Parecer 14/2020 sobre o projeto de decisão da autoridade de controlo competente da Irlanda relativa à aprovação dos requisitos de acreditação de um organismo de certificação nos termos do artigo 43.º, n.º 3 (RGPD)

Aprovado em 25 de maio de 2020

Aprovado

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 (Regulamento Geral sobre a Proteção de Dados, 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 Diretrizes 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 Diretrizes do CEPD relativas à acreditação dos organismos de certificação).

2) Nos termos do artigo 43.º do RGPD, as autoridades de controlo competentes devem aprovar 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 «Diretrizes 4/2018 relativas à acreditação dos organismos de certificação nos termos do artigo 43.º do Regulamento Geral sobre Proteção de Dados (2016/679)» (a seguir designadas «Diretrizes») e as «Diretrizes 1/2018 relativas à certificação e à seleção de critérios de certificação em

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

conformidade com os artigos 42.º e 43.º do Regulamento (UE) 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, esta deve estabelecer requisitos de acreditação, incluindo, entre outros, os requisitos especificados no artigo 43.º, n.º 2, do RGPD. Em comparação com as obrigações relativas à acreditação de organismos de certificação pelos organismos nacionais de acreditação, o artigo 43.º do RGPD 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), do RGPD. O CEPD observa que o artigo 43.º, n.º 2, alíneas a) a e), do RGPD, reflete e especifica requisitos da norma ISO 17065, o que contribuirá para a coerência[2].

6) O parecer do CEPD é aprovado 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.

APROVOU O PRESENTE PARECER:

1 EXPOSIÇÃO SUMÁRIA DOS FACTOS

1. A Autoridade de Controlo da Irlanda (adiante designada «AC da Irlanda») apresentou o respetivo projeto de requisitos de acreditação nos termos do artigo 43.º, n.º 1, alínea b) ao CEPD. O processo foi considerado completo em 13 de fevereiro de 2020. O organismo nacional de acreditação (INAB) da Irlanda procederá à acreditação de organismos de certificação com recurso aos critérios de certificação do RGPD. Isto significa que o INAB utilizará a norma ISO 17065 e os requisitos adicionais estabelecidos pela AC da Irlanda, 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] Diretrizes 4/2018 relativas à acreditação de organismos de certificação nos termos do artigo 43.º do Regulamento Geral sobre a Proteção de Dados, ponto 39. Disponível em: https://edpb.europa.eu/our-work-tools/our-documents/retningslinjer/guidelines-42018-accreditation-certification-bodies_en

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 Irlanda decidiu recorrer ao seu organismo nacional de acreditação (ONA) para a emissão da acreditação, tendo estabelecido requisitos adicionais em conformidade com as Diretrizes, que devem ser utilizados pelo respetivo ONA quando da emissão da acreditação.

4. A avaliação dos requisitos adicionais de acreditação da AC da Irlanda destina-se a analisar as diferenças (aditamentos ou supressões) em relação às Diretrizes e, em particular, ao seu Anexo I. 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 Diretrizes relativas à acreditação dos organismos de certificação consiste em auxiliar as AC na definição dos seus requisitos de acreditação. O Anexo das Diretrizes 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 Diretrizes (adiante designado «Anexo»). Quando o presente parecer não se pronuncia relativamente a uma determinada secção do projeto de requisitos de acreditação da AC da Irlanda, tal significa que o Comité não tem observações a formular, nem solicita à AC da Irlanda que tome medidas adicionais.

9. O presente parecer não aborda aspetos referidos pela AC da Irlanda 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 Diretrizes 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 Diretrizes 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 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, devem também ser aplicados os requisitos adicionais estabelecidos pela autoridade de controlo competente;

f. O Anexo 1 das Diretrizes 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 INTRODUÇÃO (secção 0 do projeto de requisitos de acreditação da AC da Irlanda)

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 a referência às Diretrizes relativas à acreditação como «WP 261» não está atualizada. O CEPD aprovou as Diretrizes 4/2018 relativas à acreditação de organismos de certificação nos termos do artigo 43.º do Regulamento Geral sobre a Proteção de Dados (2016/679). Deste modo, o Comité incentiva a AC da Irlanda a alterar a redação e a fazer referência às Diretrizes 4/2018.

2.2.3 OBSERVAÇÕES GERAIS

13. O Comité observa que o projeto de requisitos da AC da Irlanda refere-se reiteradamente à «autoridade de controlo competente». Uma vez que a AC competente neste caso é a AC da Irlanda, o Comité encoraja a AC da Irlanda a substituir a referência por «DPC» ou «a AC da Irlanda», para evitar confusão.

14. O Comité reconhece que o projeto de requisitos da AC da Irlanda inclui uma secção relativa aos termos e definições. Contudo, alguns dos termos não são usados de uma forma consistente ao longo do documento (por exemplo, «objeto de avaliação» e «alvo de avaliação». A fim de evitar confusão, o Comité encoraja a AC da Irlanda a usar terminologia consistente no projeto de requisitos.

2.2.4 REQUISITOS GERAIS PARA ACREDITAÇÃO (secção 4 do projeto de requisitos de acreditação)

15. No tocante à cláusula 7 da subsecção 4.1.2 do projeto de requisitos de acreditação da AC da Irlanda, o Comité considera que a redação é ligeiramente confusa no que diz respeito a quem são fornecidas as razões para aprovar a certificação. Além disso, a referência a «facilitar» o registo é também pouco clara. Por conseguinte, o Comité encoraja a AC da Irlanda a reformulá-la de uma forma mais clara.

2.2.5 REQUISITOS ESTRUTURAIS (secção 5 do projeto de requisitos de acreditação)

16. O Comité observa que o projeto de requisitos de acreditação da AC da Irlanda faz referência à nomeação de «uma pessoa com a antiguidade relevante, responsável por supervisionar a conformidade da proteção de dados e a governação das informações.» A referência à antiguidade relevante deverá ser clarificada em termos de experiência e o âmbito de autoridade. Além disso, as funções desta figura parecem similares às de um encarregado da proteção de dados. O Comité encoraja a AC da Irlanda a definir de forma clara as funções desta figura e a especificar a experiência relevante.

2.2.6 REQUISITOS EM MATÉRIA DE RECURSOS (secção 6 do projeto de requisitos de acreditação)

17. No que se refere ao pessoal do organismo de certificação (subsecção 6.1), o Comité observa que os requisitos para pessoal com competências técnicas responsável por tomar decisões incluem ter, pelo menos, cinco anos de experiência profissional relacionada com a temática da certificação, ao passo que o pessoal responsável pelas avaliações deve ter, pelo menos, dois anos de experiência profissional. De igual modo, o pessoal com competências jurídicas que toma decisões deve ter, pelo menos, cinco anos de experiência profissional, ao passo que os encarregados das avaliações devem ter, pelo menos, dois anos de experiência. 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 a tónica deve ser colocada no tipo diferente de competências, ao invés do número de anos de experiência profissional. No entender do Comité, os avaliadores devem ter competências mais especializadas e experiência profissional em procedimentos técnicos (por exemplo, auditorias e certificações), ao passo que os decisores devem ter competências mais gerais e abrangentes e experiência profissional na proteção de dados. Assim, o Comité encoraja a AC da Irlanda a dar maior ênfase ao conhecimento substantivo e/ou experiência diferentes para os avaliadores e os decisores e a reduzir as divergências nos anos experiência que lhes são exigidos.

2.2.7 REQUISITOS RELATIVOS AO PROCESSO (secção 7 do projeto de requisitos de acreditação)

18. No atinente à subsecção 7.10 do projeto de requisitos de acreditação da AC da Irlanda («Mudanças que afetam a certificação»), o Comité observa que não existe referência aos procedimentos de mudança a serem acordados, de acordo com a secção 7.10 do Anexo. O Comité encoraja a AC da Irlanda a incluir essa referência e a mencionar alguns dos procedimentos que poderiam ser criados (por exemplo, períodos de transição, processo de aprovações com a AC competente...). Adicionalmente, o Comité considera que as mudanças no estado-da-arte também são relevantes e podem afetar a certificação. Por conseguinte, o Comité encoraja a AC da Irlanda a incluir esta possibilidade na lista de alterações que afetam a certificação. Por último, o Comité saúda a inclusão de violações e infrações de dados pessoais do RGPD na lista de mudanças que podem afetar a certificação. Todavia, a fim de assegurar clareza, o Comité encoraja a AC da Irlanda a especificar que violações ou infrações do RGPD devem ser tidas em conta apenas na medida em que estejam relacionadas com a certificação.

19. No tocante às mudanças que afetam a certificação (subsecção 7.10 do projeto de requisitos da AC da Irlanda) e, em particular, o quinto ponto, o Comité observa que a AC da Irlanda se refere a «decisões vinculativas aplicáveis do Comité Europeu para a Proteção de Dados» e também ao artigo 39.º do Regulamento Interno do CEPD, que inclui «todos os documentos finais aprovados pelo CEPD». A fim de assegurar uma compreensão clara do que se entende por «decisões do Comité Europeu para a Proteção de Dados», o Comité aconselha a AC da Irlanda a clarificar a referência. Poderia, por exemplo, referir-se a «documentos aprovados pelo Comité Europeu para a Proteção de Dados».

20. O Comité observa que a subsecção 7.11 do projeto de requisitos da AC da Irlanda (cessação, restrição, suspensão ou retirada de certificação) não contém a obrigação de o organismo de certificação aceitar decisões e ordens da AC da Irlanda para retirar ou não emitir certificação a um

requerente, se os requisitos para certificação não estiverem ou deixarem de estar satisfeitos. Por conseguinte, o Comité recomenda que a AC da Irlanda inclua essa obrigação.

3 CONCLUSÕES/RECOMENDAÇÕES

21. O projeto de requisitos de acreditação da Autoridade de Controlo da Irlanda poderá conduzir a uma aplicação incoerente da acreditação de organismos de certificação, pelo que é necessário introduzir as seguintes alterações:

22. No que diz respeito aos «requisitos relativos ao processo», o Comité recomenda que a AC da Irlanda:

1) inclua, na subsecção 7.11, a obrigação de o organismo de certificação aceitar decisões e ordens da AC da Irlanda para retirar ou não emitir certificação a um requerente, se os requisitos para certificação não estiverem ou deixarem de estar satisfeitos.

4 OBSERVAÇÕES FINAIS

23. A AC da Irlanda é a destinatária do presente parecer, que será tornado público nos termos do artigo 64.º, n.º 5, alínea b), do RGPD.

24. Nos termos do artigo 64.º, n.^{os} 7 e 8, do RGPD, a AC da Irlanda comunicará 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.

25. A AC da Irlanda 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)