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

Versão 3.0

4 de junho de 2019

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

Adotadas

Histórico das versões

Versão 3.0	4 de junho de 2019	Inclusão do anexo 2 (versão 2.0 do anexo 2, adotada em 4 de junho de 2019 após consulta pública)
Versão 2.1	9 de abril de 2019	Aprovação de uma retificação às Diretrizes (ponto 45)
Versão 2.0	23 de janeiro de 2019	Adoção das Diretrizes após consulta pública — Na mesma data, o anexo 2 (versão 1.0) foi adotado para consulta pública
Versão 1.0	25 de maio de 2018	Adoção das Diretrizes para consulta pública

Índice

O Comité Europeu para a Proteção de Dados

Tendo em conta o artigo 70.º, n.º 1, alínea e), 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 EEE, nomeadamente o seu 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,

Tendo em conta o artigo 12.º e o artigo 22.º do seu regulamento interno, de 25 de maio de 2018,

Tendo em conta os resultados da consulta pública sobre as Diretrizes que tiveram lugar entre 30 de maio de 2018 e 12 de julho de 2018, e sobre o anexo 2, que teve lugar entre 15 de fevereiro e 29 de março de 2019, em conformidade com o artigo 70.º, n.º 4, do RGPD.

ADOTOU AS SEGUINTES DIRETRIZES:

1 INTRODUÇÃO

1. O Regulamento Geral sobre a Proteção de Dados (Regulamento (UE) 2016/679, «o RGPD» ou «o regulamento») prevê um quadro modernizado, de responsabilização e de respeito pelos direitos fundamentais para a proteção de dados na Europa. Um conjunto de medidas que facilitam o cumprimento das disposições do RGPD são fundamentais para este novo quadro. Entre estas, incluem-se requisitos obrigatórios em circunstâncias específicas (incluindo a nomeação de responsáveis pela proteção de dados e a realização de avaliações de impacto sobre a proteção de dados) e medidas voluntárias, como códigos de conduta e procedimentos de certificação.
2. Antes da adoção do RGPD, o Grupo de Trabalho do artigo 29.º concluiu que a certificação poderia desempenhar um papel importante no quadro de responsabilidade em matéria de proteção de dados1. Para que a certificação possa fornecer provas fiáveis da conformidade em matéria de proteção de dados, devem ser estabelecidas regras claras que estabeleçam requisitos para a concessão da certificação2. O artigo 42.º do RGPD constitui a base jurídica para a elaboração dessas regras.
3. O artigo 42.º, n.º 1, do RGPD dispõe o seguinte:

   «Os Estados-Membros, as autoridades de controlo, o Comité [Europeu para a Proteção de Dados] e a Comissão promovem, em especial ao nível da União, a criação de procedimentos de certificação em matéria de proteção de dados, bem como selos e marcas de proteção de

[1] Grupo de Trabalho do artigo 29.º, Parecer 3/2010 sobre o princípio da responsabilidade, WP173, 13 de julho de 2010, pontos 69-71.
[2] Parecer do Grupo de Trabalho do artigo 29.º 3.º/2010 sobre o princípio da responsabilidade (WP173), ponto 69.

dados, para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente regulamento. Serão tidas em conta as necessidades específicas das micro, pequenas e médias empresas.»

4. Os procedimentos de certificação3 podem melhorar a transparência face aos titulares dos dados, mas também nas relações entre empresas, por exemplo entre responsáveis pelo tratamento e subcontratantes. O considerando 100 do RGPD estabelece que a criação de procedimentos de certificação pode reforçar a transparência e o cumprimento do regulamento e permitir que os titulares dos dados avaliem o nível de proteção de dados proporcionado pelos produtos e serviços em causa4.

5. O RGPD não introduz um direito ou uma obrigação de certificação para os responsáveis pelo tratamento e subcontratantes; nos termos do artigo 42.º, n.º 3, a certificação é um processo voluntário para ajudar a demonstrar a conformidade com o RGPD. Os Estados-Membros e as autoridades de controlo são convidados a incentivar a criação de procedimentos de certificação e determinarão a participação das partes interessadas no processo de certificação e no ciclo de vida.

6. Além disso, a adesão ou não a procedimentos de certificação aprovados é um fator que as autoridades de supervisão têm de considerar como um fator agravante ou atenuante ao decidir sobre a aplicação de uma coima e ao decidir sobre o montante desta (artigo 83.º, n.º 2, alínea j))5.

1.1 Âmbito de aplicação das orientações

7. As presentes diretrizes têm um âmbito de aplicação limitado; não são um manual de procedimento de certificação em conformidade com o RGPD. O principal objetivo destas orientações é identificar os requisitos e critérios gerais que possam ser relevantes para todos os tipos de procedimentos de certificação aprovados em conformidade com os artigos 42.º e 43.º do RGPD. Para o efeito, as orientações:

   - examinam a fundamentação da certificação como instrumento de responsabilização;
   - explicam os conceitos fundamentais das disposições de certificação constantes dos artigos 42.º e 43.º; e
   - esclarecem o âmbito do que pode ser certificado nos termos dos artigos 42.º e 43.º e o objetivo da certificação;
   - contribuem para que o resultado da certificação seja relevante, inequívoco, tão reprodutível quanto possível e comparável, independentemente do certificador (comparabilidade).

[3] As presentes orientações designarão coletivamente os procedimentos de certificação e os selos e marcas de proteção de dados como «procedimentos de certificação», ver ponto 1.3.2.
[4] O considerando 100 estabelece que a criação de procedimentos de certificação deverá ser encorajada a fim de «reforçar a transparência e o cumprimento do [...] regulamento, [para permitir] aos titulares avaliar rapidamente o nível de proteção de dados proporcionado pelos produtos e serviços em causa».
[5] Ver Grupo de Trabalho do artigo 29.º, Diretrizes de aplicação e fixação de coimas para efeitos do Regulamento (UE) 2016/679 (WP 253).

8. O RGPD prevê várias formas de os Estados-Membros e as autoridades de controlo aplicarem os artigos 42.º e 43.º. As orientações fornecem conselhos sobre a interpretação e a aplicação das disposições dos artigos 42.º e 43.º e ajudarão os Estados-Membros, as autoridades de controlo e os organismos nacionais de acreditação a estabelecer uma abordagem mais coerente e harmonizada para a aplicação dos procedimentos de certificação em conformidade com o RGPD.

9. Os conselhos contidos nas orientações serão pertinentes para:

   - as autoridades de controlo competentes e o Comité Europeu para a Proteção de Dados («o CEPD»), aquando da aprovação dos critérios de certificação nos termos do artigo 42.º, n.º 5, do artigo 58.º, n.º 3, alínea f), e do artigo 70.º, n.º 1, alínea o);
   - os organismos de certificação, na elaboração e revisão dos critérios de certificação antes da apresentação à autoridade de controlo competente para aprovação, em conformidade com o artigo 42.º, n.º 5;
   - o CEPD, ao aprovar um selo europeu de proteção de dados, nos termos do artigo 42.º, n.º 5, e do artigo 70.º, n.º 1, alínea o);
   - as autoridades de controlo, na elaboração dos seus próprios critérios de certificação;
   - a Comissão Europeia, que está habilitada a adotar atos delegados a fim de especificar os requisitos a ter em conta para os procedimentos de certificação nos termos do artigo 43.º, n.º 8;
   - o CEPD, ao dar parecer à Comissão Europeia a respeito dos requisitos de certificação em conformidade com o artigo 70.º, n.º 1, alínea q), e o artigo 43.º, n.º 8;
   - os organismos nacionais de acreditação, que terão de ter em conta os critérios de certificação com vista à acreditação dos organismos de certificação, em conformidade com a norma EN-ISO/IEC 17065/2012 e os requisitos adicionais nos termos do artigo 43.º; e
   - os responsáveis pelo tratamento e subcontratantes, ao definirem a sua própria estratégia de conformidade com o RGPD e considerarem a certificação como um meio para demonstrar a conformidade.

10. O CEPD publicará orientações separadas para abordar a identificação de critérios para a aprovação de procedimentos de certificação como instrumentos de transferência para países terceiros ou organizações internacionais, em conformidade com o artigo 42.º, n.º 2.

1.2 Objetivo da certificação ao abrigo do RGPD

11. O artigo 42.º, n.º 1, prevê a criação de procedimentos de certificação «para efeitos de comprovação da conformidade das operações de tratamento de responsáveis pelo tratamento e subcontratantes com o presente regulamento».

12. O RGPD exemplifica o contexto em que os procedimentos de certificação aprovados podem ser utilizados como um elemento para demonstrar o cumprimento das obrigações dos responsáveis pelo tratamento e dos subcontratantes no que diz respeito, nomeadamente:

- à aplicação e demonstração de medidas técnicas e organizativas adequadas, tal como referido no artigo 24.º, nºs 1 e 3, no artigo 25.º e no artigo 32.º, nºs 1 e 3;
- à apresentação das garantias suficientes (subcontratante ao responsável pelo tratamento) a que se refere o artigo 28.º, n.ºs 1 (subcontratante ulterior ao subcontratante) e 4 (cf. artigo 28.º, n. º 5).

13. Uma vez que a certificação não prova a conformidade em si e por si só, sendo antes um elemento que pode ser utilizado para demonstrar a conformidade, deve ser efetuada de forma transparente. A demonstração da conformidade exige documentação de apoio, nomeadamente relatórios escritos que não só repitam, como descrevam o modo como os critérios são cumpridos e, caso estes não tenham sido inicialmente cumpridos, detalhem as correções e as medidas corretivas, bem como a sua adequação, fornecendo assim as razões para a concessão e manutenção da certificação. Tal inclui as linhas gerais da decisão individual de concessão, renovação ou revogação de um certificado, que deve indicar os motivos, argumentos e provas resultantes da aplicação dos critérios e as conclusões, ilações ou deduções dos factos ou pressupostos recolhidos durante a certificação.

1.3 Conceitos fundamentais

14. A secção seguinte analisa os conceitos fundamentais dos artigos 42.º e 43.º. Esta análise procura contribuir para uma melhor compreensão dos termos básicos e do âmbito da certificação ao abrigo do RGPD.

1.3.1 Interpretação do termo «certificação»

15. O RGPD não define «certificação». A Organização Internacional de Normalização (ISO) estabelece uma definição universal de certificação como «o fornecimento, por um organismo independente, da garantia por escrito (certificado) de que o produto, serviço ou sistema em causa cumpre requisitos específicos.» A certificação é também conhecida por «avaliação da conformidade por terceiros», e os organismos de certificação também podem ser designados como «organismos de avaliação da conformidade (OAC)». Na norma EN-ISO/IEC 17000: 2004 - Avaliação da conformidade - Vocabulário e princípios gerais (a que se refere a norma ISO17065) - a certificação é definida do seguinte modo: «Atestação por terceiros [...] relativa a produtos, processos e serviços».

16. Atestação é a «emissão de uma comprovação, com base numa decisão decorrente de uma análise, de que o cumprimento dos requisitos especificados foi demonstrado» (ponto 5.2, ISO 17000: 2004).

17. No contexto da certificação nos termos dos artigos 42.º e 43.º do RGPD, a certificação refere-se a uma atestação por terceiros relativa a operações de tratamento efetuadas por responsáveis pelo tratamento e subcontratantes.

1.3.2 Procedimentos de certificação, selos e marcas

18. O RGPD não define «procedimentos de certificação, selos ou marcas», antes utiliza os termos coletivamente. Um certificado é uma declaração de conformidade. O selo ou marca pode ser utilizado para indicar a conclusão com êxito do processo de certificação. Um selo ou uma marca refere-se geralmente a um logótipo ou símbolo cuja presença (para além de um certificado) indica que o objeto da certificação foi avaliado de forma independente num procedimento de certificação e está em conformidade com os requisitos especificados, constantes de documentos normativos, tais como regulamentos, normas ou especificações técnicas. Estes requisitos no contexto da certificação ao abrigo do RGPD são definidos nos requisitos adicionais que complementam as regras de acreditação dos organismos de certificação na norma EN-ISO/IEC 17065/2012 e nos critérios de certificação aprovados pela autoridade de controlo competente ou pelo Comité. Um certificado, selo ou marca nos termos do RGPD só pode ser emitido após a avaliação independente das provas por um organismo de certificação acreditado ou por uma autoridade de controlo competente, declarando que os critérios de certificação foram cumpridos.

19. O quadro constitui um exemplo genérico de um processo de certificação.

Apresentação do pedido pelo responsável pelo tratamento ou pelo subcontratante	Controlo formal pelo Comité	Avaliação Pré-avaliação	Avaliação Avaliação do ToE	Avaliação Validação de resultados	Informação à autoridade de controlo competente	Certificação	Controlo	Renovação da certificação
A descrição do alvo de avaliação (target of evaluation) (ToE) é unívoca e completa, incluindo as interfaces?	A descrição do ToE pode ser aceite?	Quais são os critérios aplicáveis?	O ToE satisfaz os critérios?	Todos os critérios pertinentes especificados têm em conta o ToE?	Os motivos de concessão ou de retiro da certificação foram apresentados?	O certificado pode ser concedido?	O ToE continua a satisfazer os critérios?	O tratamento continua a satisfazer os critérios de certificação?
O acesso às atividades de tratamento do ToE pode ser concedido?	Todos os documentos estão completos e atualizados?	Quais são os métodos de avaliação aplicáveis?	A documentação do ToE está correta?	A avaliação foi suficientemente documentada?		Os relatórios estão prontos para serem publicados?	O certificado/selo/marca de confiança são utilizados corretamente?	Os domínios de desenvolvimento foram tratados de forma satisfatória?
Artigo 42.º, n.º 6	Artigo 42.º, n.º 7	Artigo 43.º, n.º 4	Artigo 42.º, n.º 5, artigo 43.º, n.º 4	Artigo 43.º, n.º 4	Artigo 43.º, n.º 1, artigo 43.º, n.º 5	Artigo 43.º, n.º 1 Artigo 42.º, n.º 7	Artigo 42.º, n.º 7	Artigo 42.º, n.º 7

2 O PAPEL DAS AUTORIDADES DE CONTROLO

20. O artigo 42.º, n.º 5, prevê que a certificação seja emitida por um organismo de certificação acreditado ou por uma autoridade de controlo competente. O RGPD não impõe a emissão de certificações como uma tarefa obrigatória das autoridades de controlo, permitindo, pelo

contrário, que possam adotar vários modelos diferentes. Por exemplo, uma autoridade de controlo pode decidir por uma ou mais das seguintes opções:

- emitir ela própria a certificação, com respeito ao seu próprio sistema de certificação;
- emitir ela própria a certificação, com respeito ao seu próprio sistema de certificação, mas delegar a terceiros a totalidade ou parte do processo de avaliação;
- criar o seu próprio sistema de certificação e confiar aos organismos de certificação o procedimento da emissão da certificação; e
- incentivar o mercado a desenvolver procedimentos de certificação.

21. Uma autoridade de controlo terá também de considerar o seu papel à luz das decisões tomadas a nível nacional sobre os procedimentos de acreditação – em especial se a própria autoridade de controlo estiver habilitada a acreditar organismos de certificação nos termos do artigo 43.º, n.º 1, do RGPD. Assim, cada autoridade de controlo determinará qual a abordagem a adotar para prosseguir o objetivo geral da certificação ao abrigo do RGPD. Tal será determinado no contexto não só das atribuições e dos poderes previstos nos artigos 57.º e 58.º, mas também na contabilização da certificação como fator a ter em conta na fixação das coimas e, de um modo mais geral, como meio de demonstrar a conformidade.

2.1 A autoridade de controlo como organismo de certificação

22. Se uma autoridade de controlo decidir realizar a certificação, terá de avaliar cuidadosamente o seu papel no que diz respeito às atribuições que lhe incumbem ao abrigo do RGPD. O seu papel deve ser transparente no exercício das suas funções. Terá de ter em conta, especificamente, a separação de poderes em matéria de investigação e de execução, a fim de evitar potenciais conflitos de interesses.

23. Ao atuar na qualidade de organismo de certificação, uma autoridade de controlo terá de garantir a criação adequada de um procedimento de certificação e desenvolver os seus próprios critérios de certificação ou adotar tais critérios. Além disso, cada autoridade de controlo que emita certificações tem a atribuição de proceder à sua revisão periódica (artigo 57.º, n.º 1, alínea o)) e o poder de as revogar se os requisitos de certificação não estiverem ou deixarem de estar cumpridos (artigo 58.º, n.º 2, alínea h)). Para cumprir estes requisitos, é útil prever um procedimento de certificação e requisitos processuais e, salvo disposto em contrário pela legislação nacional, estabelecer um acordo juridicamente vinculativo para a prestação de atividades de certificação com a organização candidata individual. Deve garantir-se que este acordo em matéria de certificação exija que o requerente cumpra, pelo menos, os critérios de certificação, incluindo os procedimentos necessários para realizar a avaliação, o controlo do cumprimento dos critérios e a revisão periódica, incluindo o acesso a informações e/ou instalações, a documentação e a publicação de relatórios e resultados, bem como a investigação de reclamações. Espera-se também que uma autoridade de controlo siga os requisitos estabelecidos nas orientações para a acreditação de organismos de certificação, para além dos requisitos previstos no artigo 43.º, n.º 2.

2.2 Outras atribuições da autoridade de controlo em matéria de certificação

24. Nos Estados-Membros em que comecem a operar organismos de certificação, a autoridade de controlo, independentemente das suas próprias atividades, tem as seguintes atribuições e poderes:

    - avaliar os critérios de um sistema de certificação e elaborar um projeto de decisão (artigo 42.º, n.º 5);
    - comunicar ao Comité o projeto de decisão quando pretenda aprovar os critérios de certificação (artigo 64.º, n.º 1, alínea c), e artigo 64.º, n.º 7)) e ter em conta o parecer do Comité (artigo 64.º, n.º 1, alínea c), e artigo 70.º, n.º 1, alínea t));
    - aprovar os critérios de certificação (artigo 58.º, n.º 3, alínea f)) antes de a acreditação e a certificação poderem ter lugar (artigo 42.º, n.º 5, e artigo 43.º, n.º 2, alínea b));
    - publicar os critérios de certificação (artigo 43.º, n.º 6);
    - atuar como autoridade competente para os sistemas de certificação à escala da UE, o que pode dar lugar a um selo europeu de proteção de dados aprovado pelo CEPD (artigo 42.º, n.º 5, e artigo 70.º, n.º 1, alínea o)); e
    - ordenar a um organismo de certificação a) que não emita uma certificação ou b) que retire a certificação se os requisitos de certificação (procedimentos ou critérios de certificação) não estiverem ou deixarem de estar cumpridos (artigo 58.º, n.º 2, alínea h)).

25. O RGPD encarrega a autoridade de controlo da aprovação dos critérios de certificação, mas não do desenvolvimento de critérios. A fim de aprovar os critérios de certificação nos termos do artigo 42.º, n.º 5, a autoridade de controlo deve ter um conhecimento claro do que esperar, especificamente em termos de âmbito e conteúdo, para demonstrar a conformidade com o RGPD e também no que se refere à sua atribuição de controlar e fazer cumprir o regulamento. O anexo fornece orientações para garantir uma abordagem harmonizada aquando da avaliação dos critérios para efeitos de aprovação.

26. O artigo 43.º, n.º 1, exige que, antes de emitirem ou renovarem as certificações, os organismos de certificação informem a autoridade de controlo competente para que esta possa exercer os seus poderes de correção nos termos do artigo 58.º, n.º 2, alínea h). Além disso, o artigo 43.º, n.º 5, exige também que os organismos de certificação forneçam à autoridade de controlo competente os motivos para a concessão ou revogação da certificação solicitada. Embora o RGPD permita que as autoridades de controlo determinem o modo como receber, reconhecer, analisar e tratar estas informações do ponto de vista operacional (o que pode incluir, por exemplo, soluções tecnológicas que permitam a elaboração de relatórios pelos organismos de certificação), poderão adotar-se processos e critérios para tratar as informações e os relatórios apresentados pelo organismo de certificação sobre cada projeto de certificação bem sucedido, em conformidade com o artigo 43.º, n.º 1. Com base nestas informações, a autoridade de controlo pode exercer o seu poder de ordenar ao organismo de certificação que retire ou não emita uma certificação (artigo 58.º, n.º 2, alínea h)), bem como de controlar e fazer cumprir os requisitos e critérios

de certificação ao abrigo do RGPD (artigo 57.º, n.º 1, alínea a), e artigo 58.º, n.º 2, alínea h)). Tal permitirá uma abordagem harmonizada e a comparabilidade da certificação por diferentes organismos de certificação, além de garantir que as autoridades de controlo conheçam as informações sobre o estatuto de certificação de uma organização.

3 O PAPEL DO ORGANISMO DE CERTIFICAÇÃO

27. O papel do organismo de certificação consiste em emitir, rever, renovar e retirar certificações (artigo 42.º, n.ºs 5 e 7)) com base num procedimento de certificação e em critérios aprovados (artigo 43.º, n.º 1). Tal exige que o organismo de certificação ou o proprietário do sistema de certificação determine e estabeleça critérios e procedimentos de certificação, incluindo mecanismos de controlo do cumprimento, revisão, tratamento de reclamações e revogação. Os critérios de certificação são examinados no âmbito do processo de acreditação, que analisa as regras e os procedimentos ao abrigo dos quais são emitidas as certificações, os selos ou as marcas (artigo 43.º, n.º 2, alínea c)).

28. A existência de um procedimento e de critérios de certificação é necessária para que o organismo de certificação possa obter a acreditação nos termos do artigo 43.º. O âmbito e o tipo de critérios de certificação que influem nos procedimentos de certificação têm um impacto importante sobre o que faz um organismo de certificação e vice-versa. Critérios específicos podem, por exemplo, exigir métodos de avaliação específicos, como inspeções no local e a análise de códigos. Estes procedimentos são obrigatórios para efeitos de acreditação e são explicados de forma mais pormenorizada nas orientações relativas à acreditação.

29. O RGPD exige que o organismo de certificação forneça informações às autoridades de controlo, nomeadamente sobre as certificações individuais, o que é necessário para controlar a aplicação do procedimento de certificação (artigo 42.º, n.º 7, artigo 43.º, n.º 5, e artigo 58, n.º 2, alínea h)).

4 APROVAÇÃO DOS CRITÉRIOS DE CERTIFICAÇÃO

30. Os critérios de certificação fazem parte integrante de qualquer procedimento de certificação. Por conseguinte, o RGPD exige que os critérios de certificação de um procedimento de certificação sejam aprovados pela autoridade de controlo competente (artigos 42.º , n.º 5, e artigo 43.º, n.º 2, alínea b)). No caso de um selo europeu de proteção de dados, os critérios de certificação são aprovados pelo CEPD (artigo 42.º, n.º 5, e artigo 70.º, n.º 1, alínea o)). Ambas as vias de aprovação dos critérios de certificação são explicadas a seguir.

31. O CEPD reconhece os seguintes objetivos para a aprovação dos critérios de certificação:

- refletir adequadamente os requisitos e princípios relativos à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, tal como estabelecidos no Regulamento (UE) 2016/679; e
- contribuir para a aplicação coerente do RGPD.

32. A aprovação é concedida com base no requisito do RGPD segundo o qual o procedimento de certificação deve permitir aos responsáveis pelo tratamento e aos subcontratantes demonstrar que a conformidade com o RGPD está plenamente refletida nos critérios de certificação.

4.1 Aprovação dos critérios pela autoridade de controlo competente

33. Os critérios de certificação devem ser aprovados pela autoridade de controlo competente antes ou durante o processo de acreditação de um organismo de certificação. É igualmente necessária a aprovação de regimes ou conjuntos de critérios atualizados ou adicionais, ao abrigo da norma ISO 17065, pelo mesmo organismo de certificação, antes de serem utilizados os procedimentos de certificação alterados (artigo 42.º, n.º 5, e artigo 43.º, n.º 2, alínea b)). As autoridades de controlo devem tratar todos os pedidos de aprovação de critérios de certificação de forma equitativa e não discriminatória, de acordo com um procedimento publicamente disponível que especifique as condições gerais a preencher e a descrição do processo de aprovação.

34. Um organismo de certificação só pode emitir uma certificação num determinado Estado-Membro de acordo com os critérios aprovados pela autoridade de controlo desse Estado-Membro. Por outras palavras, os critérios de certificação têm de ser aprovados pela autoridade de controlo competente do país onde o organismo de certificação pretenda realizar a certificação e obter acreditação. Ver a secção seguinte no que se refere aos sistemas de certificação a nível europeu.

4.2 Aprovação de critérios pelo CEPD para o Selo Europeu de Proteção de Dados

35. Um organismo de certificação também pode emitir uma certificação de acordo com os critérios aprovados pelo CEPD para um selo europeu de proteção de dados. Os critérios de certificação aprovados pelo CEPD nos termos do artigo 63.º podem dar lugar ao Selo Europeu de Proteção de Dados (artigo 42.º, n.º 5). À luz das atuais convenções em matéria de certificação e acreditação, o CEPD reconhece que é desejável evitar a fragmentação do mercado da certificação em matéria de proteção de dados. Observa que o artigo 42.º, n.º 1, prevê que os Estados-Membros, as autoridades de controlo, o Comité e a Comissão promovam, em especial ao nível da União, a criação de procedimentos de certificação.

4.2.1 Pedido de aprovação

36. O pedido de aprovação de critérios, nos termos do artigo 42.º, n.º 5, e do artigo 70.º, n.º 1, alínea o), pelo CEPD deve ser apresentado através de uma autoridade de controlo competente e indicar a intenção do proprietário do sistema e do organismo de certificação candidato ou acreditado de cumprir os critérios, num procedimento de certificação aplicável aos responsáveis pelo tratamento e aos subcontratantes em todos os Estados-Membros. A

autoridade de controlo competente apresentará um projeto ao CEPD quando considerar que os critérios podem ser por este aprovados.

37. A escolha do local onde apresentar um pedido de aprovação dos critérios dependerá do local da sede dos proprietários dos sistemas de certificação ou dos organismos de certificação.

38. Se um organismo de certificação apresentar um pedido, encontrar-se-á normalmente em processo de requisição da acreditação, ou estará já acreditado pela autoridade de controlo competente ou pelo organismo nacional de acreditação do respetivo Estado-Membro. Se o organismo de certificação já estiver acreditado para um procedimento de certificação nos termos do RGPD, tal poderá ajudar a agilizar o processo de aprovação.

4.2.2 Critérios do Selo Europeu de Proteção de Dados

39. O CEPD coordenará o processo de avaliação e aprovará os critérios relativos ao Selo Europeu de Proteção de Dados, conforme exigido. A avaliação incidirá em domínios como o âmbito dos critérios e a capacidade de servir de certificação comum. Caso os critérios sejam aprovados pelo CEPD, a autoridade de controlo competente para a sede da UE do organismo de certificação deverá tratar as reclamações relativas ao próprio procedimento e informar as restantes autoridades de controlo. Esta autoridade de controlo é igualmente competente para tomar medidas contra o organismo de certificação. Se for caso disso, a autoridade de controlo competente notificará as restantes autoridades de controlo e o CEPD.

40. Os critérios de certificação aplicáveis a uma certificação comum estão sujeitos a exigências a nível da UE e deverão fornecer um procedimento específico para fazer face a estas exigências. Os procedimentos de certificação europeus devem destinar-se a ser utilizados em todos os Estados-Membros. Com base no artigo 42.º, n.º 5, o procedimento relativo ao Selo Europeu de Proteção de Dados, bem como os seus critérios, devem poder ser adaptados de modo a ter em conta a regulamentação setorial nacional, quando aplicável, por exemplo para o tratamento de dados nas escolas, e prever uma aplicação à escala europeia.

41. Exemplo: Uma escola internacional que oferece educação escolar a titulares de dados na União tem a sua sede no Estado-Membro «A». A escola deseja certificar o seu processo de candidatura em linha com um sistema de certificação a nível da UE para obter um selo europeu de proteção de dados e pretende solicitar a certificação das operações de tratamento oferecidas por um organismo de certificação estabelecido no Estado-Membro «B» com base num selo europeu de proteção de dados. Os critérios do selo, concebidos e documentados no procedimento apropriado, devem poder ter em conta a regulamentação aplicável às escolas do Estado-Membro «A». Os critérios devem também exigir que o processo de candidatura em linha da escola forneça informações e tenha em conta os requisitos aplicáveis do Estado-Membro em matéria de proteção de dados, que podem diferir entre Estados-Membros. É o caso, por exemplo, dos conjuntos de dados pessoais que devem ser apresentados para efeitos de candidatura, tais como notas ou resultados de exames de jardins de infância, diferentes períodos de conservação, recolha ou tratamento de dados financeiros ou biométricos, outras limitações de tratamento adicionais.

- Nos critérios de elevado nível para a aprovação de um procedimento relativo ao Selo Europeu de Proteção de Dados incluem-se:

- critérios aprovados pelo Comité;
- aplicação em todos os países, refletindo, se for caso disso, os requisitos legais nacionais e os regulamentos setoriais específicos;
-

- critérios harmonizados que possam ser adaptados de modo a refletir os requisitos nacionais;
  - descrição do procedimento de certificação, especificando:
  - os acordos de certificação que cumpram os requisitos pan-europeus;
  - procedimentos para garantir e fornecer soluções para as variações nacionais e garantir que o selo contribui para demonstrar a conformidade com o RGPD; e
  - a língua dos relatórios dirigidos a todas as autoridades de controlo em causa.

42. O anexo contém igualmente recomendações sobre os critérios relativos ao Selo Europeu de Proteção de Dados.

4.2.3 Papel da acreditação

43. Tal como indicado no ponto 4.2.1, quando os critérios são identificados como adequados para a certificação comum e foram aprovados como tal pelo Comité nos termos do artigo 42.º, n.º 5, os organismos de certificação podem ser acreditados para realizar a certificação ao abrigo desses critérios a nível da União.

44. Os sistemas que se destinem a ser oferecidos apenas em determinados Estados-Membros não serão candidatos aos selos da UE. A acreditação para o âmbito de aplicação de um selo europeu de proteção de dados necessitará de uma acreditação no Estado-Membro da sede do organismo de certificação que pretende gerir o sistema, ou seja, que é responsável pela emissão de certificações e pela gestão das atividades de certificação das suas entidades e filiais noutros Estados-Membros. Nos casos em que outros estabelecimentos ou serviços gerem e realizam a certificação de forma autónoma, cada um desses estabelecimentos ou serviços deverá ser objeto de uma acreditação separada no Estado-Membro em que se encontram estabelecidos. Por outras palavras, a acreditação só é necessária no Estado-Membro da sede do organismo de certificação nos casos em que apenas esta entidade emite os certificados. Em contrapartida, quando outros estabelecimentos do organismo de certificação também emitem certificados, esses estabelecimentos devem igualmente ser acreditados.

45. Por conseguinte, se um organismo de certificação não estiver acreditado para certificar ao abrigo do Selo Europeu de Proteção de Dados, os critérios aprovados pelo CEPD não podem ser utilizados e o selo não pode ser concedido.

5 ELABORAÇÃO DOS CRITÉRIOS DE CERTIFICAÇÃO

46. O RGPD estabeleceu o quadro para a elaboração de critérios de certificação. Embora os artigos 42.º e 43.º abordem os requisitos fundamentais relativos ao processo de certificação, prevendo ao mesmo tempo critérios essenciais para os procedimentos de certificação, a base dos critérios de certificação deve decorrer dos princípios e regras do RGPD e ajudar a garantir que estes são cumpridos.

47. A elaboração dos critérios de certificação deve centrar-se na verificabilidade, relevância e adequação destes últimos para demonstrar a conformidade com o regulamento. Os critérios de certificação devem ser formulados de forma a serem claros e compreensíveis e a permitirem uma aplicação prática.

48. Se for caso disso, na elaboração dos critérios de certificação devem ser tidos em conta, entre outros, os seguintes aspetos de conformidade em apoio da avaliação das operações de tratamento:

- a licitude do tratamento, nos termos do artigo 6.º;
- os princípios relativos ao tratamento de dados pessoais, nos termos do artigo 5.º;
- os direitos dos titulares dos dados, nos termos dos artigos 12.º a 23.º;
- a obrigação de notificar as violações de dados, nos termos do artigo 33.º;
- a obrigação de proteção de dados desde a conceção e por defeito, nos termos do artigo 25.º;
- se foi realizada uma avaliação de impacto sobre a proteção de dados, nos termos do artigo 35.º, n.º 7, alínea d), se aplicável; e
- as medidas técnicas e organizativas adotadas, nos termos do artigo 32.º.

49. O impacto destas considerações nos critérios pode variar em função do âmbito da certificação, que pode incluir o tipo de operação(ões) de tratamento e o domínio da certificação (por exemplo, o setor da saúde).

5.1 O que pode ser certificado ao abrigo do RGPD?

50. O CEPD considera que o RGPD prevê um âmbito alargado para o que pode ser certificado ao seu abrigo, desde que a tónica seja colocada na comprovação da conformidade das operações de tratamento dos responsáveis pelo tratamento e dos subcontratantes com o presente regulamento (artigo 42.º, n.º 1).

51. Na avaliação de uma operação de tratamento, devem ser tidos em conta, quando aplicável, as três componentes principais seguintes:

1. dados pessoais (âmbito material do RGPD);

2. sistemas técnicos - as infraestruturas, como o *hardware* e o *software*, utilizadas para tratar os dados pessoais; e

3. processos e procedimentos relacionados com a(s) operação(ões) de tratamento.

52. Cada componente utilizada nas operações de tratamento deve ser sujeita a uma avaliação em função dos critérios definidos. Pelo menos quatro fatores relevantes diferentes podem ter influência: 1) a organização e a estrutura jurídica do responsável pelo tratamento ou do subcontratante; 2) o departamento, o ambiente e as pessoas envolvidas na(s) operação(ões) de tratamento; 3) a descrição técnica dos elementos a avaliar; e, por último, 4) a infraestrutura informática de apoio à operação de tratamento, incluindo sistemas operativos, sistemas virtuais, bases de dados, sistemas de autenticação e autorização, encaminhadores (*routers*) e barreiras de segurança (*firewalls*), sistemas de armazenamento, infraestruturas de comunicação ou acesso à Internet e medidas técnicas associadas.

53. As três componentes principais são relevantes para a conceção dos procedimentos e critérios de certificação. A sua tomada em consideração pode variar consoante o objeto da certificação. Por exemplo, em alguns casos, algumas componentes podem ser ignoradas se forem consideradas não pertinentes para o objeto da certificação.

54. Para especificar mais pormenorizadamente o que pode ser certificado nos termos do RGPD, este contém orientações adicionais. Decorre do artigo 42.º, n.º 7, que as certificações ao abrigo do RGPD são emitidas apenas aos responsáveis pelo tratamento de dados e aos subcontratantes, o que exclui, por exemplo, a certificação de responsáveis pela proteção de dados. O artigo 43.º, n.º 1, alínea b), faz referência à norma ISO 17065, que prevê a acreditação dos organismos de certificação que avaliam a conformidade de produtos, serviços e processos. Uma operação ou um conjunto de operações de tratamento pode dar lugar a um produto ou serviço na terminologia da norma ISO 17065, que, como tal, pode ser objeto de certificação. Por exemplo, o tratamento de dados dos trabalhadores para efeitos de pagamento de salários ou de gestão de licenças constitui um conjunto de operações na aceção do RGPD e pode dar lugar a um produto, um processo ou um serviço na terminologia da ISO.

55. Com base nestas considerações, o CEPD considera que o âmbito da certificação ao abrigo do RGPD diz respeito a operações ou conjuntos de operações de tratamento. Estas podem incluir processos de governação no sentido de medidas organizativas, ou seja, como parte integrante de uma operação de tratamento (por exemplo, o processo de governação estabelecido para o tratamento de reclamações no âmbito do tratamento de dados dos trabalhadores para efeitos de pagamento de salários).

56. A fim de avaliar a conformidade da operação de tratamento com os critérios de certificação, deve ser apresentado um caso de utilização. Por exemplo, a conformidade da utilização de uma infraestrutura técnica implantada numa operação de tratamento depende das categorias de dados que visa tratar. As medidas organizativas dependem das categorias e do volume de dados e da infraestrutura técnica utilizada para o tratamento, tendo em conta a natureza, o âmbito, o conteúdo e as finalidades do tratamento, bem como os riscos para os direitos e liberdades dos titulares de dados.

57. Além disso, há que ter em mente que as aplicações informáticas podem ser muito diferentes, ainda que sirvam os mesmos fins de tratamento. Por conseguinte, este aspeto deve ser tido em conta na definição do âmbito dos procedimentos de certificação e na elaboração dos critérios de certificação, ou seja, o âmbito da certificação e os critérios não devem ser tão restritos que excluam as aplicações informáticas concebidas de forma diferente.

5.2 Determinação do objeto da certificação

58. O âmbito de um procedimento de certificação deve ser distinguido do objeto - também denominado «alvo de avaliação» (do inglês «target of evaluation», TOE) - em projetos de certificação individuais ao abrigo de um procedimento de certificação. Um procedimento de certificação pode definir o seu âmbito, quer de um modo geral quer em relação a um tipo ou domínio específico de operações de tratamento, podendo, assim, já identificar os objetos da certificação que se inserem no seu âmbito (por exemplo, armazenamento seguro e proteção de dados pessoais contidos num cofre digital). Em qualquer caso, uma avaliação fiável e significativa da conformidade só pode ocorrer se o objeto individual de um projeto de certificação for descrito com precisão. Essa avaliação deve descrever claramente quais as operações de tratamento que são incluídas no objeto da certificação e, em seguida, as componentes essenciais, ou seja, os dados, processos e infraestruturas técnicas que serão avaliados e os que não o serão. Para tal, as interfaces com outros processos devem ser sempre consideradas e descritas. Evidentemente, o que não é conhecido não pode fazer parte da avaliação e, por conseguinte, não pode ser certificado. Em todo o caso, o objeto individual da certificação deve ser relevante no que respeita à mensagem ou alegação formulada na/pela certificação e não deve induzir em erro o utilizador, o cliente ou o consumidor.

59. [Exemplo 1]

Um banco oferece aos seus clientes um sítio Web para a prestação de serviços bancários em linha. No âmbito deste serviço, existe a possibilidade de efetuar transferências, comprar ações, criar ordens permanentes e gerir a conta. O banco pretende certificar os seguintes elementos no âmbito de um procedimento de certificação em matéria de proteção de dados de alcance geral, com base em critérios genéricos:

a) Início de sessão («log-in») seguro

O início de sessão seguro é uma operação de tratamento que é compreensível para o utilizador final e é relevante do ponto de vista da proteção de dados, uma vez que desempenha um papel importante para garantir a segurança dos dados pessoais em causa. Por conseguinte, esta operação de tratamento é necessária para iniciar uma sessão segura, podendo, portanto, constituir um alvo de avaliação relevante se o certificado indicar claramente que só a operação de início de sessão é certificada.

b) «Web front-end» (interface frontal da Web)

Embora possa ser pertinente do ponto de vista da proteção de dados, o «Web front-end» não é compreensível para o utilizador final e, portanto, não pode constituir um

alvo de avaliação relevante. Além disso, o utilizador não sabe de forma clara que serviços no sítio Web e, logo, que operações de tratamento são abrangidas pela certificação.

c) Operações bancárias em linha

As operações a nível da interface frontal, ou seja do lado do utilizador, («front-end web») e da interface a nível do servidor («back-end web) são operações de tratamento prestadas no âmbito do serviço bancário em linha, que podem ser significativas para o utilizador. Neste contexto, ambas devem ser incluídas nos alvos de avaliação, ao passo que as operações de tratamento que não estejam diretamente relacionadas com a prestação do serviço bancário em linha, tais como as operações de tratamento para efeitos de prevenção do branqueamento de capitais, podem ser excluídas dos alvos de avaliação.

No entanto, os serviços bancários em linha oferecidos pelo banco através do seu sítio Web podem também incluir outros serviços que, por sua vez, necessitam das suas próprias operações de tratamento. Neste contexto, outros serviços podem incluir, por exemplo, a oferta de um produto de seguros. Uma vez que este serviço adicional não está diretamente relacionado com a finalidade de prestar serviços bancários em linha, pode ser excluído dos alvos de avaliação. Se este serviço adicional (seguros) for excluído dos alvos de avaliação, as interfaces para este serviço integrado no sítio Web fazem parte dos alvos de avaliação, devendo, por conseguinte, ser descritas de modo a estabelecer uma distinção clara entre os serviços. Essa descrição é necessária para identificar e avaliar possíveis fluxos de dados entre os dois serviços.

60. [Exemplo 2]

Um banco oferece aos seus clientes um serviço que lhes permite agregar as informações relativas a diferentes contas e cartões de crédito de vários bancos (agregação de contas) e pretende ter o seu serviço certificado ao abrigo do RGPD. A autoridade de controlo competente aprovou um conjunto específico de critérios de certificação centrados neste tipo de atividade. O âmbito do procedimento de certificação incide apenas nos seguintes aspetos de conformidade:

- autenticação do utilizador; e
- formas aceitáveis de obter de outros bancos/serviços os dados a serem agregados.

Uma vez que o âmbito deste procedimento de certificação define o alvo de avaliação por si só, não é possível restringir este último de forma relevante sob o âmbito proposto e certificar apenas as características específicas ou uma única atividade de tratamento. Neste cenário, um alvo de avaliação deve corresponder a um âmbito específico.

5.3 Métodos de avaliação e metodologia de avaliação

61. Uma avaliação da conformidade que ajude a demonstrar a conformidade das operações de tratamento de dados exige a identificação e determinação dos métodos de avaliação e da

metodologia de avaliação. É importante saber se a informação para a avaliação é recolhida apenas com base na documentação (que, por si só, não seria suficiente) ou se é recolhida de forma ativa no local e mediante acesso direto ou indireto. A forma como a informação é recolhida tem impacto na relevância da certificação, pelo que deve ser definida e descrita.

Os procedimentos para a emissão e a revisão periódica das certificações devem incluir especificações para identificar o nível adequado de avaliação (profundidade e granularidade) para cumprir os critérios de certificação e incluir, nomeadamente:

- o fornecimento de informações e especificações sobre os métodos de avaliação aplicados e os resultados obtidos, por exemplo, durante auditorias no local ou a partir de documentação,
- métodos de avaliação centrados nas operações de tratamento (dados, sistemas, processos) e na finalidade do tratamento,
- a identificação das categorias de dados e das necessidades de proteção e a determinação da participação ou não de subcontratantes ou de terceiros,
- a identificação das funções e existência de um mecanismo de controlo de acesso definido em função dos papéis e das responsabilidades.

62. A profundidade da avaliação tem impacto na relevância e valor da certificação. Ao reduzir a profundidade da avaliação para fins pragmáticos ou redução dos custos, a relevância de uma certificação em matéria de proteção de dados será diminuída. As decisões sobre a granularidade da avaliação, por outro lado, podem exceder as capacidades financeiras do candidato e, muitas vezes, a capacidade dos avaliadores e auditores. Para fins de demonstração da conformidade, pode nem sempre ser crucial obter uma análise muito pormenorizada dos sistemas informáticos utilizados para continuar a ser relevante.

5.4 Documentação da avaliação

63. A documentação de certificação deve ser exaustiva e completa. A falta de documentação significa que não é possível realizar uma avaliação adequada. A função essencial da documentação de certificação é garantir a transparência do processo de avaliação ao abrigo do procedimento de certificação. A documentação dá resposta às perguntas sobre os requisitos estabelecidos por lei. Os procedimentos de certificação devem prever uma metodologia normalizada de documentação. A avaliação posterior permitirá a comparação da documentação de certificação com o estado real no local e com os critérios de certificação.

64. Uma documentação completa do que foi certificado e da metodologia adotada favorece a transparência. Nos termos do artigo 43.º, n.º 2, alínea c), os procedimentos de certificação devem estabelecer procedimentos que permitam a revisão das certificações. A fim de permitir à autoridade de controlo avaliar se, e em que medida, a certificação pode ser reconhecida em investigações formais, uma documentação pormenorizada pode ser o meio mais adequado de comunicação. A documentação apresentada durante a avaliação deve, por conseguinte, incidir em três aspetos principais:

- consistência e coerência dos métodos de avaliação executados;

- métodos de avaliação destinados a demonstrar a conformidade do objeto de certificação com os critérios de certificação e, consequentemente, com o regulamento; e
- demonstração de que os resultados da avaliação foram validados por um organismo de certificação independente e imparcial.

5.5 Documentação dos resultados

65. O considerando 100 contém informação sobre os objetivos prosseguidos com a introdução da certificação.

«A fim de reforçar a transparência e o cumprimento do presente regulamento, deverá ser encorajada a criação de procedimentos de certificação e selos e marcas de proteção de dados, que permitam aos titulares avaliar rapidamente o nível de proteção de dados proporcionado pelos produtos e serviços em causa.»

66. Para reforçar a transparência, a documentação e a comunicação dos resultados desempenham um papel importante. Os organismos de certificação que utilizam procedimentos de certificação, selos ou marcas direcionados para os titulares de dados (na sua qualidade de consumidores ou de clientes) devem fornecer informações facilmente acessíveis, inteligíveis e pertinentes sobre a(s) operação(ões) de tratamento certificada(s). Esta informação ao público deve incluir, pelo menos,
    - a descrição do alvo de avaliação;
    - a referência aos critérios aprovados aplicados ao alvo de avaliação específico;
    - a metodologia para a avaliação dos critérios (avaliação no local, documentação, etc.); e
    - o período de validade do certificado; e
    - deve permitir às autoridades de controlo e ao público comparar os resultados.

6 ORIENTAÇÕES PARA A DEFINIÇÃO DOS CRITÉRIOS DE CERTIFICAÇÃO

67. Os critérios de certificação são parte integrante de um procedimento de certificação. O procedimento de certificação inclui os requisitos respeitantes à indicação de «como, por quem e em que medida» e à granularidade da avaliação a realizar em projetos de certificação individuais relativos a um objeto específico ou ao alvo de avaliação. Os critérios de certificação estabelecem os requisitos nominais em relação aos quais é avaliada a operação de tratamento definida no alvo de avaliação. As presentes orientações para a

definição dos critérios de certificação fornecem conselhos genéricos que facilitarão a avaliação dos critérios de certificação para efeitos de aprovação.

- As considerações gerais que se seguem devem ser tidas em conta aquando da aprovação ou definição dos critérios de certificação. Os critérios de certificação devem:
- ser uniformes e verificáveis,
- ser passíveis de auditoria, a fim de facilitar a avaliação das operações de tratamento efetuadas ao abrigo do RGPD, especificando, em especial, os objetivos e as orientações de execução para a realização desses objetivos;
- ser pertinentes em relação ao público visado (por exemplo, entre empresas, B2B, e entre empresas e consumidores, B2C);
- ter em conta e, se for caso disso, ser interoperáveis com outras normas (como as normas ISO e as normas a nível nacional); e
- ser flexíveis e redimensionáveis para a aplicação a diferentes tipos e dimensões de organizações, incluindo micro, pequenas e médias empresas, em conformidade com o artigo 42.º, n.º 1, e a abordagem baseada no risco, em conformidade com o considerando 77.

68. Uma pequena empresa local, como um retalhista, realizará, normalmente, operações de tratamento menos complexas do que um grande retalhista multinacional. Embora os requisitos de licitude das operações de tratamento sejam os mesmos, o âmbito do tratamento dos dados e a sua complexidade devem ser tidos em conta, sendo necessário, por conseguinte, que os procedimentos de certificação e os seus critérios sejam redimensionáveis de acordo com a atividade de tratamento em causa.

6.1 Normas existentes

69. Os organismos de certificação terão de analisar a forma como critérios específicos tomam em consideração os instrumentos pertinentes existentes, como os códigos de conduta, as normas técnicas ou as iniciativas regulamentares e jurídicas nacionais. Idealmente, os critérios serão interoperáveis com as normas existentes, que podem ajudar um responsável pelo tratamento ou um subcontratante a cumprir as obrigações que lhe incumbem ao abrigo do RGPD. No entanto, embora as normas da indústria se centrem frequentemente na proteção e segurança da organização contra ameaças, o RGPD visa a proteção dos direitos fundamentais das pessoas singulares. Esta diferente perspetiva deve ser tida em conta aquando da conceção dos critérios ou da aprovação de critérios ou procedimentos de certificação com base nas normas do setor.

6.2 Definição de critérios

70. Os critérios de certificação devem corresponder à declaração de certificação (mensagem ou alegação) de um procedimento ou sistema de certificação e ir ao encontro das expectativas que este suscita. A designação de um procedimento de certificação poderá já identificar o âmbito de aplicação e terá impacto na determinação dos critérios.

71. [Exemplo 3]

    Um procedimento denominado «HealthPrivacyMark» deve limitar o seu âmbito ao setor da saúde. O nome do selo gera a expectativa de que os requisitos em matéria de proteção de dados relacionados com os dados relativos à saúde foram examinados. Por conseguinte, os critérios deste procedimento devem ser adequados para avaliar os requisitos em matéria de proteção de dados neste setor.

72. [Exemplo 4]

    Um procedimento relacionado com a certificação das operações de tratamento que incluem sistemas de governação no tratamento de dados deve identificar critérios que permitam o reconhecimento e a avaliação dos processos de governação e das respetivas medidas técnicas e organizativas de apoio.

73. [Exemplo 5]

    Os critérios aplicáveis a um procedimento relacionado com a computação em nuvem devem ter em conta os requisitos técnicos especiais necessários para a utilização de serviços baseados na computação em nuvem. Por exemplo, se os servidores forem utilizados fora da UE, os critérios devem ter em conta as condições estabelecidas no capítulo V do RGPD no que diz respeito às transferências de dados para países terceiros.

74. Os critérios concebidos para se adequarem a diferentes alvos de avaliação em diferentes setores e/ou Estados-Membros devem permitir a aplicação a diferentes cenários e a identificação das medidas adequadas para se adequarem a pequenas, médias ou grandes operações de tratamento e refletirem os riscos, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, em conformidade com o RGPD. Por conseguinte, os procedimentos de certificação (por exemplo, para a documentação, os testes, ou o método e a profundidade da avaliação), que complementam os critérios, devem responder a essas necessidades, além de permitir e estabelecer regras, por exemplo, para aplicar os critérios pertinentes em projetos de certificação individuais. Os critérios devem facilitar a avaliação da existência, ou não, de garantias suficientes para a aplicação de medidas técnicas e organizativas adequadas.

6.3 Vigência dos critérios de certificação

75. Os critérios de certificação, embora devam ser fiáveis ao longo do tempo, não devem ser imutáveis. Serão sujeitos a revisão, por exemplo, sempre que:

    - o quadro jurídico seja alterado;
    - os termos e disposições sejam interpretados por acórdãos do Tribunal de Justiça das Comunidades Europeias; ou

- o estado da técnica tenha evoluído.

Pelo Comité Europeu para a Proteção de Dados

A Presidente

(Andrea Jelinek)

ANEXO 1: ATRIBUIÇÕES E PODERES DAS AUTORIDADES DE CONTROLO EM MATÉRIA DE CERTIFICAÇÃO EM CONFORMIDADE COM O RGPD

	Disposições	Requisitos
Atribuições	Artigo 43.º, n.º 6	Estabelece que as autoridades de controlo publiquem os critérios referidos no artigo 42.º, n.º 5, sob uma forma facilmente acessível e que os comuniquem ao Comité.
	Artigo 57.º, n.º 1, alínea n)	Exige que a autoridade de controlo aprove os critérios de certificação nos termos do artigo 42.º, n.º 5.
	Artigo 57.º, n.º 1, alínea o)	Estabelece que, se necessário (ou seja, quando emite uma certificação), a autoridade de controlo procede a uma revisão periódica das certificações emitidas, nos termos do artigo 42.º, n.º 7.
	Artigo 64.º, n.º 1, alínea c)	Exige que a autoridade de controlo envie o projeto de decisão ao Comité, quando vise aprovar os critérios de certificação a que se refere o artigo 42.º, n.º 5.
Poderes	Artigo 58.º, n.º 1, alínea c)	Estabelece que a autoridade de controlo dispõe do poder de rever as certificações emitidas nos termos do artigo 42.º, n.º 7.
	Artigo 58.º, n.º 2, alínea h)	Estabelece que a autoridade de controlo dispõe do poder de retirar ou ordenar ao organismo de certificação que retire uma certificação, ou de ordenar ao organismo de certificação que não emita uma certificação.
	Artigo 58.º, n.º 3, alínea e)	Estabelece que a autoridade de controlo dispõe do poder de acreditar organismos de certificação.
	Artigo 58.º, n.º 3, alínea f)	Estabelece que a autoridade de controlo dispõe do poder de emitir certificações e aprovar os critérios de certificação.
	Artigo 58.º, n.º 3, alínea e)	Estabelece que a autoridade de controlo dispõe do poder de acreditar organismos de certificação.
	Artigo 58.º, n.º 3, alínea f)	Estabelece que a autoridade de controlo dispõe do poder de emitir certificações e aprovar os critérios de certificação.

ANEXO 2

1 INTRODUÇÃO

O anexo 2 fornece diretrizes para a análise e avaliação dos critérios de certificação nos termos do artigo 42.º, n.º 5. Identifica os tópicos que a autoridade responsável pela proteção de dados e o CEPD irão analisar e aplicar para a aprovação de critérios de certificação de um mecanismo de certificação. As perguntas devem ser tidas em conta pelos organismos de certificação e pelos proprietários de sistemas de certificação que pretendem definir e apresentar critérios para aprovação. A lista não é exaustiva, mas apresenta os tópicos mínimos a considerar. Nem todas as perguntas serão aplicáveis; no entanto, devem ser tidas em conta no momento da elaboração dos critérios e, se for caso disso, será necessários explicar por que razão os critérios os critérios não abrangem determinados aspetos específicos. Algumas questões são repetidas, embora sob una perspetiva diferente. Estas diretrizes devem ser consideradas em conformidade com os requisitos legais previstos pelo RGPD e, se for caso disso, pela legislação nacional.

2 ÂMBITO DO MECANISMO DE CERTIFICAÇÃO E ALVO DA AVALIAÇÃO («TARGET OF EVALUATION» - TOE)

a. O âmbito do mecanismo de certificação (para o qual devem ser aplicados os critérios de proteção de dados) é claramente descrito?

b. O âmbito do mecanismo de certificação é relevante para o público destinatário e não é suscetível de induzir em erro?

- *Exemplo: Um «selo de empresa de confiança» sugere que o conjunto das atividades de tratamento de uma empresa foram controladas, embora apenas certas operações de tratamento específicas, como, por exemplo, o tratamento dos pagamentos em linha, são de facto sujeitas a certificação. O âmbito de aplicação induz, por conseguinte, em erro.*

c. O âmbito do mecanismo de certificação reflete todos os aspetos relevantes das operações de tratamento?

- *Exemplo: Uma «marca de privacidade no domínio da saúde» deve incluir todos os dados de avaliação relativos à saúde, a fim de satisfazer os requisitos estabelecidos no artigo 9.º.*

d. O âmbito do mecanismo de certificação permite uma certificação de proteção de dados relevante, tendo em conta a natureza, o conteúdo e o risco das operações de tratamento conexas?

- *Exemplo: Se o âmbito do mecanismo de certificação se centrar apenas em aspetos específicos das operações de tratamento, como a recolha de dados, mas não sobre as operações de tratamento adicionais, como o tratamento para efeitos de criação de perfis para publicidade ou da gestão dos direitos dos titulares de dados, não seria relevante para os titulares dos dados.*

e. O âmbito do mecanismo de certificação abrange o tratamento de dados pessoais no país de aplicação pertinente ou compreende o tratamento transfronteiriço e/ou as transferências?

f. Os critérios de certificação descrevem suficientemente a forma como os ToE devem ser definidos?

- *Exemplo: Um «selo de privacidade» que ofereça um âmbito geral que exija «uma especificação do tratamento que é objeto da certificação» não fornece orientações claras e suficientes sobre a forma de estabelecer e descrever os ToE.*
- *Exemplo: Um âmbito (específico) de um «selo de privacidade para os cofres digitais», relativo à conservação segura dos dados pessoais, deveriam descrever pormenorizadamente os requisitos a preencher, como a definição de cofre, os requisitos do sistema, as medidas técnicas e organizativas obrigatórias. Deste modo, o âmbito pode definir claramente o ToE.*

(1) Os critérios exigem que o ToE inclua uma identificação de todas as operações de tratamento relevantes, uma ilustração dos fluxos de dados e a determinação do âmbito do TOE?

- *Exemplo: Um mecanismo de certificação oferece a certificação de operações de tratamento de responsáveis pelo tratamento de dados ao abrigo do RGPD sem especificar em pormenor o âmbito de aplicação (âmbito geral). Os critérios utilizados pelo mecanismo exigem que o responsável pelo tratamento de dados determine a operação de tratamento visada (ToE) em termos de tipos de dados, de sistemas e de processos utilizados.*

(2) Os critérios exigem que o requerente indique claramente onde tem início e onde termina o tratamento sujeito a avaliação? Os critérios exigem que o ToE inclua interfaces sempre que as operações de tratamento interdependentes não estejam incluídas no ToE? E tal justifica-se de forma satisfatória?

- *Exemplo: Um ToE que descreve suficientemente em pormenor as operações de tratamento de um serviço em linha, como, por exemplo, o registo dos utilizadores, a prestação de serviços, a faturação, o registo dos endereços IP, as interfaces com os utilizadores e com terceiros, mas não o alojamento em servidor (incluindo todavia os contratos de tratamento e os contratos relativos às medidas técnicas e organizativas).*

g. Os critérios garantem que cada um dos ToE pode ser compreendido pelo público visado, incluindo, se for caso disso, os titulares dos dados?

3 REQUISITOS GERAIS

a. O conjunto dos termos pertinentes utilizados no catálogo de critérios (ou seja, no conjunto completo de critérios de certificação) são identificados, explicados e descritos?

b. Todas as referências normativas são identificadas?

c. Os critérios incluem a definição das responsabilidades em matéria de proteção de dados, dos procedimentos e do tratamento abrangidos pelo âmbito do mecanismo de certificação?

4 OPERAÇÃO DE TRATAMENTO, ARTIGO 42.º, N.º 1

No que diz respeito ao âmbito do mecanismo de certificação (geral ou específico), todos os componentes relevantes das operações de tratamento (dados, sistemas e processos) são abrangidos pelos critérios?

a. Os critérios exigem a identificação das bases jurídicas válidas do tratamento no que diz respeito ao ToE?

b. No que diz respeito ao ToE, os critérios reconhecem as fases relevantes do tratamento e todo o ciclo de vida completo dos dados, incluindo o apagamento e ou anonimização?

c. No que diz respeito ao ToE, os critérios exigem a portabilidade dos dados?

d. No que diz respeito ao ToE, os critérios permitem identificar e refletir tipos especiais de operações de tratamento, como, por exemplo, a tomada de decisões automatizadas, a definição de perfis?

e. No que diz respeito ao ToE, os critérios permitem identificar categorias especiais de dados?

f. Os critérios permitem e exigem a avaliação do risco das operações individuais de tratamento e das necessidades de proteção dos direitos e liberdades dos titulares dos dados?

g. Os critérios permitem e exigem uma contabilização adequada dos riscos para os direitos e liberdades das pessoas singulares?

...

5 LICITUDE DO TRATAMENTO

a. Os critérios exigem a verificação da licitude do tratamento para as operações individuais de tratamento no que diz respeito à finalidade e à necessidade do tratamento?

b. Os critérios exigem o controlo de todos os requisitos de uma base jurídica para operações individuais de tratamento?

6 PRINCÍPIOS, ARTIGO 5.º

a. Os critérios integram de forma adequada todos os princípios de proteção de dados, em conformidade com o artigo 5.º?

b. Os critérios exigem a demonstração da minimização de dados para cada ToE?

...

7 OBRIGAÇÕES GERAIS DOS RESPONSÁVEIS PELO TRATAMENTO E DOS SUBCONTRATANTES

a. Os critérios exigem prova de acordos contratuais entre subcontratantes e responsáveis pelo tratamento?

b. Os contratos entre responsáveis pelo tratamento e subcontratantes são sujeitos a avaliação?

c. Os critérios refletem as obrigações do responsável pelo tratamento nos termos do capítulo IV?

d. Os critérios exigem prova de revisão e atualização das medidas técnicas e organizativas implementadas pelo responsável pelo tratamento nos termos do artigo 24.º, n.º 1?

e. Os critérios verificam se a organização avaliou se um encarregado da proteção de dados (EPD) deve ser nomeado em conformidade com o artigo 37.º? Se for caso disso, o EPD preenche os requisitos previstos nos artigos 37.º a 39.º?

f. Os critérios verificam que os registos relativos às atividades de tratamento são exigidos em conformidade com o artigo 30.º, n.º 5, e respondem de forma adequada aos requisitos previstos no artigo 30.º?

8 DIREITOS DOS TITULARES DOS DADOS

a. Os critérios têm em conta de forma adequada do direito do titular dos dados à informação e exigem a adoção de medidas nesse sentido?

b. Os critérios exigem que aos titulares dos dados seja garantido um acesso e um controlo adequados, ou mesmo maiores, dos seus dados, incluindo a portabilidade dos dados?

c. Os critérios exigem a adoção de medidas que prevejam a possibilidade de intervir na operação de tratamento de dados, a fim de garantir os direitos dos titulares dos dados e permitir as retificações, o apagamento ou a limitação do tratamento?

...

9 RISCOS PARA OS DIREITOS E LIBERDADES DAS PESSOAS SINGULARES

a. Os critérios permitem e exigem uma avaliação dos riscos para os direitos e liberdades das pessoas singulares?

b. Os critérios preveem ou exigem uma metodologia de avaliação do risco reconhecida? Se for caso disso, é esta proporcional?

c. Os critérios permitem e exigem uma avaliação do impacto do previsto tratamento de dados nos direitos e liberdades das pessoas singulares?

d. Os critérios exigem uma consulta prévia sobre os riscos remanescentes que não possam ser atenuados, com base nos resultados da avaliação de impacto sobre a proteção de dados (AIPD)?

10 MEDIDAS TÉCNICAS E ORGANIZATIVAS QUE GARANTAM A PROTEÇÃO

a. Os critérios exigem a aplicação de medidas técnicas e organizativas que prevejam a confidencialidade das operações de tratamento?

b. Os critérios exigem a aplicação de medidas técnicas e organizativas que prevejam a integridade das operações de tratamento?

c. Os critérios exigem a aplicação de medidas técnicas e organizativas que prevejam a disponibilidade das operações de tratamento?

d. Os critérios exigem a aplicação de medidas que garantam a transparência das operações de tratamento de dados no que respeita a:

e. Responsabilidade?

f. Direitos dos titulares de dados?

g. Avaliação de operações individuais de tratamento, por exemplo, em matéria de transparência algorítmica?

h. Os critérios exigem a aplicação de medidas técnicas e organizativas que garantam os direitos dos titulares dos dados, por exemplo, a capacidade de prestar informações ou a portabilidade dos dados?

i. Os critérios exigem a aplicação de medidas técnicas e organizativas que prevejam a possibilidade de intervir na operação de tratamento de dados, a fim de garantir o direito dos titulares dos dados e permitir as retificações, o apagamento ou a limitação do tratamento?

j. Os critérios exigem a aplicação de medidas que prevejam a possibilidade de intervir na operação de tratamento de dados, a fim de reparar ou verificar o sistema ou o processo?

k. Os critérios exigem a aplicação de medidas técnicas e organizativas para garantir a minimização dos dados, por exemplo, dissociando ou separando os dados do titular dos dados, mediante processos de anonimização ou de pseudonimização ou ainda de isolamento dos sistemas de dados?

l. Os critérios exigem medidas técnicas para implementar a proteção de dados por defeito?

m. Os critérios exigem medidas técnicas e organizativas para implementar a proteção de dados desde a conceção, por exemplo, um sistema de gestão da proteção de dados para demonstrar, informar, controlar e fazer cumprir os requisitos em matéria de proteção de dados?

n. Os critérios exigem a adoção de medidas técnicas e organizativas para assegurar a formação e educação periódicas adequadas para o pessoal que tem acesso permanente ou regular aos dados pessoais?

o. Os critérios exigem medidas de revisão?

p. Os critérios exigem uma autoavaliação/auditoria interna?

q. Os critérios exigem a adoção de uma medida que garanta que os deveres relativos à notificação de uma violação de dados pessoais são efetuados em tempo útil e com o alcance adequado?

r. Os critérios exigem o estabelecimento e a verificação de procedimentos de gestão de incidentes?

s. Os critérios exigem o acompanhamento da evolução das questões relacionadas com a privacidade e a tecnologia, bem como a atualização do sistema em função das necessidades?

...

11 OUTRAS CARACTERÍSTICAS ESPECIAIS QUE RESPEITAM A PROTEÇÃO DOS DADOS

a. Os critérios exigem a aplicação de técnicas de reforço da proteção de dados? Tal poderia incluir critérios que exijam uma maior proteção dos dados, através da eliminação ou redução dos dados pessoais e/ou do risco para a proteção de dados.

- *Exemplo: Os critérios que exigem uma indissociação reforçada utilizando uma tecnologia de gestão da identidade centrada no utilizador, como a tecnologia «attribute-based credentials» (ABC), em vez de um método de gestão da identidade centrada na organização, iriam no sentido de uma técnica de reforço da proteção de dados.*

b. Os critérios exigem a realização de controlos reforçados dos titulares dos dados para facilitar a autodeterminação e a liberdade de escolha?

...

12 CRITÉRIOS PARA DEMONSTRAR A EXISTÊNCIA DE GARANTIAS ADEQUADAS PARA A TRANSFERÊNCIA DE DADOS PESSOAIS

Estes critérios serão tratados nas próximas diretrizes consagradas ao artigo 42.º, n.º 2.

13 CRITÉRIOS ADICIONAIS PARA UM SELO EUROPEU DE PROTEÇÃO DE DADOS

a. Os critérios preveem a cobertura de todos os Estados-Membros?

b. Os critérios podem ter em conta a legislação ou os cenários em matéria de proteção de dados dos Estados-Membros?

c. Os critérios exigem uma avaliação de cada ToE no que diz respeito às disposições setoriais da legislação dos Estados-Membros em matéria de proteção de dados?

d. Os critérios exigem que o responsável pelo tratamento ou o subcontratante forneçam informações aos titulares dos dados e às partes interessadas nas línguas dos Estados-Membros

e. sobre o tratamento/ToE?

f. sobre a documentação do tratamento/ToE?

g. sobre os resultados da avaliação?

...

14 AVALIAÇÃO GLOBAL DOS CRITÉRIOS

a. Os critérios abrangem integralmente o âmbito do mecanismo de certificação (ou seja, são critérios abrangentes) para oferecer garantias suficientes de que a certificação é de confiança?

- *Exemplo: Se o âmbito do mecanismo de certificação se centrar nas operações de tratamento de dados de saúde, deve ser garantido um nível elevado de proteção de dados mediante a definição de critérios que garantam, por exemplo, uma avaliação aprofundada e a aplicação de princípios de privacidade desde a conceção e de privacidade por defeito.*

b. Os critérios são consentâneos com a dimensão da operação de tratamento abrangida pelo âmbito do mecanismo de certificação, com a sensibilidade das informações e com o risco de tratamento?

c. São os critérios suscetíveis de melhorar a proteção dos dados dos responsáveis pelo tratamento e dos subcontratantes?

d. Os titulares dos dados irão beneficiar no que diz respeito aos seus direitos de ser informados, incluindo a explicação dos resultados pretendidos?