

Opinion of the Board (Art. 64)



Translations proofread by EDPB Members.

This language version has not yet been proofread.

Parecer 12/2021 sobre o projeto de decisão da autoridade de controlo competente de Portugal relativa à aprovação dos requisitos de acreditação de um organismo de certificação nos termos do artigo 43.º, n.º 3 (RGPD)

Adotado em 23 de março de 2021

Índice

1	Exposição sumária dos factos	4
2	Avaliação	4
2.1	Argumentação geral do CEPD em relação ao projeto de decisão apresentado.....	4
2.2	Principais prioridades (artigo 43.º, n.º 2, do RGPD e anexo 1 das Linhas de orientação do CEPD) estabelecidas pelos requisitos de acreditação, para uma avaliação coerente dos seguintes elementos:.....	5
2.2.1	PREFIXO	6
2.2.2	OBSERVAÇÕES GERAIS	6
2.2.3	REQUISITOS GERAIS DE ACREDITAÇÃO	7
2.2.4	REQUISITOS EM MATÉRIA DE RECURSOS	8
2.2.5	REQUISITOS PROCESSUAIS	9
2.2.6	REQUISITOS DO SISTEMA DE GESTÃO.....	12
2.2.7	OUTROS REQUISITOS ADICIONAIS	12
3	Conclusões/Recomendações	13
4	Observações finais.....	14

O Comité Europeu para a Proteção de Dados,

Tendo em conta o artigo 63.º, o artigo 64.º, n.º 1, alínea c), e n.ºs 3 a 8, e o artigo 43.º, n.º 3, 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 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 2018¹,

Tendo em conta os artigos 10.º e 22.º do seu regulamento interno, de 25 de maio de 2018,

Considerando o seguinte:

(1) A principal função do Comité consiste em assegurar a coerência na aplicação do Regulamento (UE) 2016/679 (a seguir designado por «RGPD»), em todo o Espaço Económico Europeu. Em conformidade com o artigo 64.º, n.º 1, do RGPD, o Comité emite parecer sempre que uma autoridade de controlo (AC) tenha a intenção de aprovar os requisitos de acreditação de organismos de certificação nos termos do artigo 43.º. O presente parecer visa, por conseguinte, criar uma abordagem harmonizada no que diz respeito aos requisitos que uma autoridade de controlo da proteção de dados ou o organismo nacional de acreditação aplicarão para a acreditação de um organismo de certificação. Embora não imponha um conjunto único de requisitos de acreditação, o RGPD promove a coerência. O Comité procura atingir este objetivo nos seus pareceres, em primeiro lugar, incentivando as AC a elaborarem os seus requisitos de acreditação de acordo com a estrutura definida no anexo das Linhas de orientação do CEPD relativas à acreditação de organismos de certificação e, em segundo lugar, analisando-os com base num modelo fornecido pelo CEPD que permite a avaliação comparativa desses requisitos (que devem nortear-se pela norma ISO 17065 e pelas Linhas de orientação do CEPD relativas à acreditação de organismos de certificação).

(2) Em conformidade com o disposto no artigo 43.º do RGPD, as autoridades de controlo competentes devem adotar requisitos de acreditação. No entanto, deverão aplicar o procedimento de controlo da coerência de modo a permitir criar confiança no procedimento de certificação, estabelecendo, em particular, um nível elevado de exigência.

(3) Embora os requisitos de acreditação estejam sujeitos ao procedimento de controlo da coerência, tal não significa que os requisitos devam ser idênticos. As autoridades de controlo competentes dispõem de uma margem de discricionariedade para terem em conta o contexto nacional ou regional e a legislação local. O parecer do CEPD não tem por objetivo definir um conjunto único de requisitos a nível da UE, mas sim evitar incoerências significativas suscetíveis de afetar, por exemplo, a confiança na independência ou nos conhecimentos especializados dos organismos de certificação acreditados.

(4) As «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)» (a seguir designadas por «Linhas de orientação») e as «Diretrizes 1/2018 relativas à certificação e à definição

¹ As referências à «União» no presente parecer devem ser entendidas como referências ao «EEE».

dos critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento» servirão de fio condutor no contexto do procedimento de controlo da coerência.

(5) 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 pormenores 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 requisitos 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 CEPD 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 coerência².

(6) O parecer do CEPD é adotado nos termos do artigo 64.º, n.º 1, alínea c), e n.ºs 3 e 8, do RGPD, em conjugação com o artigo 10.º, n.º 2, do Regulamento Interno do CEPD, no prazo de oito semanas a contar do primeiro dia útil após a decisão de que o processo está completo, tomada pela presidente e pela autoridade de controlo competente. Por decisão da presidente, este prazo pode ser prorrogado por mais seis semanas, em virtude da complexidade do assunto em apreço,

ADOTOU O PRESENTE PARECER:

1 EXPOSIÇÃO SUMÁRIA DOS FACTOS

1. A autoridade de controlo portuguesa (a seguir designada por «AC de Portugal») apresentou ao CEPD o seu projeto de requisitos de acreditação nos termos do artigo 43.º, n.º 1, alínea b). O processo foi considerado completo em 26 de janeiro de 2021. O organismo nacional de acreditação (ONA) de Portugal procederá à acreditação dos organismos de certificação para que estes possam certificar utilizando os critérios de certificação do RGPD. Tal significa que o ONA utilizará a norma ISO 17065 e os requisitos adicionais estabelecidos pela AC de Portugal, uma vez aprovados pela mesma, na sequência de um parecer do Comité sobre o projeto de requisitos, para acreditar os organismos de certificação.

2 AVALIAÇÃO

2.1 Argumentação geral do CEPD em relação ao projeto de decisão apresentado

2. O objetivo do presente parecer é avaliar os requisitos de acreditação desenvolvidos por uma AC, seja em relação à norma ISO 17065, seja como um conjunto completo de requisitos, com vista a permitir

² 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, n.º 39. Disponíveis em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-42018-accreditation-certification-bodies-under_pt.

que um organismo nacional de acreditação ou uma AC, nos termos do artigo 43.º, n.º 1, do RGPD, proceda à acreditação de um organismo de certificação responsável pela emissão e renovação da certificação, em conformidade com o artigo 42.º do RGPD. Tal não prejudica as atribuições e poderes da AC competente. Neste caso concreto, o Comité observa que a AC de Portugal decidiu recorrer ao seu organismo nacional de acreditação (ONA) para a emissão da acreditação, tendo estabelecido requisitos adicionais em conformidade com as Linhas de orientação, que devem ser utilizados pelo seu ONA aquando da emissão da acreditação.

3. Esta avaliação dos requisitos adicionais de acreditação da AC de Portugal visa analisar as variações (aditamentos ou supressões) em relação às Linhas de orientação e, nomeadamente, ao seu anexo 1. Adicionalmente, o parecer do CEPD centra-se igualmente em todos os aspetos suscetíveis de afetar uma abordagem coerente à acreditação de organismos de certificação.
4. Importa observar que o objetivo das Linhas de orientação relativas à acreditação de organismos de certificação consiste em auxiliar as AC na definição dos seus requisitos de acreditação. O anexo das Linhas de orientação não constitui, enquanto tal, um requisito de acreditação. Por conseguinte, os requisitos de acreditação de organismos de certificação devem ser definidos pela AC de modo a permitir a sua aplicação prática e coerente, conforme exigido pelo contexto da AC.
5. O Comité reconhece que, atendendo aos conhecimentos especializados dos ONA, deve ser-lhes concedida margem de manobra para definir certas disposições específicas no âmbito dos requisitos de acreditação aplicáveis. No entanto, o Comité considera necessário salientar que, sempre que sejam estabelecidos requisitos adicionais, estes devem ser definidos de forma a permitir a sua aplicação prática e coerente e revisão, conforme necessário.
6. O Comité observa que as normas ISO, em particular a norma ISO 17065, estão sujeitas a direitos de propriedade intelectual, pelo que não fará referência ao texto do documento conexo no presente parecer. Consequentemente, o Comité decidiu, quando pertinente, remeter para secções específicas da norma ISO, sem, contudo, reproduzir o texto.
7. Por último, o Comité realizou a sua avaliação em conformidade com a estrutura prevista no anexo 1 das Linhas de orientação (a seguir designado por «anexo»). Sempre que o presente parecer não se pronuncie sobre uma secção específica do projeto de requisitos de acreditação da AC de Portugal, tal deve ser entendido no sentido de que o Comité não tem quaisquer observações a fazer e não solicita à AC de Portugal que tome outras medidas.
8. O presente parecer não aborda aspetos referidos pela AC de Portugal que não se inscrevam no âmbito de aplicação do artigo 43.º, n.º 2, do RGPD, como as referências à legislação nacional. No entanto, o Comité observa que a legislação nacional deve, quando necessário, estar em conformidade com o RGPD.

2.2 Principais prioridades (artigo 43.º, n.º 2, do RGPD e anexo 1 das Linhas de orientação do CEPD) estabelecidas pelos requisitos de acreditação, para uma avaliação coerente dos seguintes elementos:

- a. Abordagem de todos os domínios-chave realçados no anexo das Linhas de orientação e análise de eventuais desvios em relação ao anexo;
- b. Independência do organismo de certificação;
- c. Conflitos de interesses do organismo de certificação;

- d. Conhecimentos especializados do organismo de certificação;
- e. Garantias adequadas com vista a assegurar que os critérios de certificação do RGPD são adequadamente aplicados pelo organismo de certificação;
- f. Procedimentos para a emissão, revisão periódica e revogação da certificação ao abrigo do RGPD; e
- g. Tratamento transparente das reclamações relativas a violações da certificação.

9. Tendo em conta que:

- a. O artigo 43.º, n.º 2, do RGPD fornece uma lista de condições de acreditação que um organismo de certificação tem de satisfazer para ser acreditado;
- b. O artigo 43.º, n.º 3, do RGPD estabelece que os requisitos de acreditação dos organismos de certificação devem ser aprovados pela autoridade de controlo competente;
- c. O artigo 57.º, n.º 1, alíneas p) e q), do RGPD prevê que uma autoridade de controlo competente deve redigir e publicar os requisitos de acreditação dos organismos de certificação, podendo decidir proceder ela própria à respetiva acreditação;
- d. O artigo 64.º, n.º 1, alínea c), do RGPD prevê que o Comité deve emitir um parecer sempre que uma autoridade de controlo tenha a intenção de aprovar os requisitos de acreditação aplicáveis a um organismo de certificação nos termos do artigo 43.º, n.º 3;
- e. 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;
- f. O anexo 1 das Linhas de orientação relativas à acreditação de organismos de certificação sugere 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,

o Comité considera que:

2.2.1 PREFIXO

10. O Comité reconhece que os termos de cooperação que regulam a relação entre um organismo nacional de acreditação e a sua autoridade de controlo da proteção de dados não constituem, por si só, um requisito para a acreditação dos organismos de certificação. No entanto, por razões de exaustividade e transparência, o Comité considera que tais termos de cooperação, quando existam, devem ser tornados públicos num formato que a AC considere adequado.

2.2.2 OBSERVAÇÕES GERAIS

11. O Comité observa que a secção relativa ao «âmbito» no projeto de requisitos de acreditação da AC de Portugal não inclui os elementos pertinentes do anexo. Em especial, deve ficar claro que a certificação nos termos do RGPD só é aplicável às operações de tratamento e aos responsáveis pelo tratamento e subcontratantes. Por conseguinte, o CEPD convida a AC de Portugal a incluir essa clarificação.

12. Além disso, o Comité observa que a utilização dos termos «cliente» e «requerente» não é clara no texto, sobretudo tendo em conta que a definição constante do anexo e da norma ISO 17065 difere. Acresce que alguns termos, como «objeto da certificação, alvo de avaliação (AA), objeto da avaliação, objetivo da avaliação», são utilizados indistintamente no projeto de requisitos. Por conseguinte, o Comité incentiva a AC de Portugal a clarificar estes termos e a assegurar a utilização de uma redação clara e coerente em todo o documento.

2.2.3 REQUISITOS GERAIS DE ACREDITAÇÃO

13. No que diz respeito à secção 4.1.1 do projeto de requisitos de acreditação da AC de Portugal (Responsabilidade legal), o Comité considera que a obrigação de os organismos de certificação disporem de procedimentos atualizados que comprovem o cumprimento das responsabilidades legais estipuladas nos termos de acreditação deve ser explicitamente incluída nos requisitos de acreditação. Além disso, o organismo de certificação deve ser capaz de apresentar provas da existência de procedimentos e medidas em conformidade com o RGPD, especificamente para o controlo e gestão dos dados pessoais da organização dos clientes no âmbito do processo de certificação. Por conseguinte, o Comité recomenda que a AC de Portugal altere o projeto de requisitos em conformidade.
14. No que diz respeito ao acordo de certificação (secção 4.1.2), o Comité observa que o primeiro ponto não inclui a obrigação de o cliente cumprir igualmente os requisitos gerais de certificação na aceção do ponto 4.1.2.2, alínea a), da norma ISO 17065, conforme indicado no anexo. Por conseguinte, o Comité convida a AC de Portugal a incluir essa clarificação.
15. No que diz respeito à obrigação de manifestar total transparência perante a AC de Portugal a respeito do procedimento de certificação (ponto 2), deve ficar claro que as informações a que a AC de Portugal tem acesso incluem assuntos contratualmente confidenciais relacionados com o cumprimento da proteção de dados. O CEPD recomenda que o projeto de requisitos seja alterado em conformidade.
16. No que diz respeito ao ponto 6, o Comité observa que a referência aos prazos e procedimentos se limita aos «resultantes do procedimento de certificação», ao passo que a secção 4.1.2, quinto travessão, do anexo se refere aos prazos de forma mais ampla, referindo-se ao programa de certificação *ou a outros regulamentos*. Por conseguinte, o CEPD incentiva a AC de Portugal a alterar a redação, a fim de fazer referência aos prazos de forma geral, em consonância com o anexo.
17. No que diz respeito ao ponto 7, o Comité considera que a obrigação de incluir no acordo de certificação as regras que estabelecem intervalos apropriados para a reavaliação ou revisão deve ser explicitamente mencionada. Por conseguinte, o Comité recomenda que o projeto de requisitos seja alterado em conformidade.
18. No que diz respeito ao ponto 10, o Comité observa que o projeto de requisitos de acreditação da AC de Portugal inclui a obrigação de «Explicar as consequências da revogação ou suspensão da acreditação do organismo de certificação, incluindo as repercussões que possa ter para o cliente». A este respeito, a secção 4.1.2, ponto 9, do anexo estabelece que devem ser tidas em conta as consequências para o cliente nesses casos. O Comité entende que a intenção da AC de Portugal é assegurar que o cliente está ciente das consequências nessas situações e das potenciais opções ou medidas que podem ser tomadas. No entanto, o Comité considera que, a fim de assegurar que os acordos de certificação refletem com exatidão não só as consequências e as repercussões para os clientes, mas também as eventuais medidas futuras, os requisitos de acreditação da AC de Portugal

devem deixar claro que uma simples explicação sem abordar as potenciais medidas seguintes não será suficiente. Assim, o CEPD incentiva a AC de Portugal a deixar claro que o cliente deve estar ciente das consequências, das repercussões que estas têm para si e das eventuais medidas seguintes que poderão vir a ser tomadas.

19. Além disso, o Comité considera que o ponto 11 da secção 4.1.2 do projeto de requisitos de acreditação da AC de Portugal, relativo à obrigação do requerente de informar o organismo de certificação das violações do RGPD e de outra legislação em matéria de proteção de dados, deve ser clarificado. O Comité considera que esta obrigação não deve conduzir à autoincriminação e, por conseguinte, a obrigação deve referir-se a violações estipuladas pela AC de Portugal e/ou pelas autoridades judiciais. Por conseguinte, o Comité recomenda que a AC de Portugal inclua essa clarificação. Além disso, a fim de evitar confusões, o Comité incentiva a AC de Portugal a clarificar que as «violações» se referem a violações do RGPD ou de outra certificação em matéria de proteção de dados suscetíveis de afetar a certificação.
20. No que diz respeito à secção 4.2 do projeto de requisitos de acreditação da AC de Portugal (gestão da imparcialidade), o Comité observa que o primeiro parágrafo estabelece que «O organismo de certificação deve demonstrar *a sua independência em relação ao objeto da certificação* de forma satisfatória para a CNPD, em conformidade com o exigido no artigo 43.º, n.º 2, alínea a), do RGPD». A mesma redação consta das secções 6.1 e 6.2 do projeto de requisitos de acreditação da AC de Portugal. O CEPD entende que a intenção é fazer referência à independência «em relação à organização em avaliação» e incentiva a AC de Portugal a alterar o projeto em conformidade.
21. Além disso, o Comité regista a obrigação de estabelecer regras para prevenir conflitos de interesses. O Comité reconhece a importância de dispor de requisitos que garantam, em primeiro lugar, que não existem conflitos de interesses e, em segundo lugar, caso sejam identificados conflitos de interesses, que o organismo de certificação os gere. Por conseguinte, o Comité incentiva a AC de Portugal a esclarecer que, para além de dispor de regras de prevenção de conflitos, devem existir regras claras para gerir os conflitos de interesses identificados.
22. No que diz respeito às informações disponíveis ao público (secção 4.6 do projeto de requisitos de acreditação da AC de Portugal), o Comité observa que o ponto 1 se refere à publicação de «todas as versões (em vigor ou não) dos critérios de certificação». O Comité incentiva a AC de Portugal a utilizar uma redação mais precisa, substituindo «em vigor ou não» por «a versão atual e as anteriores».
23. Além disso, a secção 4.6 não inclui a obrigação de publicar todos os procedimentos de certificação, indicando, em geral, o respetivo período de validade, tal como indicado na secção 4.6, primeiro ponto, do anexo. Por conseguinte, o Comité recomenda que o projeto de requisitos de acreditação seja alterado em conformidade.

2.2.4 REQUISITOS EM MATÉRIA DE RECURSOS

24. No que diz respeito aos requisitos em matéria de recursos, o CEPD considera que o projeto de requisitos de acreditação deve ser mais bem alinhado com o anexo. Em especial, devem ser incluídos os elementos enumerados no primeiro parágrafo da secção 6.1 do anexo. A este respeito, apenas o ponto 3 e, em parte, o ponto 2 parecem ser abrangidos pelo projeto de requisitos. Além disso, as diferenças nos requisitos aplicáveis ao pessoal técnico e jurídico e aos avaliadores e decisores não são claras. Com efeito, o Comité observa que a secção 6.1 do projeto de requisitos não parece conter quaisquer requisitos aplicáveis ao pessoal técnico, ao passo que a secção 6.2 contém requisitos

aplicáveis ao pessoal jurídico e técnico que efetua as avaliações. O anexo contém vários requisitos aplicáveis ao pessoal técnico e jurídico que efetua as avaliações e que é responsável pela tomada de decisões. Esta diferença é pertinente, uma vez que os conhecimentos especializados e a experiência necessários variam entre o pessoal jurídico e técnico e também entre os responsáveis pelas avaliações e pela tomada de decisões. Tendo em conta que os requisitos do anexo devem ser incluídos no projeto de requisitos, o Comité aproveita a oportunidade para formular as seguintes observações, com o intuito de assegurar que a inclusão dos requisitos é feita de forma coerente: 1) no que diz respeito aos requisitos de formação para o pessoal com conhecimentos técnicos especializados, deve ser incluída a referência a um título protegido reconhecido na profissão regulamentada relevante; 2) o pessoal jurídico deve ter curso de Direito numa universidade reconhecida pela UE ou a nível nacional durante pelo menos oito semestres. Por conseguinte, o CEPD recomenda à AC de Portugal que reformule os requisitos, a fim de clarificar os elementos acima referidos, em conformidade com o anexo.

25. Além disso, o Comité considera que os requisitos em matéria de conhecimentos especializados para avaliadores e decisores devem ser adaptados tendo em conta as diferentes tarefas que desempenham. A este respeito, o Comité considera que os avaliadores devem ter conhecimentos especializados e experiência profissional mais específicos em procedimentos técnicos (por exemplo, auditorias e certificações), ao passo que os decisores devem ter conhecimentos especializados e experiência profissional mais gerais e abrangentes em matéria de proteção de dados. Tendo em conta o que precede, o Comité incentiva a AC de Portugal a reformular os requisitos, tendo em conta os diferentes requisitos em matéria de conhecimentos e/ou experiência substantivos para avaliadores e decisores. No que diz respeito à referência ao conhecimento dos decisores da norma ISO 17065 e dos requisitos de acreditação adicionais, o Comité observa que o mesmo requisito pode ser aplicável ao pessoal responsável pela avaliação e incentiva a AC de Portugal a alterar o projeto em conformidade.
26. No tocante à secção 6.2 do projeto de requisitos de acreditação, o Comité observa que a AC de Portugal incluiu requisitos adicionais. A este respeito, é importante assegurar que os requisitos das secções 6.1 e 6.2 não sejam contraditórios. Por conseguinte, o CEPD incentiva a AC de Portugal a ter em conta os requisitos adicionais a incluir na secção 6.1 e a adaptar a secção 6.2 em conformidade.

2.2.5 REQUISITOS PROCESSUAIS

27. No que diz respeito aos requisitos processuais, a secção 7.1 do projeto de requisitos de acreditação da AC de Portugal estabelece que «Se o organismo de certificação pretender agir noutros Estados-Membros, deve obter a aprovação necessária das autoridades competentes pertinentes, *ou solicitar um Selo Europeu de Proteção de Dados em conformidade com o artigo 42.º, n.º 5, do RGPD.*» Esta frase parece dar ao organismo de certificação a possibilidade de optar entre obter a aprovação das AC competentes ou solicitar um Selo Europeu de Proteção de Dados. O Comité sublinha que, mesmo quando um Selo Europeu de Proteção de Dados tenha sido aprovado, o organismo de certificação continua a ter de notificar as autoridades de controlo interessadas (ACI) relevantes antes de o utilizar num novo Estado-Membro a partir de um gabinete satélite. Este aspeto é especialmente pertinente, tendo em conta que a acreditação de um organismo de certificação que concede selos europeus de proteção de dados pode ter de ser efetuada em cada um dos Estados-Membros em que o organismo de certificação está estabelecido³. No entanto, importa salientar que as ACI devem ser

³ A este respeito, ver Diretrizes 1/2018, n.º 44.

notificadas mesmo nos casos em que a utilização de um Selo Europeu de Proteção de Dados num novo Estado-Membro não exija uma nova acreditação. Por conseguinte, o Comité recomenda que a AC de Portugal inclua a referência acima mencionada. Por exemplo, o projeto de requisitos pode indicar o seguinte (ver alterações propostas em itálico): «Se o organismo de certificação pretender agir noutros Estados-Membros, deve *notificar e, se necessário*, obter a aprovação necessária das autoridades competentes pertinentes, *nomeadamente para a utilização de um Selo Europeu de Proteção de Dados em conformidade com o artigo 42.º, n.º 5, do RGPD*».

28. No que diz respeito ao ponto 4 da secção 7.1 do projeto de requisitos de acreditação da AC de Portugal, o Comité toma nota do requisito adicional segundo o qual um organismo de certificação deve investigar o cliente «por violações do regime jurídico de proteção de dados quando for notificado pelo cliente de que está a ser objeto de uma investigação realizada pela CNPD ou se a autoridade de controlo informar a este respeito o organismo de certificação». Deve ficar claro que essa investigação deve estar ligada ao âmbito da certificação e ao alvo de avaliação. Por conseguinte, o Comité recomenda que a AC de Portugal altere o seu requisito em conformidade, especificando que a investigação deve estar ligada ao âmbito da certificação e ao alvo de avaliação.
29. O Comité observa que o ponto 2 da secção 7.2 do projeto de requisitos de acreditação da AC de Portugal («pedido») contém uma referência ao(s) contrato(s) do responsável pelo tratamento/subcontratante e às suas disposições específicas. Embora reconheça que a AC de Portugal utilizou a redação do anexo, o Comité incentiva a AC de Portugal a incluir uma referência aos responsáveis conjuntos pelo tratamento e às suas disposições específicas.
30. Além disso, o Comité observa que o ponto 3 da secção 7.2 do projeto de requisitos de acreditação da AC de Portugal inclui a obrigação de identificar «Qualquer investigação ou inquérito realizado pela CNPD ao requerente, atual ou ocorrido desde 25 de maio de 2018». No entender do Comité, a obrigação deve ser adaptada às investigações ou ações regulamentares relacionadas com o âmbito da certificação e o alvo de avaliação. Por conseguinte, o Comité incentiva a AC de Portugal a esclarecer que a investigação ou a ação regulamentar deve estar relacionada com o âmbito da certificação e o alvo de avaliação.
31. No que diz respeito à secção 7.4 do projeto de requisitos de acreditação da AC de Portugal («avaliação»), o Comité observa que os requisitos estabelecem que «O organismo de certificação deve ter em conta as orientações do CEPD no que diz respeito ao procedimento de avaliação, assegurando a homogeneidade e a coerência dos métodos de avaliação para objetos de avaliação semelhantes». Em primeiro lugar, o Comité considera que a referência às orientações do CEPD pode limitar a obrigação do organismo de certificação, no sentido de que apenas exige que sejam tidas em conta as orientações do CEPD relativas ao procedimento de avaliação. Por conseguinte, a referência deve ser suprimida ou alterada de forma a evitar essa limitação. Em segundo lugar, o Comité observa que o anexo se refere a métodos de avaliação «normalizados e geralmente aplicáveis. Tal significa que são utilizados métodos de avaliação comparáveis para alvos de avaliação comparáveis». O Comité considera que a redação do projeto de requisitos de acreditação da AC de Portugal não reflete plenamente a intenção do anexo de assegurar a normalização dos métodos de avaliação, pelo que deve ser alterada em conformidade. Por conseguinte, o CEPD incentiva a AC de Portugal a introduzir as alterações necessárias acima referidas.
32. Além disso, o CEPD recomenda à AC de Portugal que inclua a obrigação de o organismo de certificação justificar qualquer desvio em relação ao procedimento referido no ponto anterior, em conformidade com o anexo.

33. No que diz respeito ao ponto 3 do primeiro parágrafo da secção 7.4, o Comité observa que o projeto de requisitos de acreditação da AC de Portugal não menciona as garantias como um dos elementos a incluir no método de avaliação das medidas jurídicas corretivas, tal como indicado no anexo. Além disso, o Comité observa que o ponto 3 do primeiro parágrafo da secção 7.4 do anexo se refere à demonstração do cumprimento dos requisitos legais estipulados nos critérios. Esta referência não consta do projeto de requisitos de acreditação da AC de Portugal. Por conseguinte, o Comité incentiva a AC de Portugal a incluir a referência acima mencionada, em conformidade com o anexo.
34. No que diz respeito à utilização de certificações obtidas anteriormente, o Comité observa que o projeto de requisitos de acreditação da AC de Portugal menciona uma certificação que o cliente pretende «transferir». A mesma redação encontra-se na secção 7.9. O CEPD entende que a frase se refere a certificações anteriores que o cliente pretende utilizar. Assim, a fim de evitar qualquer confusão, o CEPD incentiva a AC de Portugal a clarificar o significado de «transferir». Além disso, o Comité considera que, quando a certificação existente é tida em conta no âmbito de uma nova avaliação, deve ficar claro que não será suficiente substituir completamente as avaliações (parciais) e que o âmbito dessa certificação deve ser avaliado em pormenor no que diz respeito à sua conformidade com os critérios de certificação pertinentes. Ademais, o organismo de certificação deve dispor de um relatório de avaliação completo ou de informações que permitam uma avaliação. O Comité recomenda que a AC de Portugal altere o projeto em conformidade.
35. Além disso, o Comité observa que o projeto de requisitos de acreditação da AC de Portugal prevê o recurso a peritos externos contratados pelo organismo de certificação. O Comité considera que o projeto de requisitos de acreditação deve indicar explicitamente que o organismo de certificação continuará a ser responsável pela tomada de decisões, mesmo quando recorrer a peritos externos. Por conseguinte, o Comité recomenda que a AC de Portugal altere o projeto em conformidade.
36. O CEPD entende que o n.º 8 da secção 7.4 se refere a avaliações de acompanhamento de clientes já certificados. A fim de evitar mal-entendidos, o CEPD incentiva a AC de Portugal a clarificá-lo no texto.
37. O Comité observa que o segundo parágrafo da secção 7.6 do projeto de requisitos de acreditação da AC de Portugal («decisão de certificação») inclui a obrigação de apresentar à AC de Portugal o projeto de certificação da conformidade da documentação que a substitui, antes da emissão ou renovação da certificação. Com base nas explicações fornecidas pela AC de Portugal, o Comité entende que a intenção deste requisito é aumentar a transparência e não implica uma supervisão do projeto de aprovação. O Comité incentiva a AC de Portugal a acrescentar uma clarificação nesse sentido.
38. No que diz respeito à secção 7.9 do projeto de requisitos de acreditação («Supervisão») da AC de Portugal, o Comité congratula-se com a obrigação de realizar anualmente as atividades de supervisão. Além disso, o Comité considera que os riscos associados ao tratamento devem ser tidos em conta para determinar se é necessário um controlo mais frequente. Assim, o Comité incentiva a AC de Portugal a incluir uma abordagem baseada no risco, a fim de identificar se, em casos específicos, as atividades de supervisão têm de ser realizadas mais do que uma vez por ano.
39. No que diz respeito à secção 7.10 do projeto de requisitos de acreditação da AC de Portugal («alterações que afetam a certificação»), o Comité considera que as alterações no estado da técnica também são pertinentes e podem afetar a certificação. Por conseguinte, o Comité incentiva a AC de Portugal a incluir esta possibilidade na lista de alterações suscetíveis de afetar a certificação.
40. Além disso, o Comité observa que o ponto 1 da secção 7.10 inclui «qualquer notificação de violação de dados pessoais ou de incumprimento do RGPD ou dos requisitos adicionais». O Comité considera

que, a fim de evitar a autoincriminação, a referência deve ser feita às violações estipuladas pela AC de Portugal ou pela autoridade judiciária competente. Além disso, a referência a «qualquer notificação de violação de dados» parece bastante ampla. O Comité considera que essa referência deve ser adaptada às notificações de violações de dados que possam estar relacionadas com o âmbito da certificação e o alvo de avaliação. Por conseguinte, incentiva a AC de Portugal a aditar a referência acima mencionada.

41. No que diz respeito ao quarto ponto normando («decisões pertinentes do Comité Europeu para a Proteção de Dados»), o Comité reconhece que a AC de Portugal utilizou a redação prevista no anexo 1. No entanto, a fim de assegurar uma compreensão clara do que se entende por «decisões do Comité Europeu para a Proteção de Dados», o Comité incentiva a AC de Portugal a clarificar a referência. Poderia, por exemplo, referir-se a «documentos adotados pelo Comité Europeu para a Proteção de Dados».
42. No que diz respeito à secção 7.11 do projeto de requisitos de acreditação da AC de Portugal («Cessação, redução, suspensão ou revogação da certificação»), o Comité observa que o ONA deve também ser informado da cessação, redução, suspensão ou revogação da certificação. Por conseguinte, o CEPD recomenda a inclusão dessa referência.
43. O Comité observa que a secção 7.11 do projeto de requisitos da AC de Portugal (cessação, redução, suspensão ou revogação da certificação) não contém a obrigação de o organismo de certificação aceitar decisões e ordens da AC de Portugal no sentido de revogar ou não emitir a certificação a um requerente se os requisitos de certificação não estiverem ou deixarem de estar preenchidos. Por conseguinte, o Comité recomenda que a AC de Portugal inclua essa obrigação.
44. No que diz respeito à secção 7.13 do projeto de requisitos de acreditação («Reclamações e recursos») da AC de Portugal, o Comité observa que falta o seguinte requisito do anexo: «(...) 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». O CEPD recomenda que a AC de Portugal altere o projeto em conformidade.

2.2.6 REQUISITOS DO SISTEMA DE GESTÃO

45. O Comité observa que a secção 8 do projeto de requisitos de acreditação da AC de Portugal não inclui a obrigação de divulgar à AC de Portugal os princípios de gestão e a sua implementação documentada durante o processo de acreditação e, subsequentemente, a pedido da AC de Portugal em qualquer altura durante uma investigação, tal como indicado no anexo. O CEPD recomenda que essa obrigação seja incluída nos requisitos de acreditação da AC de Portugal.

2.2.7 OUTROS REQUISITOS ADICIONAIS

46. O ponto 5 da secção 7.1 do projeto de requisitos de acreditação da AC de Portugal inclui alguns dos elementos da secção 9.3.1 do anexo («Comunicação entre o organismo de certificação e os respetivos clientes»). No entanto, o CEPD observa que continuam a faltar alguns elementos do anexo (por exemplo, referências à manutenção da documentação, a fim de permitir contactos em caso de reclamação, e à manutenção de um processo de requerimento para efeitos de ou avaliações pela AC competente). O CEPD recomenda à AC de Portugal que inclua os elementos em falta da secção 9.3.1 do anexo.

47. O ponto 3 da secção 7.4 do projeto de requisitos de acreditação da AC de Portugal inclui a obrigação de o organismo de certificação rever periodicamente os seus métodos de avaliação à luz do desenvolvimento de novas tecnologias e das alterações no quadro normativo. O Comité observa que este requisito reflete parcialmente o requisito previsto na secção 9.1 do anexo, uma vez que parece implicar a existência de regras para rever os métodos de avaliação. No entanto, deve ficar claro que o organismo de certificação deve estabelecer procedimentos para orientar a atualização dos métodos de avaliação. Além disso, a atualização deve ter em conta não só o desenvolvimento de novas tecnologias e as alterações do quadro normativo, mas também o(s) risco(s) relevante(s), o estado da técnica e os custos de implementação das medidas técnicas e organizacionais, em consonância com o anexo. Por conseguinte, o Comité incentiva a AC de Portugal a incluir os elementos supracitados.
48. Por último, a última frase da secção 7.13 do projeto de requisitos de acreditação da AC de Portugal reflete parcialmente a obrigação prevista no segundo parágrafo da secção 9.3.3 do anexo. No entanto, o Comité considera que as reclamações e objeções relevantes não só têm de ser informadas à AC de Portugal, como têm de ser partilhadas com a AC de Portugal. Por conseguinte, o Comité recomenda à AC de Portugal que reformule o requisito indicando que as reclamações e objeções relevantes devem ser partilhadas com a AC de Portugal.

3 CONCLUSÕES/RECOMENDAÇÕES

49. O projeto de requisitos de acreditação da autoridade de controlo de Portugal pode conduzir a uma aplicação incoerente da acreditação dos organismos de certificação, pelo que é necessário introduzir as seguintes alterações:
50. No que respeita aos «requisitos gerais de acreditação», o Comité recomenda que a AC de Portugal:
- 1) Altere a secção 4.1.1 em consonância com o anexo;
 - 2) Clarifique, na secção 4.1.2, segundo ponto, que as informações a que a AC de Portugal tem acesso incluem assuntos contratualmente confidenciais relacionados com o cumprimento da proteção de dados;
 - 3) Adite na secção 4.1.2, ponto 7, a obrigação de incluir no acordo de certificação as regras que definem intervalos apropriados para a reavaliação ou revisão;
 - 4) Clarifique, na secção 4.1.2, ponto 11, que a obrigação de informar sobre quaisquer violações do RGPD se refere a violações estipuladas pela AC de Portugal e/ou pelas autoridades judiciais;
 - 5) Inclua na secção 4.6 a obrigação de publicar todos os procedimentos de certificação, indicando, em geral, o respetivo período de validade.
51. No que respeita aos «requisitos em matéria de recursos», o Comité recomenda que a AC de Portugal:
- 1) Clarifique os requisitos da secção 6.1, em consonância com as observações do ponto 24 acima.
52. No que respeita aos «requisitos processuais», o Comité recomenda que a AC de Portugal:
- 1) Altere a secção 7.1 a fim de incluir as referências à notificação das ACI antes de o organismo de certificação operar num novo Estado-Membro a partir de um gabinete

satélite, nomeadamente no que se refere à utilização de um Selo Europeu de Proteção de Dados;

- 2) Clarifique na secção 7.1 que a investigação que o organismo de certificação pode realizar deve estar ligada ao âmbito da certificação e ao alvo de avaliação;
- 3) Inclua na secção 7.4 a obrigação de o organismo de certificação justificar qualquer desvio em relação aos métodos de avaliação normalizados e geralmente aplicáveis;
- 4) Inclua os elementos mencionados no ponto 34 do presente parecer, relativos à utilização da certificação existente no âmbito de uma nova avaliação;
- 5) Indique explicitamente que o organismo de certificação continuará a ser responsável pela tomada de decisões, mesmo quando recorrer a peritos externos;
- 6) Clarifique que o ONA deve também ser informado sobre a cessação, redução, suspensão ou revogação da certificação;
- 7) Inclua a obrigação de o organismo de certificação aceitar decisões e ordens da AC de Portugal no sentido de revogar ou não emitir a certificação a um requerente se os requisitos de certificação não estiverem ou deixarem de estar preenchidos;
- 8) Altere a secção 7.13 para incluir o elemento em falta do anexo, tal como indicado no ponto 44 acima.

53. No que respeita aos «requisitos do sistema de gestão», o Comité recomenda que a AC de Portugal:

- 1) Inclua a obrigação de divulgar à AC de Portugal os princípios de gestão e a sua implementação documentada durante o processo de acreditação e, subsequentemente, a pedido da AC de Portugal em qualquer altura durante uma investigação, tal como indicado no anexo.

54. No que respeita a «outros requisitos adicionais», o Comité recomenda que a AC de Portugal:

- 1) Inclua os elementos em falta da secção 9.3.1 do anexo;
- 2) Reformule a última frase da secção 7.13, indicando que as reclamações e objeções relevantes devem ser partilhadas com a AC de Portugal.

4 OBSERVAÇÕES FINAIS

55. A autoridade de controlo de Portugal é a destinatária do presente parecer, que será tornado público nos termos do artigo 64.º, n.º 5, alínea b), do RGPD.

56. Nos termos do artigo 64.º, n.ºs 7 e 8, do RGPD, a AC de Portugal comunica à presidente, por via eletrónica, no prazo de duas semanas a contar da receção do parecer, se tenciona manter ou alterar o seu projeto de lista. Dentro do mesmo prazo, apresenta o projeto de lista alterado ou, se não tencionar seguir o parecer do Comité, apresenta os motivos pertinentes pelos quais não tenciona seguir, no todo ou em parte, o referido parecer.

57. A AC de Portugal comunica a decisão final ao Comité com vista à sua inclusão no registo das decisões objeto do procedimento de controlo da coerência, em conformidade com o artigo 70.º, n.º 1, alínea y), do RGPD.

Pelo Comité Europeu para a Proteção de Dados

A presidente

(Andrea Jelinek)