontratantes, à luz dos elementos essenciais que os procedimentos de certificação são obrigados a estabelecer. 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 respetiva adenda intitulada *Guidance on certification criteria assessment* [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 abordado individualmente e não prejudica a avaliação de qualquer outro procedimento de certificação.

[1] As referências a «Estados-Membros» ao longo do presente documento devem ser entendidas como referências a «Estados do EEE».

6. Os procedimentos de certificação devem permitir que os responsáveis pelo tratamento e os subcontratantes demonstrem a conformidade com o RGPD. Por conseguinte, os respetivos critérios devem refletir adequadamente os requisitos e princípios relativos à proteção de dados pessoais previstos no RGPD e contribuir para a sua aplicação coerente.

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

8. Consequentemente, as certificações devem acrescentar valor aos responsáveis pelo tratamento e aos subcontratantes, ao contribuir para a aplicação de medidas organizativas e técnicas normalizadas e especificadas que, comprovadamente, facilitem e melhorem 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 dos sistemas para elaborar procedimentos de certificação que, ao aumentar a transparência, 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.

10. O CEPD recorda que as certificações são instrumentos voluntários de responsabilização e que a adesão a um procedimento de certificação não reduz a responsabilidade dos responsáveis pelo tratamento ou dos subcontratantes em relação à conformidade com o RGPD, nem impede as autoridades de controlo de exercerem as suas funções e poderes nos termos do RGPD e da legislação nacional pertinente.

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

12. O presente parecer do CEPD centra-se exclusivamente nos critérios de certificação. O CEPD pode exigir informações de alto nível sobre os métodos de avaliação, a fim de poder avaliar exaustivamente a auditabilidade dos critérios no contexto do seu parecer. Todavia, tal não abrange qualquer tipo de aprovação desses métodos de avaliação.

13. O parecer do CEPD é aprovado 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 subsequente à decisão da presidente e da autoridade de controlo competente de que o processo está completo. Por decisão da presidente, este prazo pode ser prorrogado por mais seis semanas, em virtude da complexidade do assunto em apreço. Se o parecer do CEPD concluir que não é possível aprovar os critérios em causa, a AC pode voltar a apresentar os critérios para aprovação depois de as preocupações expressas no parecer inicial do CEPD serem abordadas,

Adotou o seguinte parecer:

1 Resumo dos factos

14. Em conformidade com o artigo 42.º, n.º 5, do RGPD e com as diretrizes, o European Center for Certification and Privacy (a seguir designado por «proprietário do sistema») elaborou os critérios de certificação Europrivacy (versão 82) (a seguir designados por «critérios de certificação»).

15. Em 29 de janeiro de 2026, a autoridade de controlo do Luxemburgo (a seguir designada por «AC do Luxemburgo») apresentou os critérios de certificação Europrivacy (versão 82) ao CEPD para aprovação nos termos do artigo 64.º, n.º 2, do RGPD.

16. A decisão de que o processo está completo foi tomada em 31 de março de 2026.

17. O CEPD recorda que aprovou os critérios de certificação Europrivacy (versão 60) em 10 de outubro de 2022, através da emissão do Parecer 28/2022 do CEPD, enquanto Selo Europeu de Proteção de Dados nos termos do artigo 42.º, n.º 5, do RGPD («parecer anterior do CEPD»).

18. O presente parecer aborda a versão alterada dos critérios de certificação Europrivacy (versão 82). Em primeiro lugar, o Comité observa que, na referida versão dos critérios de certificação, atualmente apresentada ao CEPD, o âmbito de aplicação foi alargado de modo a incluir os requerentes sujeitos ao artigo 3.º, n.º 2, do RGPD e, a este respeito, foi introduzido um critério sobre potenciais conflitos de legislação de países terceiros. Além disso, o Comité observa que alguns dos critérios de certificação que o CEPD aprovou em 2022 foram ajustados, aperfeiçoados e/ou clarificados na versão alterada dos critérios de certificação Europrivacy (versão 82). Essas alterações dizem respeito, nomeadamente, ao seguinte: a designação de um representante no EEE e a cooperação com os pedidos apresentados pelas autoridades de proteção de dados (APD) competentes no EEE; o relatório de avaliação do cumprimento das obrigações nacionais («NOCAR»), o tratamento posterior, as garantias que acompanham o tratamento de categorias especiais de dados pessoais, os direitos dos titulares dos dados, a contratação de subcontratantes ulteriores, o tratamento de violações de dados, a avaliação dos riscos para o tratamento de dados, bem como a política e os requisitos de segurança.

19. O CEPD sublinha que a alteração dos critérios de certificação já aprovados em 2022 afetará as certificações emitidas até à data, bem como os processos de certificação em curso. Por conseguinte, deve ser gerido de forma adequada e transparente um período de transição entre os Selos Europeus de Proteção de Dados emitidos de acordo com os critérios de certificação aprovados por meio do parecer anterior do CEPD (versão 60) e os emitidos de acordo com os critérios de certificação (versão 82) avaliados no presente parecer. A este respeito, o Comité entende, com base na documentação que o proprietário do sistema facultou, que todos os processos de certificação em curso devem ser concluídos até ao final de 2026 e que, após esse momento, os critérios de certificação aprovados por meio do parecer anterior do CEPD (versão 60) deixarão de ser utilizados para emitir novos certificados. Os certificados emitidos até à data permanecerão válidos até ao final do respetivo período de validade de três anos e serão renovados segundo os critérios de certificação (versão 82). Por conseguinte, após o final de 2029, os critérios de certificação aprovados por meio do parecer anterior do CEPD (versão 60) serão totalmente substituídos pelos critérios de certificação (versão 82). Além disso, o proprietário do sistema disponibilizará ao público as informações relativas a este plano de transição. Podem ser necessários alguns ajustamentos da acreditação realizada pelos organismos de certificação, mas o presente parecer não aborda esta questão, pois não é da competência do CEPD.

20. O sistema geral de certificação Europrivacy não se destina a ser utilizado enquanto instrumento para as transferências nos termos do artigo 42.º, n.º 2, e do artigo 46.º, n.º 2, alínea f), do RGPD. Em 29 de janeiro de 2026, a AC do Luxemburgo apresentou igualmente ao CEPD, para aprovação nos termos do artigo 64.º, n.º 2, do RGPD, um conjunto adicional de critérios de certificação (*The Europrivacy Certification Scheme Extension for Certifying Data Importers under Article 46*, extensão do sistema de certificação Europrivacy para a certificação de importadores de dados nos termos do artigo 46.º), cujo âmbito abrange os responsáveis pelo tratamento e os subcontratantes localizados fora do EEE que não estão

diretamente sujeitos ao RGPD nos termos do artigo 3.º, n.º 2, do RGPD, mas que tratam dados pessoais recebidos de outro responsável pelo tratamento ou subcontratante sujeito ao RGPD. Relativamente a este conjunto de critérios de certificação destinados a ser utilizados enquanto instrumento para as transferências nos termos do artigo 46.º, n.º 2, alínea f), do RGPD, o CEPD adotou o Parecer 15/2026.

2 Avaliação

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

22. No contexto do presente parecer e a fim de aprovar os critérios de certificação, o CEPD avaliou os controlos e verificações preliminares do pedido e do alvo da avaliação (A), os critérios fundamentais do RGPD do Europrivacy (G), os controlos e verificações das medidas tecnológicas e organizativas (T), fornecidos juntamente com os critérios de certificação.

23. Além disso, o Comité observa, a este respeito, que as «verificações e controlos contextuais complementares»[2], facultados juntamente com os critérios de certificação aprovados com o parecer anterior do CEPD (versão 60), destinados a assegurar que o tratamento de dados envolvido no alvo da avaliação («ToE») cumpre os requisitos específicos por domínio e por tecnologia[3], não foram aprovados pelo CEPD no seu parecer anterior e que essas «verificações e controlos contextuais complementares» já não estão presentes na documentação atualizada fornecida no contexto do presente parecer.

24. O Comité observa, conforme clarificado nas definições do sistema, que as referências a «autoridades de proteção de dados competentes» constantes do sistema têm o significado de autoridades de proteção de dados no EEE[4].

25. No que diz respeito à definição de «legislação de países terceiros», o Comité entende que se refere à legislação aplicável ao requerente e/ou aos dados pessoais tratados no alvo da avaliação, na medida em que essa legislação não imponha limitações aos direitos de proteção de dados que vão além do necessário e proporcionado numa sociedade democrática para salvaguardar um dos objetivos enumerados no artigo 23.º, n.º 1, do RGPD, seja proporcionada ao objetivo visado, respeite a essência do direito à proteção de dados e preveja medidas específicas para salvaguardar os direitos e interesses fundamentais dos titulares dos dados.

2.1 Âmbito do procedimento de certificação e alvo da avaliação

[2] O CEPD não aprovou as «verificações e controlos contextuais complementares» no seu parecer anterior.
[3] Parecer anterior do CEPD, n.os 7 e 8.
[4] Ver a definição de «AC competente» prevista nos critérios Europrivacy: «autoridade competente em matéria de proteção de dados» refere-se às autoridades responsáveis pela proteção de dados no EEE. De um modo geral, refere-se às autoridades nacionais de proteção de dados que possuem competência para impor a conformidade dos dados pessoais tratados pelo alvo da avaliação. No caso de uma certificação no âmbito do RGPD emitida a um importador de dados nos termos do artigo 46.º do RGPD, a autoridade de proteção de dados competente é a do exportador de dados no EEE, exceto para apresentar uma reclamação, caso em que qualquer autoridade do EEE é competente.

26. O CEPD recorda[5] que o sistema 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.

27. O Comité congratula-se com o facto de, na documentação relacionada com o âmbito deste sistema de certificação facultada pela AC do Luxemburgo, o sistema Europrivacy alterado se aplicar a: **i)** responsáveis pelo tratamento e subcontratantes estabelecidos na União Europeia (UE) ou no Espaço Económico Europeu (EEE), **ii)** responsáveis pelo tratamento e subcontratantes estabelecidos fora do EEE que estejam sujeitos ao RGPD nos termos do artigo 3.º, n.º 2, do RGPD, quer porque disponibilizam bens ou serviços a titulares de dados no EEE, quer porque controlam o comportamento de titulares de dados no EEE[6]. A aplicabilidade dos critérios é definida de acordo com a função e as responsabilidades do requerente.

28. No que diz respeito aos requerentes abrangidos pelo artigo 3.º, n.º 2, do RGPD localizados num país terceiro que não estejam sujeitos a uma decisão de adequação que abranja o ToE, o critério A.2.1.6 define as condições a cumprir ao definir o ToE durante a análise do seu pedido de certificação. Em especial, antes de considerar uma auditoria de certificação, exige que o organismo de certificação verifique se o requerente está em condições de demonstrar que a legislação e as práticas nacionais do país terceiro não o impedem de cumprir os requisitos de certificação. Se tal não for o caso, o processo de certificação será interrompido durante a fase de pedido.

29. O Comité observa que um responsável pelo tratamento de dados pode apresentar ao processo de certificação Europrivacy um ToE sujeito a responsabilidade conjunta pelo tratamento (critério A.2.1.5). Caso o ToE esteja sujeito a responsabilidade conjunta pelo tratamento, o Comité gostaria de sublinhar que o organismo de certificação acreditado terá de conduzir cuidadosamente o processo de pedido, a fim de assegurar que o ToE é significativo e que o requerente é plenamente responsável pela conformidade do ToE com todas as obrigações decorrentes do RGPD que o sistema 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 pelo cumprimento das obrigações decorrentes do RGPD pode — dependendo do contexto das atividades de tratamento do ToE — impedir o requerente de cumprir os critérios de certificação.

2.2 Operações de tratamento

30. Tal como o CEPD observou no seu parecer anterior, os critérios de certificação abordam as componentes pertinentes das operações de tratamento (dados, sistemas e tratamento) no que diz respeito ao âmbito geral do sistema de certificação. Em especial, os critérios de certificação permitem identificar categorias especiais de dados, conforme definidas no artigo 9.º do RGPD (secção G.2 dos critérios sobre o tratamento de dados especiais).

2.3 Licitude do tratamento

31. Conforme o CEPD declarou no seu parecer anterior sobre os critérios de certificação já aprovados (versão 60), os critérios de certificação exigem a verificação da licitude do tratamento de dados para cada operação de tratamento individual no ToE, bem como a

[5] Parecer anterior do CEPD, n.º 6.
[6] Ver Diretrizes do CEPD sobre o âmbito de aplicação territorial do RGPD (artigo 3.º), versão 2.0, adotadas em 12 de novembro de 2019, secção 2.

verificação dos requisitos de uma base jurídica, como definido no artigo 6.º do RGPD (secção G.1 dos critérios sobre a licitude do tratamento dos dados). Em especial, o Comité congratula-se com o facto de os critérios de certificação atualizados exigirem que o consentimento dos titulares dos dados abranja cada finalidade para a qual o tratamento é efetuado e que a retirada do consentimento não prejudique o titular dos dados.

32. Além disso, conforme referido no parecer anterior do CEPD, os critérios de certificação exigem a verificação dos requisitos específicos das condições em que, nos termos do artigo 9.º, n.º 2, do RGPD, é permitido o tratamento de categorias especiais de dados pessoais (secção G.2.1 dos critérios sobre o tratamento de dados especiais) e a previsão de limitações e garantias adicionais para os direitos e liberdades do titular dos dados. Os critérios de certificação exigem igualmente a verificação dos requisitos das condições definidas no artigo 10.º do RGPD para o tratamento de dados pessoais relacionados com condenações penais e infrações (secção G.2.2 dos critérios), se for caso disso. A este respeito, o Comité congratula-se igualmente com o facto de os critérios de certificação atualizados (critério G.2.1.3 sobre as garantias adicionais para o tratamento de categorias especiais de dados pessoais) exigirem igualmente que o requerente disponha de limitações e garantias adicionais, adaptadas à natureza específica dos dados e aos riscos correspondentes, caso o tratamento envolva categorias especiais de dados pessoais.

33. Adicionalmente, no que diz respeito aos requerentes abrangidos pelo artigo 3.º, n.º 2, do RGPD localizados num país terceiro que não estejam sujeitos a uma decisão de adequação que abranja o ToE, os critérios de certificação atualizados exigem que o requerente apresente um relatório elaborado por um perito jurídico que conclua que a legislação e as práticas nacionais do país terceiro não impedem o cumprimento das suas obrigações em matéria de proteção de dados nos termos do RGPD. Da mesma forma, a avaliação deve incluir a conclusão de que a legislação nacional do país terceiro não impõe limitações aos direitos de proteção de dados que vão além do necessário e proporcionado numa sociedade democrática para salvaguardar um dos objetivos enumerados no artigo 23.º, n.º 1, do RGPD, é proporcionada ao objetivo visado, respeita a essência do direito à proteção de dados e prevê medidas específicas para salvaguardar os direitos e interesses fundamentais dos titulares dos dados. Tem igualmente de ser revista sempre que alterações regulamentares ou organizativas sejam suscetíveis de prejudicar o cumprimento dos critérios, ou afetar o ToE ou os direitos dos titulares dos dados, e seja necessário informar o organismo de certificação (critério G.1.1.5).

34. Neste contexto, os critérios de certificação atualizados clarificam, nas orientações, que se um requerente estiver estabelecido fora do EEE e beneficiar de uma decisão de adequação pertinente para o tratamento efetuado no ToE, o cumprimento deste requisito pode ser demonstrado através de um relatório simplificado. De acordo com esses critérios, o referido relatório deve ter avaliado se a decisão de adequação está em vigor e documentado as razões pelas quais o ToE é abrangido pelo âmbito de aplicação da decisão de adequação (critério G.1.1.5, letra F).

2.4 Princípios do tratamento de dados

35. O CEPD recorda que os critérios de certificação abordam adequadamente os princípios da proteção de dados nos termos do artigo 5.º do RGPD. Em especial, os critérios de certificação atualizados alargam e aprofundam o princípio da limitação das finalidades, ao incluir um critério específico que exige a demonstração de que os dados pessoais não são objeto de tratamento posterior de uma forma incompatível com essas finalidades, que qualquer tratamento posterior deve ser avaliado separadamente como lícito, e que é realizada e

devidamente documentada uma avaliação da compatibilidade das finalidades para o tratamento posterior dos dados (critério G.1.1.6).

2.5 Obrigações gerais dos responsáveis pelo tratamento e dos subcontratantes

36. O CEPD recorda que os critérios de certificação[7] refletem as obrigações do responsável pelo tratamento nos termos do artigo 24.º do RGPD (secção G.4 sobre a responsabilidade do responsável pelo tratamento) e 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 sobre os subcontratantes ou subcontratantes ulteriores).

37. Além disso, o Comité congratula-se com o aditamento realizado, segundo o qual os critérios de certificação exigem que o requerente, nos termos do artigo 3.º, n.º 2, do RGPD, designe um gabinete ou um representante no EEE, de acordo com o artigo 27.º do RGPD, cujos dados de contacto estejam disponíveis no sítio Web do requerente (critério G.4.1.4). O Comité toma nota destes critérios de certificação e recorda que nem sempre constitui uma obrigação imperativa para os responsáveis pelo tratamento e os subcontratantes nos termos do RGPD, pelo que devem ser tidas em conta as condições estabelecidas no artigo 27.º do RGPD.

38. Além disso, o CEPD observa, conforme referido no seu parecer anterior, que os critérios de certificação exigem que todos os requerentes nomeiem um encarregado da proteção de dados (EPD), mesmo caso o requerente não seja 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 sobre o encarregado da proteção de dados).

39. Da mesma forma, os critérios de certificação exigem a verificação do conteúdo dos registos de atividades de tratamento, em conformidade com o artigo 30.º do RGPD (secção G.5.3 dos critérios sobre os registos de atividades de tratamento). A este respeito, o Comité congratula-se com o facto de, para os requerentes abrangidos pelo artigo 3.º, n.º 2, do RGPD, os critérios de certificação atualizados exigirem que cooperem com os pedidos apresentados pelas APD competentes no EEE e lhes facultem, mediante pedido, o registo das atividades de tratamento (critério G.5.3.5).

40. Na mesma ordem de ideias, o CEPD observa que foram incluídos alguns critérios de certificação adicionais relativos à contratação de subcontratantes ulteriores para os requerentes que atuam como responsáveis pelo tratamento ou como subcontratantes (secção G.5.1.2 sobre a contratação de subcontratantes ulteriores). Esta distinção permite refletir melhor a separação de funções e responsabilidades entre os intervenientes na cadeia de tratamento.

2.6 Direitos dos titulares dos dados

41. Tal como no seu parecer anterior, o CEPD recorda que os critérios de certificação abordam adequadamente o direito do titular dos dados à informação, em conformidade com o capítulo III do RGPD, e exigem a adoção das respetivas medidas[8]. Os critérios de certificação 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

[7] Parecer anterior do CEPD, n.º 16.
[8] Parecer anterior do CEPD, n.º 19.

correções, apagamento ou limitações (secção G.3 dos critérios sobre os direitos dos titulares dos dados).

42. Além disso, o CEPD congratula-se com as melhorias introduzidas nos critérios de certificação no que diz respeito às informações a facultar aos titulares dos dados (secção G.3.2 sobre as informações a facultar quando os dados pessoais são recolhidos junto do titular dos dados e secção G.3.3 sobre as informações a facultar quando os dados pessoais não foram obtidos junto do titular dos dados), às modalidades de comunicação aos titulares dos dados[9] e de exercício dos direitos dos titulares dos dados[10] (secção G.3.1 sobre a transparência das informações, a comunicação e as modalidades de exercício dos direitos dos titulares dos dados), bem como ao direito de acesso (secção G.3.4 sobre o direito de acesso do titular dos dados), ao apagamento [secção G.3.6 sobre o direito de apagamento («direito de ser esquecido»)], à limitação do tratamento (critério G.3.7.1 sobre o direito à limitação do tratamento), à obrigação de notificação no que diz respeito à retificação ou ao apagamento dos dados pessoais ou à limitação do tratamento (critério G.3.8.2 sobre o dever de informar os titulares dos dados sobre os destinatários, se tal for solicitado), ao direito de oposição (secção G.3.10 sobre o direito de oposição) e ao direito de não ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis (secção G.3.11 sobre o direito de não ser sujeito a decisões individuais automatizadas, incluindo a definição de perfis).

2.7 Riscos para os direitos e liberdades

43. O CEPD já declarou, no seu parecer anterior, que os critérios de certificação exigem a avaliação do risco para os direitos e liberdades das pessoas singulares decorrentes do tratamento de dados envolvido no ToE, em conformidade com o artigo 35.º do RGPD [secção G.8 dos critérios sobre a obrigação de avaliar se é necessária uma avaliação de impacto sobre a proteção de dados (AIPD)][11].

44. O CEPD congratula-se com as alterações introduzidas nos critérios de certificação, a fim de prever que o requerente deve ter avaliado, com recurso a uma metodologia repetível, os riscos apresentados pelo tratamento que possam afetar os direitos e liberdades das pessoas singulares (secção G.6.2.4 sobre a avaliação dos riscos para o tratamento de dados).

45. Além disso, o CEPD congratula-se com os novos aditamentos e pormenores que os critérios de certificação introduziram. Por exemplo, o CEPD toma nota do aditamento ao processo de AIPD relativo às situações em que o requerente não é obrigado a realizar uma AIPD (secção G.8.2.1 sobre os requisitos do processo de AIPD).

2.8 Medidas técnicas e organizativas que garantam a proteção

46. Conforme referido no parecer anterior do CEPD, os critérios de certificação 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

[9] Por exemplo, o critério G.3.1.1 sobre o dever de informar numa linguagem clara desenvolve mais pormenorizadamente as informações sobre o tratamento de dados facultadas pelo requerente ao titular dos dados, que incluem agora que i) devem ser facultadas por escrito ou por outros meios, ii) devem estar disponíveis na(s) língua(s) oficial(ais) do requerente e iii) devem estar disponíveis na língua dos titulares dos dados visados.

[10] Por exemplo, o critério G.3.1.3 sobre a garantia de uma gestão e registo adequados dos direitos dos titulares dos dados exige agora que o requerente disponha de um procedimento ou de um mecanismo para confirmar também a receção do pedido ao titular dos dados e para conservar registos também dos pedidos dos titulares dos dados com a data de receção.

[11] Parecer anterior do CEPD, n.º 20.

defeito, em conformidade com os artigos 25.º e 32.º do RGPD (secção G.6 dos critérios sobre a proteção de dados desde a conceção e por defeito, e a segurança do tratamento, secção G.6.2 dos critérios sobre a segurança do tratamento e secção relativa aos critérios T)[12]. A este respeito, o Comité congratula-se com o facto de os critérios de certificação alterados aprofundarem (secção G.6.1.2 sobre a minimização dos dados por defeito) as regras e os procedimentos que o requerente deve aplicar para cumprir esses critérios.

47. Conforme sublinhado no parecer anterior do CEPD, os critérios de certificação 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 sobre a gestão de violações de dados).

48. A este respeito, o Comité observa que os critérios de certificação foram melhorados e desenvolvidos. Mais especificamente, os critérios de certificação incluem agora uma lista mais pormenorizada (secção G.7.1.1 sobre o dever de documentar as violações de dados) das informações que o requerente deve documentar quando ocorre uma violação de dados (por exemplo, as categorias de dados pessoais que são ou podem ser afetadas, o número aproximado de titulares de dados que são ou podem ser afetados, as categorias e o número aproximado de registos de dados pessoais a que diz respeito ou pode dizer respeito, e as consequências prováveis da violação de dados pessoais).

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

49. Conforme o Comité afirmou no seu parecer anterior, os critérios de certificação exigem a identificação de todas as transferências de dados pessoais para países terceiros e organizações internacionais envolvidas no ToE e 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 sobre as transferências de dados pessoais para países terceiros ou organizações internacionais).

50. O CEPD reconhece que, no caso dos requerentes abrangidos pelo artigo 3.º, n.º 2, do RGPD, estes critérios de certificação serão aplicáveis no caso de transferências de dados pessoais envolvidos no ToE para entidades localizadas tanto no mesmo país terceiro em que o requerente está localizado como num país terceiro diferente.

51. Além disso, o Comité congratula-se com o facto de os critérios de certificação relativos às transferências de dados pessoais terem sido agora aprofundados e preverem de forma mais clara as obrigações do requerente nesta matéria (secção G.10.1 sobre as obrigações gerais aplicáveis às transferências internacionais de dados pessoais para países terceiros ou organizações internacionais).

[12] Parecer anterior do CEPD, n.º 21.

3 Critérios adicionais para um Selo Europeu de Proteção de Dados

52. De acordo com as diretrizes, a avaliação deve incluir a questão de saber se os critérios são capazes de ter em conta a legislação ou os cenários de proteção de dados dos Estados-Membros. Conforme afirmado no parecer anterior do CEPD, a secção G.1.1.3 dos critérios de certificação exige que o requerente apresente a avaliação em causa num relatório nacional de avaliação do cumprimento das obrigações (NOCAR). Esse 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.

53. O Comité congratula-se com os ajustamentos efetuados ao NOCAR nos critérios atualizados (secção G.1.1.3 sobre a avaliação do cumprimento das obrigações nacionais). Em especial, esclarece-se agora que o requerente deve documentar num relatório de avaliação do cumprimento das obrigações nacionais (NOCAR) a avaliação efetuada sobre a conformidade do tratamento de dados com as obrigações nacionais complementares do EEE relacionadas com a proteção de dados pessoais aplicáveis ao requerente. Em especial, o NOCAR deve conter, nomeadamente, uma identificação clara do ToE que foi avaliado, a lista das obrigações nacionais complementares identificadas em matéria de proteção de dados do EEE aplicáveis ao ToE, bem como a avaliação da conformidade do ToE com as obrigações nacionais complementares identificadas em matéria de proteção de dados do EEE. O Comité considera que, caso o requerente esteja estabelecido fora do EEE e sujeito ao artigo 3.º, n.º 2, do RGPD, as obrigações nacionais em matéria de proteção de dados do EEE aplicáveis ao ToE devem ser determinadas com base na localização dos titulares dos dados a quem o requerente disponibiliza bens ou serviços ou cujo comportamento está sob controlo.

4 Conclusões/Recomendações

54. 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).

55. O CEPD considera que os critérios de certificação fazem parte integrante do sistema de certificação e 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, do RGPD.

5 Observações finais

56. O presente parecer é dirigido à AC do Luxemburgo 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

Anu Talus