Linhas de orientação n.º 4/2018 relativas à acreditação dos organismos de certificação nos termos do artigo 43.º do Regulamento Geral sobre a Proteção de Dados (2016/679)

Versão 3.0

4 de junho de 2019

Translations proofread by EDPB Members.

This language version has not yet been proofread.

Adotado

Historial das versões

Versão 3.0	4 de junho de 2019	Inclusão do anexo 1 (versão 2.0 do anexo 1 adotada em 4 de junho de 2019 após consulta pública)
Versão 2.0	4 de dezembro de 2018	Adoção das orientações após consulta pública – na mesma data, foi adotado para consulta pública o anexo 1 (versão 1.0).
Versão 1.0	6 de fevereiro de 2018	Adoção das linhas de orientação pelo Grupo do Artigo 29.º (versão para consulta da publicação). Esta versão foi aprovada pelo CEPD em 25 de maio de 2018.

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,

Tendo em conta os resultados da consulta pública sobre as linhas de orientação realizada em fevereiro de 2018, e sobre o anexo, que decorreu entre 14 de dezembro de 2018 e 1 de fevereiro de 2019, em conformidade com o artigo 70.º, n.º 4, do RGPD,

ADOTOU AS SEGUINTES LINHAS DE ORIENTAÇÃO

1 INTRODUÇÃO

1. O Regulamento Geral de Proteção de Dados [Regulamento (UE) 2016/679] (doravante «RGPD»), que entrou em vigor em 25 de maio de 2018, fornece um quadro de conformidade em matéria de proteção de dados na Europa modernizado, assente na responsabilidade e nos direitos fundamentais. Há um conjunto de medidas destinadas a facilitar o cumprimento das disposições do RGPD que são fundamentais para este novo quadro. Entre elas incluem-se requisitos obrigatórios em circunstâncias específicas (incluindo a nomeação de encarregados da 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. No âmbito do estabelecimento de procedimentos de certificação e selos e marcas de proteção de dados, o artigo 43.º, n.º 1, do RGPD exige que os Estados-Membros garantam que os organismos de certificação que emitem a certificação nos termos do artigo 42.º, n.º 1, sejam acreditados pela autoridade de controlo competente ou pelo organismo nacional de acreditação, ou por ambos. Se a acreditação for realizada pelo organismo nacional de acreditação em conformidade com a norma ISO/IEC 17065/2012, também são de aplicar os requisitos adicionais estabelecidos pela autoridade de controlo competente.

3. A existência de procedimentos de certificação significativos pode melhorar a conformidade com o RGPD e a transparência para os titulares de dados e nas relações entre empresas, por exemplo entre os responsáveis pelo tratamento e os seus subcontratantes. Os responsáveis pelo tratamento e os subcontratantes beneficiarão de uma declaração emitida por uma terceira parte independente com a finalidade de demonstrar a conformidade das suas operações de tratamento[1].

4. Neste contexto, o Comité Europeu para a Proteção de Dados reconhece que é necessário fornecer linhas de orientação relativamente à acreditação. O valor e o objetivo particulares

[1] De acordo com o considerando 100 do RGPD o estabelecimento de procedimentos de certificação pode reforçar a transparência e o cumprimento do regulamento e permitir que os titulares de dados avaliem o nível de proteção de dados proporcionado pelos produtos e serviços em causa.

da acreditação residem no facto de esta fornecer uma declaração credível da competência dos organismos de certificação que permite gerar confiança no procedimento de certificação.

5. O objetivo das linhas de orientação é fornecer orientações sobre como interpretar e implementar as disposições do artigo 43.º do RGPD. Em especial, visam ajudar os Estados-Membros, as autoridades de controlo e os organismos nacionais de acreditação a estabelecer uma linha de base coerente e harmonizada para a acreditação dos organismos de certificação que emitem a certificação em conformidade com o RGPD.

2 ÂMBITO DE APLICAÇÃO DAS LINHAS DE ORIENTAÇÃO

6. As presentes linhas de orientação:

- definem o objetivo da acreditação no contexto do RGPD;
- explicam as vias disponíveis para acreditar os organismos de certificação nos termos do artigo 43.º, n.º 1, e identificam as principais questões a considerar;
- fornecem um quadro para estabelecer requisitos de acreditação adicionais quando a acreditação é tratada pelo organismo nacional de acreditação; e
- fornecem um quadro para estabelecer requisitos de acreditação quando a acreditação é tratada pela autoridade de controlo.

7. As linhas de orientação não constituem um manual de procedimentos para a acreditação dos organismos de certificação em conformidade com o RGPD, não criando uma nova norma técnica para a acreditação de organismos de certificação para efeitos do RGPD.

8. Estas linhas de orientação destinam-se:

- aos Estados-Membros, que devem garantir que os organismos de certificação sejam acreditados pela autoridade de controlo e/ou pelo organismo nacional de acreditação;
- aos organismos nacionais de acreditação que conduzem o processo de acreditação dos organismos de certificação nos termos do artigo 43.º, n.º 1, alínea b);
- à autoridade de controlo competente que especifica «requisitos adicionais» além dos previstos na norma ISO/IEC 17065/2012[2] quando a acreditação é realizada pelo organismo nacional de acreditação nos termos do artigo 43.º, n.º 1, alínea b);
- ao Comité Europeu para a Proteção de Dados na emissão de pareceres e na aprovação dos requisitos de acreditação das autoridades de controlo competentes nos termos do artigo 43.º, n.º 3, do artigo 70.º, n.º 1, alínea p), e do artigo 64.º, n.º 1, alínea c);
- à autoridade de controlo competente que especifica os requisitos de acreditação quando a acreditação é realizada pela autoridade de controlo nos termos do artigo 43.º, n.º 1, alínea a);
- a outras partes interessadas, como potenciais organismos de certificação ou proprietários de sistemas de certificação que estabelecem critérios e procedimentos de certificação[3].

[2] Organização Internacional de Normalização: Avaliação da conformidade – Requisitos para organismos de certificação de produtos, processos e serviços.

9. Definições

10. As definições que se seguem procuram promover um entendimento comum dos elementos básicos do processo de acreditação. Há que encará-las como pontos de referência sem a pretensão de serem incontestáveis. As seguintes definições baseiam-se em quadros regulamentares e normas existentes, especialmente nas disposições relevantes do RGPD e na norma ISO/IEC 17065/2012.

11. Para efeitos das presentes linhas de orientação, entende-se por:

12. «*acreditação*» de organismos de certificação: ver secção 3 sobre a interpretação de acreditação para efeitos do artigo 43.º do RGPD;

13. «*requisitos adicionais*», os requisitos estabelecidos pela autoridade de controlo competente e com base nos quais se realiza a acreditação[4];

14. «*certificação*», a avaliação e declaração[5] imparcial emitida por uma terceira parte de que o cumprimento dos critérios de certificação foi demonstrado;

15. «*organismo de certificação*», um organismo[6] terceiro de avaliação da conformidade[7] que efetue procedimentos de certificação[8];

16. «*sistema de certificação*», um sistema de certificação relacionado com produtos, processos e serviços específicos aos quais se aplicam os mesmos requisitos especificados, regras específicas e procedimentos[9];

17. «critérios» ou critérios de certificação, os critérios com base nos quais se realiza uma certificação (avaliação da conformidade)[10];

---

[3] O proprietário de um sistema é uma organização identificável que estabeleceu critérios de certificação e os requisitos de acordo com os quais a conformidade deve ser avaliada. A acreditação é da organização que realiza avaliações (artigo 43.º, n.º 4) de acordo com os requisitos do sistema de certificação e emite os certificados (ou seja, o organismo de certificação, também conhecido como organismo de avaliação da conformidade). A organização que realiza as avaliações pode ser a mesma organização que desenvolveu e que possui o sistema, mas pode haver acordos segundo os quais uma organização possui o sistema e outra(s) realiza(m) as avaliações.

[4] Artigo 43, n.os 1, 3 e 6.

[5] Observe-se que, de acordo com a norma ISO 17000, a declaração emitida por uma terceira parte (certificação) é aplicável a todos os objetos de avaliação da conformidade (5.5), exceto para os próprios organismos de avaliação da conformidade, aos quais a acreditação é aplicável (5.6).

[6] Ver a norma ISO 17000, 2.5: organismo que presta serviços de avaliação da conformidade; norma ISO 17011: organismo que presta serviços de avaliação da conformidade e que pode ser objeto de acreditação; norma ISO 17065, 3.12.

[7] A atividade de avaliação da conformidade por terceiros é efetuada por um organismo independente tanto da pessoa ou organismo que fornece o produto como dos interesses dos utilizadores do produto – ver a norma ISO 17000, 2.4.

[8] Artigo 42.º, n.os 1 e 5, do RGPD.

[9] Ver o ponto 3.9 em conjugação com o anexo B da norma ISO 17065.

[10] Ver o artigo 42.º, n.º 5.

18. «organismo nacional de acreditação», o único organismo num Estado-Membro, nomeado em conformidade com o Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, a proceder à acreditação com poderes de autoridade pública[11].

3 INTERPRETAÇÃO DO TERMO «ACREDITAÇÃO» PARA EFEITOS DO ARTIGO 43.º DO RGPD

19. O RGPD não fornece uma definição de «acreditação». O artigo 2.º, n.º 10, do Regulamento (CE) n.º 765/2008, que estabelece os requisitos gerais aplicáveis a acreditações, define a acreditação como

20. «a declaração por um organismo nacional de acreditação de que um organismo de avaliação da conformidade cumpre, para executar as atividades específicas de avaliação da conformidade, os requisitos definidos em normas harmonizadas e, se for esse o caso, quaisquer requisitos adicionais, nomeadamente os estabelecidos em sistemas setoriais».

21. Nos termos da norma ISO/IEC 17011, entende-se por

22. acreditação, a declaração emitida por uma terceira parte em relação a um organismo de avaliação da conformidade, que comprova formalmente a sua competência para executar funções específicas de avaliação da conformidade.

23. O artigo 43.º, n.º 1, prevê:

24. «Sem prejuízo das atribuições e poderes da autoridade de controlo competente nos termos dos artigos 57.º e 58.º, um organismo de certificação que tenha um nível adequado de competência em matéria de proteção de dados emite e renova a certificação, após informar a autoridade de controlo para que esta possa exercer as suas competências nos termos do artigo 58.º, n.º 2, alínea h), sempre que necessário. Os Estados-Membros asseguram que estes organismos de certificação são acreditados:

    (a) Pela autoridade de controlo que é competente nos termos do artigo 55.º ou 56.º;
    (b) Pelo organismo nacional de acreditação, designado nos termos do Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, em conformidade com a norma EN-ISO/IEC 17065/2012 e com os requisitos adicionais estabelecidos pela autoridade de controlo que é competente nos termos do artigo 55.º ou 56.º.»

25. No que diz respeito ao RGPD, os requisitos de acreditação serão orientados:

- pela norma ISO/IEC 17065/2012 e pelos «requisitos adicionais» estabelecidos pela autoridade de controlo competente nos termos do artigo 43.º, n.º 1, alínea b), quando a acreditação é realizada pelo organismo nacional de acreditação e pela autoridade de controlo, quando é a própria a realizar a acreditação.

26. Em ambos os casos, os requisitos consolidados devem englobar os requisitos referidos no artigo 43.º, n.º 2.

[11] Ver o artigo 2.º, n.º 11, do Regulamento (CE) n.º 765/2008.

27. O Comité Europeu para a Proteção de Dados reconhece que o objetivo da acreditação é fornecer uma declaração credível da competência de um organismo para realizar a certificação (atividades de avaliação da conformidade)[12]. Nos termos do RGPD, entende-se por «acreditação»:

28. uma declaração[13] emitida por um organismo nacional de acreditação e/ou por uma autoridade de controlo, de que um organismo de certificação[14] está qualificado para realizar a certificação nos termos dos artigos 42.º e 43.º do RGPD, levando em conta a norma ISO/IEC 17065/2012 e os requisitos adicionais estabelecidos pela autoridade de controlo e/ou pelo Comité.

4 ACREDITAÇÃO NOS TERMOS DO ARTIGO 43.º, N.º 1, DO RGPD

29. O artigo 43.º, n.º 1, reconhece a existência de várias opções para a acreditação de organismos de certificação. O RGPD exige que as autoridades de controlo e os Estados-Membros definam o processo para a acreditação dos organismos de certificação. A presente secção define as vias de acreditação previstas no artigo 43.º.

4.1 Função dos Estados-Membros

30. O artigo 43.º, n.º 1, exige que os Estados-Membros assegurem que os organismos de certificação sejam acreditados, mas permite que cada Estado-Membro determine quem será responsável por conduzir a avaliação necessária à certificação. Com base no artigo 43.º, n.º 1, estão disponíveis três opções; a acreditação é conduzida:

(1) apenas pela autoridade de controlo, com base nos próprios requisitos;
(2) apenas pelo organismo nacional de acreditação designado nos termos do Regulamento (CE) n.º 765/2008 e com base na norma ISO/IEC 17065/2012 e com os requisitos adicionais estabelecidos pela autoridade de controlo competente; ou
(3) pela autoridade de controlo e o organismo nacional de acreditação (e em conformidade com todos os requisitos referidos no n.º 2 acima).

31. Cabe a cada Estado-Membro decidir se o organismo nacional de acreditação, a autoridade de controlo, ou ambos, levarão a cabo essas atividades de acreditação, mas, em qualquer caso, deve assegurar que eles disponham dos recursos adequados[15].

4.2 Interação com o Regulamento (CE) n.º 765/2008

32. O Comité Europeu para a Proteção de Dados observa que o artigo 2.º, n.º 11, do Regulamento (CE) n.º 765/2008 define um organismo nacional de acreditação como «o único organismo num Estado-Membro a proceder à acreditação com poderes de autoridade pública».

[12] Ver considerando 15 do Regulamento (CE) n.º 765/2008.
[13] Ver o artigo 2.º, n.º 10, do Regulamento (CE) n.º 765/2008 do Parlamento Europeu e do Conselho, de 9 de julho de 2008, que estabelece os requisitos de acreditação e fiscalização do mercado relativos à comercialização de produtos.
[14] Ver a definição do termo «acreditação» de acordo com a norma ISO 17011.
[15] Ver o artigo 4.º, n.º 9, do Regulamento (CE) n.º 765/2008.

33. O artigo 2.º, n.º 11, pode ser considerado incompatível com o artigo 43.º, n.º 1, do RGPD, que permite a acreditação por um organismo que não seja o organismo nacional de acreditação do Estado-Membro. O Comité Europeu para a Proteção de Dados considera que a legislação da UE visa a derrogação do princípio geral de que a acreditação seja conduzida exclusivamente pela autoridade nacional de acreditação, conferindo às autoridades de controlo o mesmo poder no que diz respeito à acreditação dos organismos de certificação. Por conseguinte, o artigo 43.º, n.º 1, constitui uma *lex specialis* em relação ao artigo 2.º, n.º 11, do Regulamento (CE) n.º 765/2008.

4.3 A função do organismo nacional de acreditação

34. O artigo 43.º, n.º 1, alínea b), prevê que o organismo nacional de acreditação acredita os organismos de certificação em conformidade com a norma ISO/IEC 17065/2012 e com os requisitos adicionais estabelecidos pela autoridade de controlo competente.

35. Por razões de clareza, o Comité Europeu para a Proteção de Dados observa que a referência específica ao «n.º 1, alínea b),» no artigo 43.º, n.º 3, pressupõe que «esses requisitos» correspondem aos «requisitos adicionais» estabelecidos pela autoridade de controlo competente nos termos do artigo 43.º, n.º 1, alínea b), e aos requisitos estabelecidos no artigo 43.º, n.º 2.

36. No processo de acreditação, os organismos nacionais de acreditação devem aplicar os requisitos adicionais que serão previstos pelas autoridades de controlo.

37. Um organismo de certificação com acreditação com base na norma ISO/IEC 17065/2012 para sistemas de certificação não relacionados com o RGPD que pretenda alargar o âmbito da sua acreditação de forma a abranger a certificação emitida de acordo com o RGPD terá de cumprir os requisitos adicionais estabelecidos pela autoridade de controlo, se a acreditação for tratada pelo organismo nacional de acreditação. Se a acreditação para a certificação ao abrigo do RGPD for oferecida apenas pela autoridade de controlo competente, um organismo de certificação que solicite a acreditação deverá cumprir os requisitos estabelecidos pela respetiva autoridade de controlo.

4.4 A função da autoridade de controlo

38. O Comité Europeu para a Proteção de Dados observa que o artigo 57.º, n.º 1, alínea q), estabelece que a autoridade de controlo *conduz* o processo de acreditação de um organismo de certificação nos termos do artigo 43.º como uma «atribuição da autoridade de controlo» nos termos do artigo 57.º, e o artigo 58.º, n.º 3, alínea e), estabelece que a autoridade de controlo dispõe dos poderes consultivos e de autorização para acreditar organismos de certificação nos termos do artigo 43.º. A redação do artigo 43.º, n.º 1, permite alguma flexibilidade, e a função de acreditação da autoridade de controlo apenas deve ser interpretada como uma atribuição nos casos em que seja apropriado. Para clarificar este ponto, pode utilizar-se a legislação do Estado-Membro. No entanto, no processo de acreditação por um organismo nacional de acreditação, o artigo 43.º, n.º 2, alínea a), exige que o organismo de certificação demonstre que goza de independência e dispõe dos

conhecimentos necessários em relação ao objeto do procedimento de certificação que oferece, de forma satisfatória para a autoridade de controlo competente[16].

39. Se um Estado-Membro determinar que os organismos de certificação devem ser acreditados pela autoridade de controlo, cabe a esta estabelecer requisitos de acreditação, incluindo, entre outros, os requisitos especificados no artigo 43.º, n.º 2. Em comparação com as obrigações relativas à acreditação de organismos de certificação pelos organismos nacionais de acreditação, o artigo 43.º fornece menos instruções sobre os requisitos de acreditação quando é a autoridade de controlo a conduzir o processo de acreditação. A fim de contribuir para uma abordagem harmonizada da acreditação, os critérios de acreditação utilizados pela autoridade de controlo devem nortear-se pela norma ISO/IEC 17065 e ser complementados pelos requisitos adicionais estabelecidos por uma autoridade de controlo nos termos do artigo 43.º, n.º 1, alínea b). O Comité Europeu para a Proteção de Dados observa que o artigo 43.º, n.º 2, alíneas a) a e), reflete e especifica requisitos da norma ISO 17065, o que contribuirá para uma maior coerência.

40. Se um Estado-Membro determinar que os organismos de certificação devem ser acreditados pelos organismos nacionais de acreditação, a autoridade de controlo deve estabelecer requisitos adicionais para complementar as convenções de acreditação existentes referidas no Regulamento (CE) n.º 765/2008 (cujos artigos 3.º a 14.º dizem respeito à organização e ao funcionamento da acreditação dos organismos de avaliação da conformidade) e nas regras técnicas que descrevem os métodos e procedimentos dos organismos de certificação. Tendo em conta este facto, o Regulamento (CE) n.º 765/2008 fornece mais orientações: o artigo 2.º, n.º 10, define a acreditação e refere-se a «normas harmonizadas» e a «quaisquer requisitos adicionais, nomeadamente os estabelecidos em sistemas setoriais». Conclui-se que os requisitos adicionais estabelecidos pela autoridade de controlo devem incluir requisitos específicos e destinar-se a facilitar a avaliação, entre outros, da independência e do nível de conhecimentos dos organismos de certificação em matéria de proteção de dados, por exemplo, a sua capacidade para avaliar e certificar operações de tratamento de dados pessoais por parte dos responsáveis pelo tratamento e subcontratantes nos termos do artigo 42.º, n.º 1. Tal inclui a competência exigida para os sistemas setoriais e no que diz respeito à proteção dos direitos e liberdades fundamentais das pessoas singulares e, em particular, ao seu direito à proteção de dados pessoais[17]. O anexo das presentes linhas de orientação pode ajudar a informar as autoridades de controlo competentes quando estabelecem os «requisitos adicionais», em conformidade com o artigo 43.º, n.º 1, alínea b), e o artigo 43.º, n.º 3.

41. O artigo 43.º, n.º 6, prevê que «[o]s requisitos referidos no n.º 3 do presente artigo, e os critérios referidos no artigo 42.º, n.º 5, são publicados pela autoridade de controlo sob uma forma facilmente acessível». Por conseguinte, para assegurar a transparência, devem ser publicados todos os critérios e requisitos aprovados por uma autoridade de controlo. Em termos de qualidade e confiança nos organismos de certificação, seria desejável que todos os requisitos de acreditação estivessem prontamente disponíveis ao público.

4.5 Autoridade de controlo que atua como organismo de certificação

[16] Os requisitos adicionais estabelecidos pela autoridade de controlo nos termos do artigo 43.º, n.º 1, alínea b), devem especificar requisitos de independência e de conhecimentos. Ver também o anexo 1 das presentes linhas de orientação.
[17] Artigo 1.º, n.º 2, do RGPD.

42. O artigo 42.º, n.º 5, estabelece que uma autoridade de controlo pode emitir certificações, mas o RGPD não exige que esta seja acreditada para cumprir os requisitos do Regulamento (CE) n.º 765/2008. O Comité Europeu para a Proteção de Dados observa que o artigo 43.º, n.º 1, alínea a), e, especificamente, o artigo 58.º, n.º 2, alínea h), e n.º 3, alíneas a), e) e f), autorizam as autoridades de controlo a proceder à acreditação e à certificação e, ao mesmo tempo, a prestar aconselhamento e, conforme aplicável, retirar certificações ou solicitar que os organismos de certificação não emitam certificações.

43. Pode haver situações em que a separação das funções e dos deveres de acreditação e certificação seja apropriada ou necessária, por exemplo, se uma autoridade de controlo e outros organismos de certificação coexistirem num Estado-Membro e ambos emitirem a mesma série de certificações. Por conseguinte, as autoridades de controlo devem tomar medidas organizacionais suficientes para separar as atribuições ao abrigo do RGPD de forma a consolidar e facilitar os procedimentos de certificação, tomando precauções para evitar conflitos de interesse que possam surgir dessas atribuições. Além disso, os Estados-Membros e as autoridades de controlo devem ter em conta o nível europeu harmonizado ao formular a legislação e os procedimentos nacionais relativos à acreditação e certificação em conformidade com o RGPD.

4.6 Requisitos de acreditação

44. O anexo das presentes linhas de orientação fornece orientações sobre o modo de identificar requisitos adicionais de acreditação. Identifica as disposições pertinentes do RGPD e sugere requisitos que as autoridades de controlo e os organismos nacionais de acreditação deverão considerar para garantir a conformidade com o RGPD.

45. Conforme estabelecido acima, quando os organismos de certificação são acreditados pelo organismo nacional de acreditação nos termos do Regulamento (CE) n.º 765/2008, a norma ISO/IEC 17065/2012 será a norma de acreditação pertinente, complementarmente aos requisitos adicionais estabelecidos pela autoridade de controlo. O artigo 43.º, n.º 2, reflete as disposições genéricas da norma ISO/IEC 17065/2012 à luz da proteção dos direitos fundamentais nos termos do RGPD. O enquadramento do anexo utiliza o artigo 43.º, n.º 2, e a ISO/IEC 17065/2012 como base para a identificação de requisitos, além de outros critérios relacionados com a avaliação dos conhecimentos em matéria de proteção de dados dos organismos de certificação e a sua capacidade de respeitar os direitos e liberdades de pessoas singulares no que diz respeito ao tratamento de dados pessoais, tal como consagrado no RGPD. O Comité Europeu para a Proteção de Dados salienta que está especialmente focalizado em garantir que os organismos de certificação tenham um nível adequado de competência em matéria de proteção de dados, em conformidade com o artigo 43.º, n.º 1.

46. Os requisitos adicionais de acreditação estabelecidos pela autoridade de controlo serão aplicados a todos os organismos de certificação que solicitem a acreditação. O organismo de acreditação avaliará se o organismo de certificação é competente para realizar a atividade de certificação, de acordo com os requisitos adicionais e o objeto da certificação. Deve haver referências a setores ou áreas de certificação específicos para os quais o organismo de certificação é acreditado.

47. O Comité Europeu para a Proteção de Dados observa ainda que, além dos requisitos da norma ISO/IEC 17065/2012, também é exigida competência especial no domínio da proteção de dados, se outros organismos externos, como laboratórios ou auditores, executarem

partes ou componentes de atividades de certificação em nome de um organismo de certificação acreditado. Nesses casos, não é possível a acreditação desses organismos externos ao abrigo do RGPD. No entanto, a fim de garantir a adequação desses organismos em relação à sua atividade em nome dos organismos de certificação acreditados, é necessário que o organismo de certificação acreditado assegure que os conhecimentos em matéria de proteção de dados exigidos ao organismo acreditado também se apliquem e sejam demonstrados no caso do organismo externo, em relação à atividade em causa realizada.

48. O quadro para identificar os requisitos adicionais de acreditação, conforme apresentado no anexo das presentes linhas de orientação, não constitui um manual de procedimentos para o processo de acreditação realizado pelo organismo nacional de acreditação ou pela autoridade de controlo. Contém orientações sobre a estrutura e a metodologia e, portanto, um conjunto de ferramentas para as autoridades de controlo na identificação dos requisitos adicionais para a acreditação.

ANEXO 1

O anexo 1 fornece orientações para a especificação de requisitos de acreditação «adicionais» no que diz respeito à norma ISO/IEC 17065/2012 e em conformidade com o artigo 43.º, n.º 1, alínea b), e o artigo 43.º, n.º 3, do RGPD.

Este anexo apresenta sugestões de requisitos que uma autoridade de controlo da proteção de dados deve elaborar e que se aplicam durante a acreditação de um organismo de certificação pelo organismo nacional de acreditação ou pela autoridade de controlo competente.[18] Estes requisitos adicionais deverão ser comunicados ao Comité Europeu para a Proteção de Dados antes da aprovação nos termos do artigo 64.º, n.º 1, alínea c).

O presente anexo deve ser lido em conjunto com a norma ISO/IEC 17065/2012. Os números das secções utilizados neste documento correspondem aos números utilizados na norma ISO/IEC 17065/2012. Quando as autoridades de controlo realizam a acreditação nos termos do artigo 43.º, n.º 1, alínea a), as boas práticas ditam que se siga esta abordagem sempre que for prático. Tal contribuirá para uma acreditação harmonizada na UE.

Não obstante as orientações que se seguem ou a ausência de orientações sobre qualquer ponto da norma ISO/IEC 17065/2012, a autoridade de controlo competente pode formular outros requisitos adicionais relativos a esses pontos desde que estejam em conformidade com o direito nacional.

0 PREFIXO

[Esta secção destina-se aos Termos de Cooperação eventualmente acordados, se for esse o caso, entre o organismo nacional de acreditação e a autoridade de controlo da proteção de dados, como, por exemplo, quem deve ser responsável por receber os requerimentos ou como organizar o reconhecimento dos critérios aprovados no âmbito do processo de acreditação.]

1 ÂMBITO DE APLICAÇÃO[19]

O âmbito de aplicação da norma ISO/IEC 17065/2012 é aplicado em conformidade com o RGPD. As linhas de orientação sobre a acreditação e a certificação fornecem mais informações. Há que tomar em conta o âmbito de aplicação de um procedimento de certificação (por exemplo, a certificação de operações de tratamento de serviços na nuvem) na avaliação levada a cabo pelo organismo nacional de acreditação e pela autoridade de controlo competente durante o processo de acreditação, sobretudo no que diz respeito aos critérios, aos conhecimentos especializados e à metodologia de avaliação. O vasto âmbito de aplicação da norma ISO/IEC 17065/2012, que abrange produtos, processos e serviços, não deve diminuir nem desprezar os requisitos do RGPD, por exemplo, um mecanismo de governação não pode ser o único elemento de um procedimento de certificação, dado que a certificação tem de incluir o tratamento de dados pessoais, ou seja, operações de tratamento. Por força do artigo 42.º, n.º 1, a certificação nos termos do RGPD só é aplicável às operações de tratamento dos responsáveis pelo tratamento e dos subcontratantes.

[18] Para informações sobre o processo de aprovação dos critérios de certificação, consultar a secção 4 das linhas de orientação relativas à certificação.
[19] A numeração refere-se à norma ISO/IEC 17065/2012.

2 REFERÊNCIAS NORMATIVAS

O RGPD tem precedência sobre a norma ISO/IEC 17065/2012. Se os requisitos adicionais ou um mecanismo de certificação fizerem referência a outras normas ISO, estas são interpretadas em consonância com os requisitos estabelecidos no RGPD.

3 TERMOS E DEFINIÇÕES

No contexto do presente anexo, aplicam-se os termos e as definições das linhas de orientação relativas à acreditação (WP 261) e à certificação (CEPD 1/2018), tendo precedência sobre as definições da ISO.

4 REQUISITOS GERAIS DE ACREDITAÇÃO

4.1 Questões jurídicas e contratuais

4.1.1 Responsabilidade legal

Um organismo de certificação deve poder demonstrar (em todas as ocasiões) ao organismo nacional de acreditação ou à autoridade de controlo competente que dispõe de procedimentos atualizados que comprovem o cumprimento das responsabilidades legais estipuladas nos termos da acreditação, incluindo os requisitos adicionais relativos à aplicação do Regulamento (UE) 2016/679. De notar que, visto que o próprio organismo de certificação é um responsável pelo tratamento/subcontratante, será capaz de apresentar provas da existência de procedimentos e medidas em conformidade com o Regulamento (UE) 2016/679, especificamente para o controlo e gestão dos dados pessoais da organização dos clientes no âmbito do processo de certificação.

A autoridade de controlo competente pode decidir adicionar outros requisitos e procedimentos para averiguar o cumprimento do RGPD por parte dos organismos de certificação antes da acreditação.

4.1.2 Acordo do certificação («AC»)

Os requisitos mínimos para um acordo de certificação são complementados pelos seguintes pontos:

Além dos requisitos da norma ISO/IEC 17065/2012, o organismo de certificação deve demonstrar que os seus acordos de certificação:

1. Exigem que o requerente cumpra sempre tanto os requisitos de certificação gerais na aceção do ponto 4.1.2.2, alínea a), da norma ISO/IEC 17065/2012, como os critérios aprovados pela autoridade de controlo competente ou pelo CEPD, em conformidade com o artigo 43.º, n.º 2, alínea b), e o artigo 42.º, n.º 5;
2. Exigem que o requerente manifeste total transparência perante a autoridade de controlo competente a respeito do procedimento de certificação, incluindo assuntos contratualmente confidenciais relacionados com o cumprimento da proteção de dados nos termos do artigo 42.º, n.º 7, e do artigo 58.º, n.º 1, alínea c);
3. Não reduzem a responsabilidade do requerente no cumprimento do Regulamento (UE) 2016/679, sem prejuízo das tarefas e poderes da autoridade de controlo competente em consonância com o artigo 42.º, n.º 5;
4. Exigem que o requerente forneça ao organismo de certificação as informações e o acesso às atividades de tratamento necessários à execução do procedimento de certificação nos termos do artigo 42.º, n.º 6;

5. Exigem que o requerente cumpra os prazos e procedimentos aplicáveis. O acordo de certificação tem de prever a obrigação de respeitar e cumprir os prazos e procedimentos resultantes, por exemplo, do programa de certificação ou de outros regulamentos;
6. Relativamente ao ponto 4.1.2.2, alínea c), n.º 1, da norma ISO/IEC 17065/2012, estabelecem as regras de validade, renovação e revogação nos termos do artigo 42.º, n.º 7, e do artigo 43.º, n.º 4, incluindo as regras que definem intervalos apropriados para a reavaliação ou revisão (periodicidade) em consonância com o artigo 42.º, n.º 7;
7. Permitem que o organismo de certificação divulgue todas as informações necessárias para conceder a certificação nos termos do artigo 42.º, n.º 8, e do artigo 43.º, n.º 5;
8. Incluem regras sobre as precauções necessárias à investigação de reclamações na aceção do ponto 4.1.2.2, alínea c), n.º 2, e ainda alínea j), e contêm igualmente afirmações explícitas sobre a estrutura e o procedimento para a gestão de reclamações em conformidade com o artigo 43.°, n.º 2, alínea d);
9. Além dos requisitos mínimos referidos no ponto 4.1.2.2 da norma ISO/IEC 17065/2012, se as consequências da revogação ou suspensão da acreditação do organismo de certificação tiverem repercussões para o cliente, caberá igualmente tê-las em conta;
10. Exigem que o requerente informe o organismo de certificação em caso de alterações significativas na sua situação efetiva ou jurídica e nos produtos, processos e serviços a que a certificação diga respeito.

4.1.3 Utilização de selos e marcas de proteção de dados

Os certificados, selos e marcas são apenas utilizados em cumprimento dos artigos 42.º e 43.º e das linhas de orientação relativas à acreditação e certificação.

4.2 Gestão da imparcialidade

O organismo de acreditação deve assegurar que, além do requisito estipulado no ponto 4.2. da norma ISO/IEC 17065/2012:

1. O organismo de certificação cumpre os requisitos adicionais da autoridade de controlo competente (nos termos do artigo 43.º, n.º 1, alínea b));
    - **a.** em consonância com o artigo 43.º, n.º 2, alínea a), o organismo de certificação fornece provas separadas da sua independência. Tal aplica-se em particular às provas relativas ao financiamento do organismo de certificação, na medida em que diga respeito à garantia de imparcialidade;
    - **b.** as suas tarefas e obrigações não resultam num conflito de interesses nos termos do artigo 43.º, n.º 2, alínea e);
2. O organismo de certificação não tem uma ligação relevante com o cliente que avalia.

4.3 Responsabilidade e financiamento

O organismo de acreditação deve assegurar regularmente que, além do requisito estipulado no ponto 4.3.1 da norma ISO/IEC 17065/2012, o organismo de certificação dispõe de medidas apropriadas (por exemplo, seguro ou reservas) para cobrir as suas responsabilidades nas regiões geográficas em que opera.

4.4 Condições de não discriminação

A autoridade de controlo poderá formular requisitos adicionais se estiverem em conformidade com o direito nacional.

4.5 Confidencialidade

A autoridade de controlo poderá formular requisitos adicionais se estiverem em conformidade com o direito nacional.

4.6 Informações disponíveis ao público

O organismo de acreditação deve exigir ao organismo de certificação que, além do requisito estipulado no ponto 4.6 da norma ISO/IEC 17065/2012, no mínimo:

1. Todas as versões (a versão atual e as anteriores) dos critérios aprovados utilizados na aceção do artigo 42.º, n.º 5, sejam publicadas e estejam facilmente disponíveis ao público, bem como todos os procedimentos de certificação, indicando, em geral, o respetivo período de validade;
2. As informações sobre os processos de gestão de reclamações e respetivos recursos sejam disponibilizadas ao público nos termos do artigo 43.º, n.º 2, alínea d).

5 REQUISITOS ESTRUTURAIS, ARTIGO 43.º, N.º 4 [«CORRETA» AVALIAÇÃO]

5.1 Estrutura organizacional e direção de topo

A autoridade de controlo poderá formular requisitos adicionais.

5.2 Mecanismos para salvaguardar a imparcialidade

A autoridade de controlo poderá formular requisitos adicionais.

6 REQUISITOS EM MATÉRIA DE RECURSOS

6.1 Certificação do pessoal do organismo

O organismo de acreditação deve assegurar que, além do requisito estipulado no ponto 6 da norma ISO/IEC 17065/2012, o pessoal de cada organismo de certificação:

1. Tenha demonstrado conhecimentos especializados (conhecimentos e experiência) apropriados e contínuos em relação à proteção de dados, nos termos do artigo 43.º, n.º 1;
2. Tenha independência e conhecimentos especializados contínuos em relação ao objeto da certificação, nos termos do artigo 43.º, n.º 2, alínea a), e não tenha um conflito de interesses nos termos do artigo 43.º, n.º 2, alínea e);
3. Se comprometa a respeitar os critérios referidos no artigo 42.º, n.º 5, nos termos do artigo 43.º, n.º 2, alínea b);
4. Tenha conhecimentos relevantes e apropriados e experiência na aplicação da legislação sobre proteção de dados;
5. Tenha conhecimentos relevantes e apropriados e experiência em medidas técnicas e organizacionais para a proteção de dados, conforme relevante;
6. Tenha capacidade para demonstrar experiência nos domínios mencionados nos requisitos adicionais 6.1.1, 6.1.4 e 6.1.5, especificamente:

Relativamente ao pessoal com conhecimentos técnicos especializados:

- Tenha obtido uma qualificação profissional numa área de especialização técnica relevante de, pelo menos, QEQ[20] nível 6 ou um título protegido reconhecido (por exemplo, Dipl. Eng.) na profissão regulamentada relevante ou tenha experiência profissional significativa;
- O pessoal responsável pelas decisões de certificação precisa de ter experiência profissional significativa na identificação e implementação de medidas de proteção de dados;
- O pessoal responsável pelas avaliações precisa de ter experiência profissional na proteção de dados técnicos, bem como conhecimentos e experiência em procedimentos comparáveis (por exemplo, certificações/auditorias), e tem de estar registado conforme aplicável.

O pessoal deve demonstrar que possui conhecimentos específicos em competências técnicas e de auditoria através de desenvolvimento profissional contínuo.

Relativamente ao pessoal com conhecimentos jurídicos especializados:

- Curso de Direito numa universidade reconhecida pela UE ou a nível nacional durante pelo menos oito semestres, incluindo o grau académico de Mestre (LL.M.) ou equivalente, ou experiência profissional significativa;
- O pessoal responsável pelas decisões de certificação deve demonstrar experiência profissional significativa na legislação sobre a proteção de dados e estar registado de acordo com as exigências do respetivo Estado-Membro;
- O pessoal responsável pelas avaliações deve demonstrar pelo menos dois anos de experiência profissional em legislação sobre a proteção de dados, bem como conhecimentos e experiência em procedimentos comparáveis (por exemplo, certificações/auditorias), e estar registado, quando exigido pelo Estado-Membro em questão.
    - O pessoal deve demonstrar que possui conhecimentos específicos em competências técnicas e de auditoria através de desenvolvimento profissional contínuo.

6.2 Recursos para avaliação

A autoridade de controlo poderá formular requisitos adicionais se estiverem em conformidade com o direito nacional.

7 REQUISITOS PROCESSUAIS, ARTIGO 43.º, N.º 2, ALÍNEAS C) E D)

7.1 Aspetos gerais

O organismo de acreditação, além do requisito estipulado na secção 7.1 da norma ISO/IEC 17065/2012, deve assegurar o seguinte:

1. Os organismos de certificação cumprem os requisitos adicionais da autoridade de controlo competente (nos termos do artigo 43.º, n.º 1, alínea b)) quando apresentam o seu requerimento, por forma que as tarefas e obrigações não resultem num conflito de interesses nos termos do artigo 43.º, n.º 2, alínea b);
2. Notificar as autoridades de controlo relevantes antes de um organismo de certificação começar a utilizar um Selo Europeu de Proteção de Dados aprovado num novo Estado-Membro a partir de um gabinete satélite.

[20] Consultar a ferramenta de comparação do quadro europeu de qualificações em https://ec.europa.eu/ploteus/en/compare?

7.2 Requerimento

Além do ponto 7.2 da norma ISO/IEC 17065/2012, deve exigir-se o seguinte:

1. O objeto da certificação (Alvo de Avaliação, AA) tem de estar descrito em detalhe no requerimento. Esses detalhes incluem as interfaces e transferências para outros sistemas e organizações, protocolos e outras garantias;
2. O requerimento deve especificar se há recurso a subcontratantes e, quando os subcontratantes são o requerente, devem descrever-se as suas responsabilidades e tarefas, além de que o requerimento deve conter o(s) contrato(s) entre o responsável pelo tratamento/subcontratante em questão.

7.3 Apreciação do requerimento

Além do ponto 7.3 da norma ISO/IEC 17065/2012, deve exigir-se o seguinte:

1. O acordo de certificação define os métodos de avaliação vinculativos relativamente ao Alvo de Avaliação (AA);
2. A avaliação referida no ponto 7.3, alínea e), relativa à existência ou não de conhecimentos suficientes, toma em consideração os conhecimentos tanto técnicos como jurídicos no domínio da proteção de dados numa medida apropriada.

7.4 Avaliação

Além do ponto 7.4 da norma ISO/IEC 17065/2012, os mecanismos de certificação deverão descrever métodos de avaliação suficientes para avaliar o cumprimento das operações de tratamento em função dos critérios de certificação, incluindo, por exemplo, quando aplicável:

1. Um método para avaliar a necessidade e proporcionalidade das operações de tratamento quanto à sua finalidade e aos titulares dos dados em questão;
2. Um método para avaliar a cobertura, composição e avaliação de todos os riscos considerados pelo responsável pelo tratamento e subcontratante a respeito das consequências legais por força dos artigos 30.º, 32.º, 35.º e 36.º do RGPD e a respeito da definição de medidas técnicas e organizacionais nos termos dos artigos 24.º, 25.º e 32.º do RGPD, na medida em que os artigos supramencionados se apliquem ao objeto da certificação;
3. Um método para avaliar as medidas jurídicas corretivas, incluindo garantias, salvaguardas e procedimentos para assegurar a proteção dos dados pessoais no contexto do tratamento a atribuir ao objeto da certificação e para demonstrar o cumprimento dos requisitos legais estipulados nos critérios; e
4. Documentação dos métodos e conclusões.

O organismo de certificação deve ser obrigado a assegurar que estes métodos de avaliação sejam normalizados e geralmente aplicáveis, permitindo a utilização de métodos de avaliação comparáveis para AA comparáveis. Qualquer desvio deste procedimento tem de ser justificado pelo organismo de certificação.

Além do ponto 7.4.2 da norma ISO/IEC 17065/2012, deve permitir-se que a avaliação fique a cargo de peritos externos reconhecidos pelo organismo de certificação.

Além do ponto 7.4.5 da norma ISO/IEC 17065/2012, deve exigir-se que a certificação em matéria de proteção de dados em conformidade com os artigos 42.º e 43.º do RGPD, a qual já abrange uma parte do objeto da certificação, possa ser incluída numa certificação atual. Porém, não será suficiente para substituir plenamente as avaliações (parciais). O organismo de certificação será obrigado a

verificar o cumprimento dos critérios. O reconhecimento implica a existência de um relatório de avaliação completo ou a disponibilidade de informações que permitam uma avaliação da atividade de certificação anterior e os respetivos resultados. Uma declaração de certificação ou certificados de certificação semelhantes não devem ser considerados suficientes para substituir um relatório.

Além do ponto 7.4.6 da norma ISO/IEC 17065/2012, deverá exigir-se que o organismo de certificação estabeleça em detalhe, no seu procedimento de certificação, em que medida a informação exigida no ponto 7.4.6 informa o cliente (requerente da certificação) sobre as eventuais não conformidades detetadas no âmbito de um procedimento de certificação. Neste contexto, importa definir, no mínimo, a natureza e a tempestividade dessa informação.

Além do ponto 7.4.9 da norma ISO/IEC 17065/2012, deve exigir-se que a autoridade de controlo da proteção de dados tenha pleno acesso à documentação necessária mediante pedido.

7.5 Revisão

Além do ponto 7.5 da norma ISO/IEC 17065/2012, são necessários procedimentos para a concessão, revisão regular e revogação das respetivas certificações por força do artigo 43.º, n.º 2, e do artigo 43.º, n.º 3.

7.6 Decisão de certificação

Além do ponto 7.6.1 da norma ISO/IEC 17065/2012, o organismo de certificação deve ser obrigado a estabelecer em detalhe, nos seus procedimentos, a forma como a sua independência e responsabilidade relativamente a decisões de certificação individuais são asseguradas.

7.7 Documentação de certificação

Além do ponto 7.7.1.e da norma ISO/IEC 17065/2012 e em conformidade com o artigo 42.º, n.º 7, do RGPD, cabe exigir que o período de validade das certificações não ultrapasse os três anos.

Além do ponto 7.7.1.e da norma ISO/IEC 17065/2012, deve exigir-se que o período do controlo pretendido na aceção da secção 7.9 também seja documentado.

Além do ponto 7.7.1.f da norma ISO/IEC 17065/2012, o organismo de certificação deve ser obrigado a identificar o objeto da certificação na documentação de certificação (indicando o estado da versão ou características semelhantes, se aplicável).

7.8 Diretório de produtos certificados

Além do ponto 7.8 da norma ISO/IEC 17065/2012, o organismo de certificação deve ser obrigado a manter a informação sobre produtos, processos e serviços certificados disponível interna e publicamente. O organismo de certificação fornecerá ao público um resumo do relatório de avaliação. O objetivo desse resumo é reforçar a transparência em termos do objeto da certificação e das modalidades de avaliação. O resumo elucidará questões como:

(a) O âmbito da certificação e uma descrição significativa do objeto da certificação (AA);

(b) Os respetivos critérios da certificação (incluindo o estado da versão ou o estado funcional);

(c) Os métodos de avaliação e testes realizados; e

(d) O(s) resultado(s).

Além do ponto 7.8 da norma ISO/IEC 17065/2012 e por força do artigo 43.º, n.º 5, do RGPD, o organismo de certificação deve informar as autoridades de controlo competentes sobre os motivos da concessão ou revogação da certificação solicitada.

7.9 Supervisão

Além dos pontos 7.9.1, 7.9.2 e 7.9.3 da norma ISO/IEC 17065/2012, e de acordo com o artigo 43.º, n.º 2, alínea c), do RGPD, cumpre exigir a obrigatoriedade de realizar medidas de controlo regular para manter a certificação durante o período de controlo.

7.10 Alterações que afetam a certificação

Além dos pontos 7.10.1 e 7.10.2 da norma EN ISO/IEC 17065/2012, as alterações passíveis de afetar a certificação a ter em conta pelo organismo de certificação devem incluir: alterações da legislação relativa à proteção de dados, a adoção de atos delegados da Comissão Europeia em conformidade com o artigo 43.º, n.º 8, e o artigo 43.º, n.º 9, decisões do Comité Europeu para a Proteção de Dados e decisões dos tribunais relativas à proteção de dados. Os procedimentos de alteração a acordar poderão incluir aspetos como: os períodos de transição, o processo de aprovação junto da autoridade de controlo competente, a reavaliação do objeto da certificação em questão e medidas apropriadas para revogar a certificação se a operação de tratamento certificada deixou de estar em conformidade com os critérios atualizados.

7.11 Cessação, redução, suspensão ou revogação da certificação

Além do capítulo 7.11.1 da norma ISO/IEC 17065/2012, o organismo de certificação deve ser obrigado a informar, de imediato e por escrito, a autoridade de controlo competente e o organismo nacional de acreditação, se pertinente, sobre as medidas tomadas e sobre a continuação, as restrições, a suspensão e a revogação da certificação.

De acordo com o artigo 58.º, n.º 2, alínea h), o organismo de certificação deve ser obrigado a aceitar as decisões e ordens emitidas pela autoridade de controlo competente para revogar ou não emitir a certificação a um cliente (requerente) em caso de incumprimento dos requisitos de certificação.

7.12 Registos

O organismo de certificação deve ser obrigado a manter toda a documentação completa, compreensível, atualizada e disponível para auditoria.

7.13 Reclamações e recursos, artigo 43.º, n.º 2, alínea d)

Além do ponto 7.13.1 da norma ISO/IEC 17065/2012, o organismo de certificação deve ser obrigado a definir:

(a) Quem pode apresentar reclamações ou objeções;

(b) Quem as processa por parte do organismo de certificação;

(c) Que verificações são levadas a cabo neste contexto; e

(d) As possibilidades existentes de consultar as partes interessadas.

Além do ponto 7.13.2 da norma ISO/IEC 17065/2012, o organismo de certificação deve ser obrigado a definir:

(a) Como e a quem dar a referida confirmação;

(b) Os prazos para o efeito; e

(c) Os processos a iniciar ulteriormente.

Além do ponto 7.13.1 da norma ISO/IEC 17065/2012, o organismo de certificação tem de definir a forma de assegurar a separação entre as atividades de certificação e o processamento dos recursos e reclamações.

8 REQUISITOS DO SISTEMA DE GESTÃO

Um requisito geral do sistema de gestão de acordo com o capítulo 8 da norma ISO/IEC 17065/2012 é a documentação, avaliação, controlo e supervisão independente da aplicação de todos os requisitos dos capítulos anteriores, no âmbito da aplicação do procedimento de certificação pelo organismo de certificação acreditado.

O princípio básico da gestão é a criação de um sistema que defina com eficácia e eficiência os seus objetivos, nomeadamente a implementação dos serviços de certificação através de especificações adequadas. Tal exige a transparência e a verificabilidade da implementação dos requisitos de acreditação por parte do organismo de certificação e a observância constante dos mesmos.

Para o efeito, o sistema de gestão tem de especificar uma metodologia para concretizar e controlar esses requisitos em conformidade com os regulamentos em matéria de proteção de dados e para os verificar continuamente com o próprio organismo acreditado.

Estes princípios de gestão e a sua implementação documentada têm de ser transparentes e divulgados pelo organismo de certificação acreditado no processo de acreditação por força do artigo 58.º e, subsequentemente, a pedido da autoridade de controlo da proteção de dados em qualquer altura durante uma investigação, sob a forma de revisões da proteção de dados nos termos do artigo 58.º, n.º 1, alínea b), ou de uma revisão das certificações emitidas em conformidade com o artigo 42.º, n.º 7, nos termos do artigo 58.º, n.º 1, alínea c).

Em particular, o organismo de certificação acreditado tem de divulgar publicamente, de forma permanente e contínua, que certificações se realizaram e com base em quê (procedimentos ou sistemas de certificação), o período de validade das certificações e ao abrigo de que quadro e condições (considerando 100).

8.1 Requisitos gerais do sistema de gestão

A autoridade de controlo competente pode especificar e adicionar outros requisitos adicionais desde que estejam em conformidade com o direito nacional.

8.2 Documentação do sistema de gestão

A autoridade de controlo competente pode especificar e adicionar outros requisitos adicionais desde que estejam em conformidade com o direito nacional.

8.3 Controlo de documentos

A autoridade de controlo competente pode especificar e adicionar outros requisitos adicionais desde que estejam em conformidade com o direito nacional.

8.4 Supervisão dos registos

A autoridade de controlo competente pode especificar e adicionar outros requisitos adicionais desde que estejam em conformidade com o direito nacional.

8.5 Revisão da gestão

A autoridade de controlo competente pode especificar e adicionar outros requisitos adicionais desde que estejam em conformidade com o direito nacional.

8.6 Auditorias internas

A autoridade de controlo competente pode especificar e adicionar outros requisitos adicionais desde que estejam em conformidade com o direito nacional.

8.7 Ações corretivas

A autoridade de controlo competente pode especificar e adicionar outros requisitos adicionais desde que estejam em conformidade com o direito nacional.

8.8 Ações preventivas

A autoridade de controlo competente pode especificar e adicionar outros requisitos adicionais desde que estejam em conformidade com o direito nacional.

9 OUTROS REQUISITOS ADICIONAIS21

9.1 Atualização dos métodos de avaliação

O organismo de certificação deve estabelecer procedimentos para orientar a atualização dos métodos de avaliação a aplicar no contexto da avaliação nos termos do ponto 7.4. A atualização deve realizar-se no decurso de alterações no quadro normativo, no(s) risco(s) relevante(s), no estado da técnica e nos custos de implementação de medidas técnicas e organizacionais.

9.2 Manutenção dos conhecimentos especializados

Os organismos de certificação devem estabelecer procedimentos para assegurar a formação dos seus funcionários com vista a atualizar as respetivas competências, tomando em consideração os desenvolvimentos enumerados no ponto 9.1.

9.3 Responsabilidades e competências

9.3.1 Comunicação entre o organismo de certificação e os respetivos clientes

Deve prever-se um dispositivo para a aplicação dos procedimentos e estruturas de comunicação apropriados entre o organismo de certificação e o cliente respetivo, incluindo, nomeadamente:

1. Manutenção da documentação de tarefas e responsabilidades pelo organismo de certificação acreditado, para efeitos de:
    a. pedidos de informação ou
    b. contactos em caso de reclamação sobre uma certificação
2. Manutenção de um processo de requerimento para efeitos de:
    a. informação sobre o estado de um requerimento
    b. avaliações pela autoridade de controlo competente sobre:
        i. opiniões e informação de retorno
        ii. decisões da autoridade de controlo competente

9.3.2 Documentação das atividades de avaliação

A autoridade de controlo poderá formular requisitos adicionais.

9.3.3 Gestão do tratamento das reclamações

Cumpre estabelecer um procedimento de tratamento das reclamações como parte integrante do sistema de gestão, o qual deve, em particular, aplicar os requisitos dos pontos 4.1.2.2, alínea c), 4.1.2.2, alínea j), 4.6, alínea d) e 7.13 da norma ISO/IEC 17065/2012.

---

[21] A autoridade de controlo competente pode especificar e adicionar outros requisitos adicionais desde que estejam em conformidade com o direito nacional.

As reclamações e objeções relevantes devem ser partilhadas com a autoridade de controlo competente.

9.3.4 Gestão da revogação

Os procedimentos em caso de suspensão ou revogação da acreditação devem ser integrados no sistema de gestão do organismo de certificação, incluindo as notificações aos clientes.