Parecer 15/2020 sobre o projeto de decisão das autoridades de controlo competentes da Alemanha relativo 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.

Adotado

Índice

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 «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 o seguinte:

(1) A principal função do Comité consiste em assegurar a coerência na aplicação do Regulamento (UE) n.º 2016/679 («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 I das Orientações 4/2018 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 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 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 na competência técnica dos organismos de certificação acreditados.

(4) As «Orientações 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 «Orientações») e as «Orientações 1/2018 relativas à certificação e à deleção dos critérios de

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

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, esta deve 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 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 coerência[2].

(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 da Autoridade Europeia para a Proteção de Dados (AEPD), 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.

APROVOU O PRESENTE PARECER:

1 RESUMO DOS FACTOS

1. As Autoridades de Controlo alemãs da Federação e dos Länder (a seguir designadas «AC da Alemanha») apresentaram ao CEPD o seu projeto de requisitos de acreditação ao abrigo do artigo 43.º, n.º 1, alínea b). O processo foi considerado completo em 13 de fevereiro de 2020. O organismo nacional de acreditação (ONA) alemão, DakkS, procederá à acreditação dos organismos de certificação com recurso aos critérios de certificação do RGPD. Isto significa que o ONA recorrerá à norma ISO 17065 e aos requisitos adicionais estabelecidos pelas AC da Alemanha, uma vez aprovados por estas, 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] Orientações 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 as AC da Alemanha decidiram recorrer à acreditação conjunta pelo seu organismo nacional de acreditação (ONA), DakkS, e pela AC competente, para a emissão da acreditação, tendo estabelecido requisitos adicionais em conformidade com as Orientações, que devem ser aplicados aquando da emissão da acreditação.

4. Esta avaliação dos requisitos adicionais de acreditação das AC da Alemanha 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 pelas AC de modo a permitir a sua aplicação prática e coerente, conforme exigido pelo contexto das AC.

6. O Comité reconhece que, dados os conhecimentos especializados dos ONA e das AC competentes nesta área, deve ser-lhes concedida margem de manobra, quando aplicável, 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 e revisão práticas e coerentes, 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 «Anexo»). Quando o presente Parecer não se pronunciar relativamente a uma determinada secção do projeto de requisitos de acreditação das AC da Alemanha, tal significa que o Comité não tem observações a formular, nem solicita às AC da Alemanha que tomem medidas adicionais.

9. O presente parecer não aborda aspetos referidos pelas AC da Alemanha 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 da avaliação (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:

1) abordagem de todos os domínios-chave realçados no Anexo das Orientações e análise de eventuais desvios ao Anexo;

2) independência do organismo de certificação;

3) conflitos de interesses do organismo de certificação;

4) competência técnica do organismo de certificação;

5) garantias adequadas com vista a assegurar que os critérios de certificação do RGPD são adequadamente aplicados pelo organismo de certificação;

6) procedimentos para a emissão, revisão periódica e retirada da certificação ao abrigo do RGPD; e

7) 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 são 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 TERMOS E DEFINIÇÕES

12. O Comité observa que o capítulo 3 («Definições») do projeto de requisitos de acreditação das AC da Alemanha define os tipos de sistemas de certificação permitidos, especificando que devem cumprir os requisitos da norma DIN EN ISO/IEC 17065. A este respeito, importa salientar que os pontos 5.1 e 5.2 das Orientações do CEPD já explicitam de forma exaustiva o que pode ser certificado ao abrigo do RGPD. Por conseguinte, o Comité reconhece que a intenção das AC da Alemanha não é limitar o que é estabelecido nas Orientações e que as afirmações contidas no capítulo 3 do projeto de requisitos de acreditação das AC da Alemanha devem ser consideradas aplicáveis no contexto destes requisitos de acreditação.

2.2.3 OBSERVAÇÕES GERAIS

13. O Comité observa que a secção «notas gerais» do projeto de requisitos de acreditação das AC da Alemanha se refere à «autorização» dos critérios de certificação pelo CEPD «em conformidade com o artigo 63.º e com o artigo 64.º, n.º 1, alínea c), do RGPD». O Comité observa que o RGPD não confere ao CEPD competência para «autorizar» critérios de certificação. No entanto, de acordo com os artigos acima mencionados, o CEPD pode aprovar critérios de certificação. Por conseguinte, o Comité recomenda às AC da Alemanha que eliminem a referência à «autorização pelo CEPD», a fim de alinhar o projeto com a redação do RGPD.

2.2.4 REQUISITOS GERAIS DE ACREDITAÇÃO (capítulo 4 do projeto de requisitos de acreditação)

14. No que se refere ao requisito de responsabilidade legal (secção 4.1 do projeto de requisitos de acreditação das AC da Alemanha), o Comité observa que, no documento de apoio, as AC da Alemanha explicam que há uma expetativa de que o organismo de certificação disponha de procedimentos atualizados e que, por conseguinte, não é necessário acrescentar outros requisitos a esse respeito. No entanto, o Comité considera que uma expetativa não obriga os organismos de certificação a disporem desses procedimentos. Tal como estabelecido na secção 4.1.1 do Anexo das Orientações, os organismos de certificação devem dispor de procedimentos atualizados que comprovem o cumprimento das responsabilidades legais estipuladas nos termos da 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 às AC da Alemanha que alterem o projeto de requisitos, a fim de o alinhar com as Orientações.

15. No que se refere à subsecção 4.1.2.2 do projeto de requisitos de acreditação das AC da Alemanha («acordo de certificação»), o Comité observa que o projeto de requisitos de acreditação das AC da Alemanha não inclui a obrigação de permitir a plena transparência à AC competente no que se refere ao procedimento de certificação, incluindo questões contratuais confidenciais. Além disso, não existe qualquer referência à obrigação do requerente de facultar ao organismo de certificação o acesso às

suas atividades de tratamento. Por conseguinte, o Conselho recomenda às AC da Alemanha que incluam as obrigações acima referidas no seu projeto.

16. O Comité observa que a referência explícita às tarefas e poderes da AC competente (3.º travessão da secção 4.1.2 do Anexo) não está incluída na subsecção 4.1.2.2 do projeto de requisitos de acreditação das AC da Alemanha. O Comité considera que esta referência deverá ser aditada ao projeto de requisitos, pelo que recomenda que as AC da Alemanha alterem o projeto em conformidade.

17. Por outro lado, o projeto de requisitos das AC da Alemanha no que respeita ao acordo de certificação não inclui a obrigação de permitir que o organismo de certificação divulgue todas as informações necessárias para a concessão da certificação nos termos do artigo 42.º, n.º 8, e do artigo 43.º, n.º 5, do RGPD (7.º travessão da secção 4.1.2 do Anexo). Embora essa obrigação esteja incluída na secção de gestão do processo do projeto de requisitos de acreditação das AC da Alemanha, o Comité considera que deve fazer parte do acordo de certificação, a fim de reforçar o seu caráter vinculativo. Deste modo, o Comité recomenda às AC da Alemanha que incluam a obrigação acima referida como parte dos elementos do acordo de certificação.

18. De acordo com o Anexo, o requerente tem de informar o organismo de certificação de alterações significativas na sua situação efetiva ou jurídica e nos seus produtos, processos e serviços a que a certificação diga respeito (10.º travessão da secção 4.1.2 do Anexo). No entanto, no projeto de requisitos de acreditação das AC da Alemanha, o travessão 6 da subsecção 4.1.2.2 inclui apenas a obrigação de informar o organismo de certificação de alterações significativas nas circunstâncias efetivas ou jurídicas, mas não menciona expressamente os produtos, processos e serviços. O Comité recomenda às AC da Alemanha que incluam essa referência, em conformidade com o Anexo.

19. No que se refere à subsecção 4.2.7 do projeto de requisitos de acreditação das AC da Alemanha («tratamento da imparcialidade»), o Comité recomenda o reforço dos critérios aplicáveis aos organismos de certificação que pertençam ou sejam controlados por uma pessoa coletiva distinta, de modo a ter em consideração que qualquer tipo de relação económica entre o organismo de certificação e a pessoa coletiva, em função das suas características, pode afetar a imparcialidade das suas atividades de certificação.

20. No que se refere à secção 4.6 do projeto de requisitos de acreditação das AC da Alemanha («informações acessíveis ao público»), o Comité observa que não existe qualquer referência à publicação de todas as versões dos critérios aprovados e dos procedimentos de certificação. Consequentemente, o Comité incentiva as AC da Alemanha a alterarem o projeto de requisitos de acreditação, a fim de explicitar que a publicação inclui todas as versões dos critérios aprovados e dos procedimentos de certificação. Além disso, o Comité observa que o número dois da secção 4.6 estabelece que «os sistemas de certificação utilizados pelo organismo de certificação os critérios aprovados em conformidade com o artigo 42.º, n.º 5, do RGPD que indicam a duração autorizada do pedido *devem ser publicados em geral*». Para evitar qualquer ambiguidade, o Comité incentiva as AC da Alemanha a eliminarem a expressão «em geral» e a incluir um «e» entre «organismo de certificação» e «os critérios aprovados».

2.2.5 REQUISITOS EM MATÉRIA DE RECURSOS (capítulo 6 do projeto de requisitos de acreditação)

21. No que respeita aos requisitos em matéria de conhecimentos especializados e, especificamente, à subsecção 6.1.2.1 do projeto de requisitos de acreditação das AC da Alemanha («competência em

matéria de recursos humanos»), o Comité observa que os conhecimentos exigidos nos domínios enumerados não especificam que os conhecimentos devem ser relevantes e apropriados. A fim de garantir a coerência com o nível de conhecimentos especializados exigido no Anexo, o Comité recomenda às AC da Alemanha que alinhem a redação com as Orientações, exigindo que os conhecimentos sejam relevantes e apropriados.

22. O Comité observa ainda que os requisitos aplicáveis ao pessoal com conhecimentos técnicos especializados responsável pela tomada de decisões incluem, pelo menos, sete anos de experiência profissional ou cinco anos de experiência profissional em matéria de proteção de dados técnicos, em função do seu nível de educação, ao passo que o pessoal responsável pelas avaliações deve ter quatro anos de experiência profissional ou dois anos de experiência profissional em matéria de proteção de dados técnicos e experiência no procedimento de testes, em função do seu nível de educação. De igual modo, o pessoal com conhecimentos jurídicos especializados que tome decisões deve ter, pelo menos, cinco anos de experiência profissional em legislação sobre a proteção de dados, ao passo que os encarregados das avaliações devem ter, pelo menos, dois anos de experiência em legislação sobre a proteção de dados e nos procedimentos de auditoria. O Comité observa que o número mínimo de anos exigido de experiência profissional entre o pessoal responsável pela tomada de decisões e o pessoal responsável pela avaliação difere ligeiramente. A este respeito, o Comité considera que os requisitos de competência aplicáveis aos avaliadores e aos decisores deverão ser adaptados tendo em conta as diferentes tarefas que desempenham, e não o número de anos de experiência. No entender do Comité, os avaliadores deverão ter conhecimentos e experiência profissional mais especializados em procedimentos técnicos (por exemplo, auditorias e certificações), ao passo que os decisores deverão ter conhecimentos e experiência profissional mais gerais e abrangentes em matéria de proteção de dados. Assim, o Comité incentiva as AC da Alemanha a darem maior ênfase ao conhecimento substantivo e/ou experiência diferentes para os avaliadores e para os decisores, e a reduzirem as divergências nos anos de experiência que lhes são exigidos.

23. Além disso, o Comité considera que o conhecimento dos sistemas de gestão relevantes para o domínio da certificação deverá ser estendido à norma ISO/IEC 27701:2019 – Técnicas de segurança – Extensão à norma ISO/IEC 27001 e norma ISO/IEC 27002 sobre gestão da privacidade da informação – Requisitos e orientações e incentiva as AC da Alemanha a incluírem tal referência.

24. Por último, no que se refere aos requisitos de educação do pessoal técnico, o Comité considera que a lista de matérias já está adaptada aos conhecimentos técnicos especializados exigidos pelo Anexo. Por conseguinte, o Comité incentiva as AC da Alemanha a eliminarem a referência às «ciências naturais» da lista de disciplinas relativas ao ensino universitário do pessoal técnico.

2.2.6 REQUISITOS PROCESSUAIS (capítulo 7 do projeto de requisitos de acreditação)

25. O Comité observa que o capítulo 7 do projeto de requisitos de acreditação das AC da Alemanha faz várias referências ao termo «os seus critérios» (por exemplo, nas secções 7.4, 7.6, 7.11 e 7.13). A fim de evitar qualquer ambiguidade, o Comité incentiva as AC da Alemanha a esclarecerem o significado desse termo, por exemplo, aditando uma explicação no apêndice 1 (glossário).

26. No que se refere à secção 7.1 do projeto de requisitos de acreditação das AC da Alemanha («informações gerais»), o Comité observa que não existe qualquer referência expressa à obrigação do organismo de certificação de cumprir os requisitos adicionais. Embora tal obrigação possa ser inferida do texto do projeto de requisitos, o Comité considera que deverá ser incluída uma referência expressa

à obrigação acima referida. Por conseguinte, o Comité recomenda que as AC da Alemanha alterem o projeto em conformidade.

27. O Comité observa que o projeto de requisitos adicionais das AC da Alemanha não contém qualquer referência ao funcionamento de um Selo Europeu de Proteção de Dados aprovado, em conformidade com a secção 7.1.2 do Anexo. O Comité considera que esta referência deverá ser incluída, tendo especialmente 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 estabelecido [3]. Por conseguinte, o Comité recomenda às AC da Alemanha que incluam a referência acima mencionada. Por exemplo, o projeto de requisitos poderia estabelecer o seguinte: *«A AC competente deve ser notificada antes de um organismo de certificação começar a utilizar um Selo Europeu de Proteção de Dados num novo Estado-Membro a partir de um escritório de representação.»*

28. O Comité observa que, na secção 7.2 («requerimento»), o projeto de requisitos de acreditação das AC da Alemanha prevê a situação em que há recurso a subcontratantes para efetuar operações de tratamento de dados, em conformidade com o Anexo das Orientações. No entanto, o Comité observa que, quando houver recurso a subcontratantes, o requerimento deve incluir o(s) contrato(s) do responsável pelo tratamento de dados/subcontratante em questão, conforme indicado no Anexo. Por conseguinte, o Comité recomenda às AC da Alemanha que alinhem a redação com as orientações, incluindo a referência ao(s) contrato(s) do responsável pelo tratamento/subcontratante. Além disso, o Comité incentiva as AC da Alemanha a ponderarem se, neste caso, também deveria ser mencionada uma referência aos responsáveis conjuntos pelo tratamento e aos seus acordos específicos.

29. O Comité observa que a secção 7.2 do projeto de requisitos de acreditação das AC da Alemanha especifica que «o responsável pelo tratamento de dados e o subcontratante têm o direito de requerer a certificação». A possibilidade de os subcontratantes requererem a certificação dependerá do sistema de certificação específico. Por conseguinte, a fim de evitar confusões, o Comité incentiva as AC da Alemanha a eliminarem a referência acima mencionada ou a esclarecerem que a possibilidade de certificação dos subcontratantes dependerá do âmbito do sistema de certificação.

30. No que se refere à secção 7.3 do projeto de requisitos de acreditação das AC da Alemanha («pedidos de avaliação»), o Comité observa que o projeto de requisitos de acreditação das AC da Alemanha prevê que «os métodos de avaliação previstos devem ser contratualmente estabelecidos [...]». A fim de deixar claro que se trata de um requisito, o Comité incentiva as AC a reformularem o primeiro parágrafo, a fim de esclarecer que os métodos de avaliação devem ser incluídos no acordo de certificação, ou seja, a reformularem o requisito segundo o qual «os métodos de avaliação previstos devem ser contratualmente estabelecidos [...]». O Comité incentiva ainda as AC da Alemanha a substituírem a referência à secção 7.3.1.b da norma ISO 17065 pela secção 7.3 da norma ISO 17065, a fim de alinhar a redação com o Anexo. Além disso, o Comité observa que o quarto parágrafo refere competências técnicas e jurídicas apropriadas. Por uma questão de clareza, o Comité incentiva as AC da Alemanha a aditarem «no domínio da proteção de dados».

31. O Comité observa que a secção 7.4 do projeto de requisitos de acreditação das AC da Alemanha («métodos de avaliação») não inclui a obrigação do organismo de certificação de descrever métodos de avaliação suficientes para avaliar o cumprimento das operações de tratamento em função dos critérios de certificação. O Comité recomenda às AC da Alemanha que alterem o projeto de requisitos,

[3] A este respeito, consultar as Orientações 1/2018, número 44.

a fim de incluírem tal referência. Poderiam, por exemplo, aditar o seguinte: *«O organismo de certificação deve assegurar que os mecanismos utilizados para conceder a certificação descrevam métodos de avaliação suficientes para avaliar o cumprimento das operações de tratamento em função dos critérios de certificação*.» Além disso, no que se refere ao primeiro domínio que será abrangido pelos métodos de avaliação, o Comité considera que a necessidade e a proporcionalidade devem ser avaliadas também em relação aos titulares dos dados em questão, quando aplicável. Por último, o Comité regista que não existe qualquer referência à documentação dos métodos e conclusões. Assim, o Comité incentiva as AC da Alemanha a alterarem o projeto e a incluírem expressamente essas referências.

32. No que se refere às certificações existentes (secção 7.4 do projeto de requisitos de acreditação das AC da Alemanha), o Comité considera que o quarto travessão da página 13 gera confusão, uma vez que não é clara a relação entre os períodos de validade da certificação atual e da certificação anterior nem a forma como se combinam entre si. Além disso, não parece viável pôr em causa a validade da certificação anteriormente emitida por um outro organismo de certificação acreditado. Em suma, o parágrafo beneficiaria de alguma clareza no que respeita à relação entre os diferentes elementos mencionados. O Comité recomenda às AC da Alemanha que alterem o projeto, em especial clarificando que o prazo de validade da certificação do RGPD não deve ser condicionada à validade de outros tipos de certificações.

33. Relativamente à secção 7.5 («avaliação») do projeto de requisitos de acreditação das AC da Alemanha, o Comité incentiva as AC da Alemanha a alterarem o título da secção para «revisão».

34. No que diz respeito às alterações que afetam a certificação (secção 7.10 do projeto de requisitos de acreditação das AC da Alemanha), o Comité regista que o projeto de requisitos de acreditação das AC da Alemanha estabelece que «o cliente é informado atempadamente sobre as alterações ao quadro normativo que o afetem». Tendo em conta a necessidade de preservar a imparcialidade do organismo de certificação, o Comité incentiva as AC da Alemanha a reformularem a frase de modo a deixar claro que são atempadamente prestadas ao cliente informações gerais sobre as alterações que o possam afetar. Além disso, a fim de assegurar uma compreensão clara do que se entende por «decisões do Comité Europeu para a Proteção de Dados», o Comité incentiva as AC da Alemanha a clarificarem a referência. Poderia, por exemplo, referir-se a «documentos aprovados pelo Comité Europeu para a Proteção de Dados».

35. O Comité observa que a secção 7.11 do projeto de requisitos de acreditação das AC da Alemanha («cessação, restrição, suspensão ou revogação da certificação») não contém a obrigação do organismo de certificação de aceitar decisões e ordens emitidas pelas AC da Alemanha para revogar ou não emitir a certificação a um requerente se os requisitos de acreditação não forem ou deixarem de ser cumpridos. Por conseguinte, o Comité recomenda que as AC da Alemanha incluam essa obrigação. O Comité incentiva ainda as AC da Alemanha a substituírem o termo «restrição» por «redução» no título da secção, em conformidade com o Anexo das Orientações.

2.2.7 OUTROS REQUISITOS ADICIONAIS

36. No que se refere à subsecção 8.11.3 do projeto de requisitos de acreditação das AC da Alemanha («gestão de reclamações»), o Comité incentiva as AC da Alemanha a substituírem a referência a «reclamações justificadas» por «reclamações fundamentadas», a fim de proporcionar maior clareza.

3 CONCLUSÕES/RECOMENDAÇÕES

37. O projeto de requisitos de acreditação da Autoridades de Controlo da Federação e dos Länder poderá conduzir a uma aplicação incoerente da acreditação de organismos de certificação, pelo que é necessário introduzir as seguintes alterações:

38. A título de «observação geral», o Comité recomenda que as AC da Alemanha:

    1) eliminem a referência à «autorização pelo CEPD», a fim de alinhar o projeto com a redação do RGPD.

39. No que diz respeito aos «requisitos gerais de acreditação», o Comité recomenda que as AC da Alemanha:

    1) alterem os requisitos relativos à responsabilidade legal (subsecção 4.1), a fim de os colocar em conformidade com as orientações.

    2) alterem a subsecção 4.1.2.2 para incluir, no acordo de certificação, a obrigação de permitir total transparência às AC da Alemanha a respeito do procedimento de certificação e para fornecer ao organismo de certificação acesso às atividades de tratamento do requerente.

    3) incluir, na subsecção 4.1.2.2, uma referência expressa às tarefas e poderes da AC competente, em conformidade com o Anexo.

    4) incluir, entre os elementos do acordo de certificação, a obrigação de permitir que o organismo de certificação divulgue todas as informações necessárias para a concessão da certificação nos termos do artigo 42.º, n.º 8, e do artigo 43.º, n.º 5, do RGPD.

    5) incluir uma referência expressa aos «produtos, processos e serviços a que a certificação diga respeito» no travessão 6 da subsecção 4.1.2.2.

    6) reforçar, na subsecção 4.2.7, os critérios aplicáveis aos organismos de certificação que pertençam ou que sejam controlados por uma pessoa coletiva distinta, de modo a ter em consideração que qualquer tipo de relação económica entre o organismo de certificação e a pessoa coletiva, em função das suas características, pode afetar a imparcialidade das suas atividades de certificação.

40. No que diz respeito aos «requisitos em matéria de recursos», o Comité recomenda que as AC da Alemanha:

    1) alinhem a redação da subsecção 6.1.2.1 com as orientações, exigindo que os conhecimentos sejam relevantes e apropriados.

41. No que diz respeito aos «requisitos processuais», o Comité recomenda que as AC da Alemanha:

    1) alterem a secção 7.1 para conter uma referência expressa à obrigação do organismo de certificação de cumprir os requisitos adicionais.

2) incluam uma referência ao funcionamento de um Selo Europeu de Proteção de Dados aprovado.

3) alinhem a redação da secção 7.2 com as orientações, incluindo a referência ao(s) contrato(s) do responsável pelo tratamento/subcontratante.

4) incluam na secção 7.4 a obrigação do organismo de certificação de descrever métodos de avaliação suficientes para avaliar o cumprimento das operações de tratamento em função dos critérios de certificação.

5) clarifiquem na secção 7.4 que o prazo de validade da certificação do RGPD não deve ser condicionado à validade de outros tipos de certificações.

6) incluir na secção 7.11 a obrigação do organismo de certificação de aceitar decisões e ordens emitidas pelas AC da Alemanha para revogar ou não emitir certificação a um requerente se os requisitos de acreditação deixarem de ser cumpridos.

4 OBSERVAÇÕES FINAIS

42. O presente parecer é dirigido às Autoridades de Controlo da Federação e dos Länder e será tornado público nos termos do artigo 64.º, n.º 5, alínea b), do RGPD.

43. Nos termos do artigo 64.º, n.ºs 7 e 8, do RGPD, as AC da Alemanha comunicam à Presidente, por via eletrónica, no prazo de duas semanas a contar da receção do parecer, se tencionam manter ou alterar o seu projeto de decisão. No mesmo prazo, apresentam o projeto de decisão alterado ou, caso não tencionem seguir o parecer do Comité, no todo ou em parte, apresentam os motivos pertinentes de tal decisão.

44. As AC da Alemanha comunicam 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)