

Parecer do Comité (artigo 64.º)



Parecer 16/2020 sobre o projeto de decisão da autoridade de controlo competente da República Checa relativa à aprovação dos requisitos de acreditação de um organismo de certificação nos termos do artigo 43.º, n.º 3 (RGPD)

Adotado em 25 de maio de 2020

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

Índice

1	EXPOSIÇÃO SUMÁRIA DOS FACTOS	4
2	AVALIAÇÃO	5
2.1	Argumentação geral do CEPD relativamente ao projeto de decisão apresentado	5
2.2	Principais prioridades (art. 43.º, n.º 2, do RGPD e anexo 1 das Orientações do CEPD) estabelecidas pelos requisitos de acreditação para uma avaliação coerente dos seguintes elementos:	6
2.2.1	PREFIXO	6
2.2.2	OBSERVAÇÕES GERAIS	7
2.2.3	REQUISITOS GERAIS PARA ACREDITAÇÃO	7
2.2.4	REQUISITOS EM MATÉRIA DE RECURSOS	8
2.2.5	REQUISITOS DO PROCESSO	9
2.2.6	SISTEMA DE GESTÃO	11
3	CONCLUSÕES/RECOMENDAÇÕES	11
4	OBSERVAÇÕES FINAIS	12

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

Tendo em conta o artigo 10.º e o artigo 22.º do seu Regulamento Interno, de 25 de maio de 2018,

Considerando que:

(1) A principal função do Comité consiste em assegurar a coerência na aplicação do Regulamento (UE) n.º 2016/679 (adiante designado por «RGPD»), em todo o Espaço Económico Europeu. Em conformidade com o artigo 64.º, n.º 1, do RGPD, o Comité emite um 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 Orientações do CEPD relativas à acreditação dos organismos de certificação e, em segundo lugar, analisando-os com base num modelo fornecido pelo CEPD que permite a avaliação comparativa desses requisitos (tendo em conta a norma ISO 17065 e as Orientações do CEPD relativas à acreditação dos organismos de certificação).

(2) Nos termos do artigo 43.º do RGPD, as autoridades de controlo competentes adotam 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, isso não significa que os requisitos devam ser idênticos. As autoridades de controlo competentes dispõem de uma margem de discricionariedade relativamente ao contexto nacional ou regional e devem ter em conta a sua legislação local. O parecer do CEPD não tem por objetivo a definição de um conjunto único de requisitos ao nível da UE, mas sim evitar incoerências significativas que possam 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 «Orientações») e as «Diretrizes 1/2018 relativas à certificação e à definição dos

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

critérios de certificação, em conformidade com os artigos 42.º e 43.º do Regulamento n.º 2016/679» 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 informações sobre os requisitos de acreditação quando cabe à própria 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 ser orientados pela norma ISO/IEC 17065 e 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 a coerência².

(6) O parecer do CEPD é adotado nos termos do artigo 64.º, n.º 1, alínea c), n.º 3 e n.º 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 subsequente à decisão da Presidente e da autoridade de controlo competente de que o processo está completo. Por decisão da Presidente, este prazo pode ser prorrogado por mais seis semanas, tendo em conta a complexidade do tema.

ADOTOU O PRESENTE PARECER:

1 EXPOSIÇÃO SUMÁRIA DOS FACTOS

1. A Autoridade de Controlo da República Checa (adiante designada por «AC da República Checa») apresentou o respetivo projeto de requisitos de acreditação nos termos do artigo 43.º, n.º 1, alínea b), do RGPD. O processo foi considerado completo em 17 de fevereiro de 2020. O organismo nacional de acreditação (ONA) da República Checa procederá à acreditação de organismos de certificação com recurso aos critérios de certificação do RGPD. Isto significa que o ONA aplicará a norma ISO 17065 e os requisitos adicionais estabelecidos pela AC da República Checa, uma vez aprovados por esta na sequência de um parecer do Comité sobre o projeto de requisitos, para a acreditação dos organismos de certificação.
2. Em conformidade com o artigo 10.º, n.º 2, do Regulamento Interno do Comité, dada a complexidade do assunto em apreço, a Presidente decidiu prorrogar o prazo de adoção inicial de oito semanas por mais seis semanas.

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. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/pokyny/guidelines-42018-accreditation-certification-bodies-under_pt

2 AVALIAÇÃO

2.1 Argumentação geral do CEPD relativamente ao projeto de decisão apresentado

3. 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 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. Tudo sem prejuízo das atribuições e dos poderes da AC competente. Neste caso específico, o Comité observa que a AC da República Checa decidiu recorrer ao seu organismo nacional de acreditação (ONA) para a emissão da acreditação, tendo estabelecido, em conformidade com as Orientações, requisitos adicionais que devem ser utilizados pelo respetivo ONA quando da emissão da acreditação.
4. Esta avaliação dos requisitos adicionais de acreditação da AC da República Checa destina-se a analisar as diferenças (aditamentos ou supressões) em relação às Orientações e, em particular, ao seu anexo 1. Adicionalmente, o parecer do CEPD centra-se igualmente em todos os aspetos suscetíveis de impactar uma abordagem coerente à acreditação de organismos de certificação.
5. Importa observar que o objetivo das Orientações relativas à acreditação dos organismos de certificação consiste em auxiliar as AC na definição dos seus requisitos de acreditação. O anexo das Orientações não constitui uma lista de requisitos de acreditação propriamente ditos. Deste modo, os requisitos de acreditação de organismos de certificação deverão ser definidos pela AC de modo a permitir a sua aplicação prática e coerente, conforme exigido pelo contexto da AC.
6. O Comité reconhece que, dados os conhecimentos dos ONA nesta área, 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.
7. 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 respetivo documento no presente parecer. Consequentemente, o Comité decidiu, quando relevante, remeter para secções específicas da norma ISO, sem, contudo, reproduzir o texto.
8. Por último, o Comité procedeu à sua avaliação à luz da estrutura prevista no anexo 1 das Orientações (adiante designado por «anexo»). Quando o presente parecer não se pronuncia relativamente a uma determinada secção do projeto de requisitos de acreditação da AC da República Checa, isso deve ser interpretado no sentido de que o Comité não tem observações a formular, nem solicita à AC da República Checa que tome medidas adicionais.
9. O presente parecer não aborda aspetos mencionados pela AC da República Checa 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 (art. 43.º, n.º 2, do RGPD e anexo 1 das Orientações 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 Orientações e análise de eventuais desvios ao anexo;
- b. independência do organismo de certificação;
- c. conflitos de interesses do organismo de certificação;
- d. competência técnica 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 retirada da certificação ao abrigo do RGPD; e
- g. tratamento transparente de reclamações relativas a violações da certificação.

10. Tendo em conta que:

- a. O artigo 43.º, n.º 2, do RGPD estabelece 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 dispõe que os requisitos de acreditação de organismos de certificação são aprovados pela autoridade de controlo competente;
- c. O artigo 57.º, n.º 1, alíneas p) e q), do RGPD dispõe que uma autoridade de controlo competente deve redigir e publicar os requisitos de acreditação de organismos de certificação, podendo decidir proceder ela própria à respetiva acreditação;
- d. O artigo 64.º, n.º 1, alínea c), do RGPD dispõe que o Comité emite 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, devem também ser aplicados os requisitos adicionais estabelecidos pela autoridade de controlo competente;
- f. O anexo 1 das Orientações relativas à acreditação dos organismos de certificação sugere determinados requisitos que uma autoridade de controlo da proteção de dados deve elaborar e que serão aplicáveis durante a acreditação de um organismo de certificação pelo organismo nacional de acreditação;

o Comité considera que:

2.2.1 PREFIXO

- 11. O Comité reconhece que as condições de cooperação que regulam a relação entre um organismo nacional de acreditação e a respetiva autoridade de controlo da proteção de dados não constituem

um requisito da acreditação dos organismos de certificação *per se*. No entanto, por razões de exaustividade e transparência, o Comité considera que tais condições de cooperação, quando existam, devem ser tornadas públicas num formato considerado adequado pela AC.

2.2.2 OBSERVAÇÕES GERAIS

12. O Comité observa que o projeto de requisitos de acreditação não respeita integralmente a estrutura definida no anexo 1 das Orientações. A título de exemplo, foram omitidas as secções relativas ao «âmbito de aplicação» e aos «termos e definições». A este respeito, por razões de clareza e para permitir uma avaliação mais fácil dos requisitos, o Comité considera que a numeração e a estrutura geral do documento podem ser melhoradas. Por conseguinte, com o objetivo de facilitar a avaliação, o Comité incentiva a AC da República Checa a seguir a estrutura do anexo no projeto de requisitos de acreditação e a acrescentar as secções em falta, revestindo especial relevância a definição dos termos utilizados em todo o documento. Além disso, o Comité observa que o projeto de requisitos de acreditação da AC da República Checa remete várias vezes para a secção respetiva da norma ISO 17065 ou para as secções respetivas do anexo, sem, no entanto, especificar essas referências. Por conseguinte, o Comité encoraja a AC da República Checa a clarificar as referências às secções da norma ISO 17065 e do anexo.
13. O Comité observa que o projeto de requisitos de acreditação da AC da República Checa refere várias vezes o «objeto avaliado» (por exemplo, nas secções 3.2.1.2.1.2.10; 3.2.1.2.6.3.1; 3.2.1.2.8.1.6.3; 3.2.1.2.10.4.1; 3.1.2.10.7.3.1; 3.1.2.10.7.3.2 e 3.2.1.2.10.10.2). O Comité entende que este termo é empregado como sinónimo de «alvo da avaliação». No entanto, a fim de garantir a clareza, o Comité incentiva a AC da República Checa a utilizar o termo «alvo da avaliação» de forma coerente.
14. O Comité observa que há vários requisitos que não são formulados como uma obrigação do organismo de certificação (por exemplo, 3.2.1.2.2 e 3.2.1.2.3). O Comité incentiva a AC da República Checa a reformular os requisitos de modo a tornar claro que são obrigatórios – ou seja, iniciar a formulação do requisito com a expressão «o organismo de certificação deve [...]».

2.2.3 REQUISITOS GERAIS PARA ACREDITAÇÃO

15. No que se refere ao acordo de certificação (secção 3.2.1.2.1.2 do projeto de requisitos de acreditação da AC da República Checa), o Comité observa que a subsecção 3.2.1.2.1.2.2 não faz qualquer referência aos «assuntos contratualmente confidenciais» a que a AC terá igualmente acesso. Por conseguinte, o Comité recomenda que a AC da República Checa altere o projeto, de modo a incluir a obrigação de também facultar à AC o acesso a assuntos contratualmente confidenciais.
16. No que se refere à subsecção 3.2.1.2.1.2.8 do projeto de requisitos de acreditação da AC da República Checa, o Comité observa que não é claro a quem devem ser divulgadas as informações. Por conseguinte, o Comité incentiva a AC da República Checa a esclarecer quem será o destinatário das informações. Além disso, as informações referidas devem ser «necessárias para conceder a certificação», conforme estabelecido no ponto 7 da secção 4.1.2 do anexo. O Comité recomenda que a AC da República Checa substitua a expressão «informações sobre a concessão da certificação» por «informações necessárias para conceder a certificação».
17. No que se refere à subsecção 3.2.1.2.1.2.9 do projeto de requisitos de acreditação da AC da República Checa, não é claro que tipo de informações devem ser comunicadas diretamente ao Comité. O artigo 42.º, n.º 8, do RGPD estabelece a obrigação do Comité de recolher, entre outros elementos, todos os

procedimentos de certificação. Neste contexto, parte-se do princípio de que as AC competentes fornecerão as informações relevantes ao Comité, que as publicará no registo público. Por conseguinte, o Comité recomenda à AC da República Checa que clarifique a subsecção 3.2.1.2.1.2.9 do projeto de requisitos, em conformidade com o artigo 42.º, n.º 8, do RGPD.

18. No que se refere à subsecção 3.2.1.2.1.2.12 do projeto de requisitos de acreditação da AC da República Checa, o Comité regista o facto de esta ter criado uma versão reformulada de parte do requisito previsto no anexo. No entanto, a AC da República Checa omitiu uma referência a [quando aplicável]: «as consequências para o cliente também devem ser abordadas». Por conseguinte, o Comité recomenda à AC da República Checa que acrescente a parte em falta no requisito acima mencionado.
19. Além disso, a subsecção 3.2.1.2.1.2.13 do projeto de requisitos de acreditação da AC da República Checa estabelece a obrigação de «incluir o compromisso do requerente de informar o organismo de certificação acerca de todas as alterações suscetíveis de afetar a conformidade do objeto certificado com os critérios de certificação». O Comité considera esta formulação demasiado genérica e recomenda à AC da República Checa que altere o projeto de requisitos, a fim de incluir a menção a «todas as alterações na sua situação efetiva ou jurídica e nos seus produtos, processos e serviços a que a certificação diga respeito».
20. No que se refere à utilização de selos e marcas de proteção de dados (secção 3.2.1.2.1.3 do projeto de requisitos de acreditação da AC da República Checa), o Comité observa que o projeto de requisitos da AC da República Checa estabelece que o acordo de certificação deve conter «regras de utilização de certificados, selos e marcas caso sejam fornecidos pelo proprietário do sistema de certificação». A mesma formulação encontra-se na subsecção 3.2.1.2.1.2.14. O Comité considera que esta obrigação já está abrangida pelo ponto 4.1.2.2., letra I), da norma ISO 17065 e que, por conseguinte, deve ser incluída em qualquer sistema de certificação (ver também ponto 4.1.3 da norma ISO 17065). Assim, por razões de clareza, o Comité recomenda à AC da República Checa que elimine as secções acima referidas.
21. No que se refere aos requisitos relativos à gestão da imparcialidade, de acordo com as informações fornecidas pela AC da República Checa no modelo, os pontos 4.2.1.b) e 4.2.2 do anexo estão suficientemente contemplados no ponto 4.2 da norma ISO 17065. No entanto, o Comité considera que estes requisitos devem ser explicitamente incluídos no projeto de requisitos de acreditação elaborado pelas AC em conformidade com o anexo. Por conseguinte, o Comité recomenda à AC da República Checa que inclua os requisitos em falta no que respeita à gestão da imparcialidade prevista no anexo.
22. No tocante à obrigação de responsabilidade e financiamento (secção 3.2.1.2.3.1 do projeto de requisitos da AC da República Checa), o Comité incentiva a AC da República Checa a especificar que deve ser garantida regularmente.

2.2.4 REQUISITOS EM MATÉRIA DE RECURSOS

23. No que se refere ao pessoal do organismo de certificação (secção 3.2.1.2.8.1.6 do projeto de requisitos de acreditação da AC da República Checa), o Comité observa que os requisitos aplicáveis ao pessoal responsável pelas avaliações (subsecção 3.2.1.2.8.1.6.3) incluem «experiência de cinco anos, com um número mínimo de dez auditorias, realizadas no âmbito da atividade de certificação no mesmo domínio ou em domínio semelhante [...], ou experiência de cinco anos no âmbito da certificação dos objetos das atribuições do organismo de certificação». Do mesmo modo, os requisitos aplicáveis ao

pessoal responsável pela tomada de decisões (subsecção 3.2.1.2.8.1.6.4) incluem a « *experiência mínima de cinco anos, com um número mínimo de dez auditorias, realizadas no âmbito da atividade de certificação no mesmo domínio ou em domínio semelhante*». A este respeito, o Comité considera que os requisitos de competência aplicáveis aos avaliadores e aos decisores devem ser adaptados tendo em conta as diferentes tarefas que desempenham. A este propósito, o Comité entende que os avaliadores devem ter conhecimentos e experiência profissional mais especializados sobre procedimentos técnicos (por exemplo, auditorias e certificações), ao passo que os decisores devem ter conhecimentos e experiência profissional mais gerais e abrangentes em matéria de proteção de dados. Tendo em conta as considerações precedentes, o Comité incentiva a AC da República Checa a reformular esta subsecção tendo em conta os diferentes requisitos de conhecimentos substantivos e/ou experiência efetiva aplicáveis aos avaliadores e decisores.

24. Além disso, o Comité regista que o ponto 3.2.1.2.9.1 do projeto de requisitos de acreditação da AC da República Checa estabelece que a externalização não é autorizada em relação às atividades de certificação. No entanto, o ponto subsequente permite a utilização de auditores externos e peritos externos na avaliação, exceto se esta consistir em atividades de certificação. O Comité considera que o projeto de requisitos de acreditação deve especificar em que casos «a avaliação consiste em atividades de certificação» ou clarificar que o organismo de certificação continuará a ser responsável pela tomada de decisões, mesmo que recorra a peritos externos. Por conseguinte, o Comité recomenda que a AC da República Checa altere o projeto em conformidade.

2.2.5 REQUISITOS DO PROCESSO

25. O Comité regista que a secção 3.2.1.2.10.1.1 do projeto de requisitos adicionais da AC da República Checa refere «todos os requisitos adicionais relativos a conflitos de interesses (7.1, ponto 1)». No entanto, o projeto de requisitos adicionais da AC da República Checa não contém requisitos adicionais relativos a conflitos de interesses. Por conseguinte, o Comité incentiva a AC da República Checa a alterar o projeto, a fim de evitar confusões.
26. No que diz respeito aos requisitos de candidatura, o Comité observa que a subsecção 3.2.1.2.10.2.3 do projeto de requisitos de acreditação da AC da República Checa parece implicar que as informações sobre os dados transferidos só serão fornecidas no pedido quando a transferência for para um país terceiro ou para uma organização internacional. No entanto, o Comité sublinha que o requerente deve sempre incluir uma descrição dos dados transferidos para outros sistemas ou organizações, independentemente da sua localização. Por conseguinte, o Comité incentiva a AC da República Checa a alterar a redação, a fim de evitar confusões.
27. O Comité observa que a obrigação de estabelecer no acordo de certificação os métodos de avaliação vinculativos (secção 3.2.1.2.1.2.6 do projeto de requisitos de acreditação da AC da República Checa) não contém uma referência ao alvo da avaliação, de acordo com o ponto 1, secção 7.3, do anexo das Orientações. Para efeitos de clareza, o Comité incentiva a AC da República Checa a incluir essa referência.
28. Além disso, o Comité observa que o projeto de requisitos de acreditação da AC da República Checa prevê os casos em que há recurso a subcontratantes para efetuar operações de tratamento de dados, em conformidade com o anexo das Orientações (secção 3.2.1.2.10.2 do projeto de requisitos de acreditação da AC da República Checa). O Comité incentiva a AC da República Checa a ponderar se,

neste caso, também deve ser feita uma referência aos responsáveis conjuntos pelo tratamento e aos seus acordos específicos.

29. No que se refere aos requisitos de avaliação (secção 3.2.1.2.10.4 do projeto de requisitos da AC da República Checa), o Comité observa que os requisitos de acreditação da AC da República Checa não preveem a obrigação do organismo de certificação de definir pormenorizadamente, no seu procedimento de certificação, de que modo devem ser fornecidas ao requerente as informações exigidas no ponto 7.4.6 da norma ISO 17065 sobre as não conformidades de um procedimento de certificação. Tal como estabelecido no anexo (subsecção 7.4), devem ser definidas, pelo menos, a natureza e o momento da prestação de tais informações. Por conseguinte, o Comité recomenda à AC da República Checa que acrescente a obrigação acima referida.
30. Além disso, a subsecção 3.2.1.2.10.4.2 do projeto de requisitos da AC da República Checa parece limitar os métodos de avaliação aos ensaios, auditorias ou inspeções. O Comité considera que podem ser utilizados outros métodos de avaliação e, por conseguinte, incentiva a AC da República Checa a alterar o projeto, a fim de deixar claro que a enumeração não é exaustiva.
31. No que se refere à subsecção 3.2.1.2.10.4.4.1.4 do projeto de requisitos de acreditação da AC da República Checa, o Comité considera que os requisitos devem indicar claramente que o organismo de certificação é obrigado a verificar o cumprimento dos critérios e incentiva a AC da República Checa a alterar o projeto em conformidade.
32. No que se refere aos requisitos de revisão (subsecção 3.2.1.2.10.5 do projeto de requisitos de acreditação da AC da República Checa), o Comité observa que o projeto de requisitos de acreditação da AC da República Checa não faz referência à obrigação de estabelecer procedimentos para a concessão e revogação de certificações. Por conseguinte, o Comité recomenda que a AC da República Checa altere o projeto em conformidade.
33. No que se refere aos requisitos em matéria de documentação de certificação, o Comité observa que a secção 3.1.2.10.7.2 do projeto de requisitos de acreditação da AC da República Checa estabelece que o organismo de certificação deve especificar que o controlo é uma condição de validade da certificação «nos casos em que esse controlo é exigido por um sistema de certificação [...]». O Comité considera que, no caso da certificação ao abrigo do RGPD, as atividades de controlo são sempre obrigatórias e, por conseguinte, recomenda à AC da República Checa que inclua essa obrigação.
34. No que se refere aos requisitos relativos ao diretório de produtos certificados (secção 3.2.1.2.10.8 do projeto de requisitos de acreditação da AC da República Checa e ponto 7.8 do anexo) e, em particular, à obrigação de informar a AC competente acerca das razões que levaram à concessão ou revogação da certificação solicitada, o Comité regista que o projeto de requisitos de acreditação da AC da República Checa remete para a secção 3.2.1.2.10.4.5. No entanto, esta secção respeita à obrigação de tornar a documentação de avaliação acessível à AC da República Checa, a pedido desta, ao passo que o requisito constante da secção 7.8 do anexo das Orientações prevê a obrigação de informar proativamente a AC dos motivos da concessão ou revogação da certificação. Por conseguinte, o Comité recomenda que a AC da República Checa altere o projeto em conformidade.
35. No que se refere às alterações que afetam a certificação, o Comité observa que o projeto de requisitos de acreditação da AC da República Checa não menciona, entre os procedimentos a acordar, o processo de aprovação a acordar com a autoridade de certificação competente, referido no anexo das Orientações (página 21). O Comité reconhece que a lista constante da secção 7.10 do anexo não é

obrigatória. No entanto, a fim de garantir a coerência, o Comité incentiva a AC da República Checa a aditar uma referência ao processo de aprovação a acordar com a AC.

36. O Comité observa que o projeto de requisitos da AC da República Checa não estabelece de forma clara a obrigação do organismo de certificação de aceitar decisões e ordens da AC competente para revogar ou não emitir a certificação a um requerente se os requisitos para certificação em caso de incumprimento dos requisitos de certificação. O Comité recomenda que a AC da República Checa inclua claramente essa obrigação no projeto de requisitos de acreditação. No que diz respeito à cessação, redução, suspensão ou revogação da certificação, o Comité observa que as secções 3.2.1.2.10.10.2 e 3.2.1.2.10.10.3 do projeto de requisitos fazem referência a uma «instigação». Se a intenção for fazer referência a «decisões e ordens» da AC, tal como estabelecido no artigo 58.º, n.º 2, alínea h), do RGPD, o Comité incentiva a AC da República Checa a utilizar a mesma terminologia que o RGPD, e a remeter para «decisões e ordens».

2.2.6 SISTEMA DE GESTÃO

37. O Comité considera que a secção 3.2.1.2.11 do projeto de requisitos adicionais da AC da República Checa não inclui a obrigação do organismo de certificação de «divulgar publicamente, de forma permanente e contínua, que certificações se realizaram e com base em quê [...], o período de validade das certificações e ao abrigo de que quadro e condições», conforme referido na secção 8 do anexo. Por conseguinte, o Comité recomenda à AC da República Checa que altere o projeto de requisitos, de modo a incluir a referência acima referida.

3 CONCLUSÕES/RECOMENDAÇÕES

38. O projeto de requisitos de acreditação da AC da República Checa poderá conduzir a uma aplicação incoerente da acreditação de organismos de certificação, pelo que é necessário introduzir as seguintes alterações:
39. No que diz respeito aos «requisitos gerais de acreditação», o Comité recomenda que a AC da República Checa:
- 1) inclua a obrigação de facultar o acesso da AC aos «assuntos contratualmente confidenciais» referidos na secção 3.2.1.2.1.2;
 - 2) substitua a expressão «informações sobre a concessão da certificação» por «informações necessárias para conceder a certificação» na subsecção 3.2.1.2.1.2.8;
 - 3) clarifique o teor da subsecção 3.2.1.2.1.2.9 em conformidade com o artigo 42.º, n.º 8, do RGPD;
 - 4) na subsecção 3.2.1.2.1.2.12, adite uma referência a [quando aplicável]: «as consequências para o cliente também devem ser abordadas»;
 - 5) altere a subsecção 3.2.1.2.1.2.13 a fim de incluir a menção a «todas as alterações na sua situação efetiva ou jurídica e nos seus produtos, processos e serviços a que a certificação diga respeito»;
 - 6) suprima a secção 3.2.1.2.1.3 e a subsecção 3.2.1.2.1.2.14;

- 7) inclua os requisitos em falta relativos à gestão da imparcialidade que se encontram previstos no anexo.
40. No que diz respeito aos «requisitos em matéria de recursos», o Comité recomenda que a AC da República Checa:
- 1) altere a secção 3.2.1.2.9.1 para especificar em que casos «a avaliação consiste em atividades de certificação» ou clarificar que o organismo de certificação continuará a ser responsável pela tomada de decisões, mesmo que recorra a peritos externos.
41. No que diz respeito aos «requisitos do processo», o Comité recomenda que a AC da República Checa:
- 1) inclua, na secção 3.2.1.2.10.4, a obrigação do organismo de certificação de definir pormenorizadamente, no seu procedimento de certificação, de que modo devem ser fornecidas ao requerente as informações exigidas no ponto 7.4.6 da norma ISO 17065 sobre as não conformidades de um procedimento de certificação;
 - 2) altere a secção 3.2.1.2.10.5 para fazer referência à obrigação de estabelecer procedimentos para a concessão e revogação de certificações;
 - 3) altere a secção 3.1.2.10.7.2 de modo a refletir que, no caso da certificação ao abrigo do RGPD, as atividades de controlo são sempre obrigatórias;
 - 4) altere a secção 3.2.1.2.10.8 de modo a refletir a obrigação do organismo de certificação de informar proativamente a AC dos motivos da concessão ou revogação da certificação;
 - 5) inclua a obrigação do organismo de certificação de aceitar decisões e ordens das AC competentes para revogar ou não emitir certificação a um requerente em caso de incumprimento dos requisitos de acreditação.
42. No que se refere ao «sistema de gestão», o Comité recomenda que a AC da República Checa:
- 1) inclua a obrigação do organismo de certificação de «divulgar publicamente, de forma permanente e contínua, que certificações se realizaram e com base em quê [...], o período de validade das certificações e ao abrigo de que quadro e condições», tal como previsto no ponto 8 do anexo.

4 OBSERVAÇÕES FINAIS

43. A autoridade de controlo da República Checa é a destinatária do presente parecer, que será tornado público nos termos do artigo 64.º, n.º 5, alínea b), do RGPD.
44. Nos termos do artigo 64.º, n.ºs 7 e 8, do RGPD, a AC da República Checa 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. No mesmo prazo, apresentará o projeto de lista alterado ou, caso não tencione seguir o parecer do Comité, no todo ou em parte, apresentará os motivos pertinentes de tal decisão.

45. A AC da República Checa comunica a decisão final ao Comité para 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)