COMISSÃO NACIONAL DE PROTEÇÃO DE DADOS

Regulamento n.º 834/2021

Sumário: Requisitos adicionais de acreditação para os organismos de certificação.

De acordo com a alínea *p*) do n.º 1 do artigo 57.º, bem como a alínea *b*) do n.º 1 do artigo 43.º e o n.º 3 do artigo 43.º, do Regulamento Geral sobre a Proteção de Dados ([1]), doravante referido como RGPD, compete à Comissão Nacional de Proteção de Dados (CNPD) fixar os requisitos adicionais de acreditação face à ISO/IEC 17065/2012.

Ao abrigo do disposto na alínea *e*) do n.º 1 do artigo 6.º da Lei n.º 58/2019, de 8 de agosto ([2]), a CNPD, enquanto autoridade nacional de controlo de proteção de dados, e o Instituto Português de Acreditação, I. P. (IPAC), enquanto organismo nacional de acreditação, estabeleceram através de protocolo os termos de cooperação e articulação entre as duas instituições no âmbito dos procedimentos de acreditação ([3]).

O presente regulamento define os requisitos adicionais de acreditação, apresentados, na sua estrutura e numeração, em conformidade com as secções correspondentes da ISO/IEC 17065/2012. Deste modo, especifica-se em cada ponto ou secção os requisitos relativos à proteção dos dados pessoais, assinalando-se ainda as situações em que não se impõem requisitos adicionais aos definidos na ISO/IEC 17065/2012.

Na elaboração dos requisitos adicionais de acreditação foram tidas em conta as diretrizes do Comité Europeu para a Proteção de Dados quanto à implementação da acreditação e da certificação do tratamento de dados pessoais ([4]).

Não se realizou consulta pública, porquanto o presente regulamento reflete, no essencial, as diretrizes aprovadas pelo Comité Europeu para a Proteção de Dados sobre esta matéria, as quais foram já objeto de consulta pública, e a cujo teor, assim como ao parecer emitido pelo mesmo Comité sobre o projeto de regulamento, a CNPD está legalmente vinculada.

Os requisitos adicionais de acreditação são vinculativos, podendo ser objeto de revisão e atualização quando tal se revelar necessário.

Assim, ao abrigo do disposto na alínea *b*) do n.º 1 do artigo 43.º, no n.º 3 do artigo 43.º e na alínea *p*) do n.º 1 do artigo 57.º do RGPD, a CNPD determina os seguintes requisitos adicionais de acreditação em relação à ISO/IEC 17065/2012:

1 — Objetivo e âmbito de aplicação

O âmbito de aplicação da ISO/IEC 17065/2012 (doravante, ISO/IEC 17065), que cobre produtos, processos e serviços, é mais lato do que o âmbito da certificação regulada pelo RGPD, pelo que, para o efeito de aplicação do presente regulamento, a ISO/IEC 17065 deve ser aplicada em conformidade com aquele.

A certificação ao abrigo do RGPD tem de abranger o tratamento de dados pessoais, só sendo aplicável às operações de tratamentos de dados realizadas pelos responsáveis e pelos subcontratantes, de acordo com o n.º 1 do artigo 42.º do RGPD.

2 — Referências normativas

O presente regulamento tem como referências normativas os seguintes atos jurídicos:

RGPD;

Lei n.º 58/2019, de 8 de agosto;

DRC001 (Regulamento Geral de Acreditação), publicado pelo IPAC, e documentos nele referenciados.

O RGPD prevalece sobre a ISO/IEC 17065. Sempre que, nos requisitos adicionais ou no procedimento de certificação, se faça referência aos requisitos da ISO/IEC 17065, devem os mesmos ser interpretados em conformidade com o RGPD.

3 — Termos e definições

Adotam-se os termos e definições da ISO/IEC 17065 sempre que não divirjam dos termos e definições do RGPD, tal como interpretados pelo Comité Europeu para a Proteção de Dados nas suas orientações relativas à acreditação e certificação ([5]), que aqui se dão por reproduzidos.

4 — Requisitos gerais

4.1 — Aspetos legais e contratuais

4.1.1 — O organismo de certificação deve estar em condições de demonstrar, a todo o tempo, ao IPAC que dispõe de procedimentos atualizados suscetíveis de comprovar o cumprimento das responsabilidades jurídicas definidas nos termos da acreditação, incluindo os requisitos adicionais relativos à aplicação do RGPD. Além disso, deve estar em condições de demonstrar que tem procedimentos conformes ao RGPD e medidas específicas para tratar os dados pessoais dos requerentes e clientes ([6]), no âmbito do processo de certificação.

Em especial, deve informar se tem conhecimento de que está a ser investigado pela CNPD e se foi condenado por violação do regime jurídico de proteção de dados nos últimos 4 (quatro) anos. Independentemente do cumprimento deste dever, o IPAC pode consultar a CNPD para obter a informação necessária no âmbito do procedimento de acreditação.

O procedimento de acreditação pode ficar prejudicado caso tenha havido violação do RGPD e decisão sancionatória emitida pela CNPD, justificando a suspensão do procedimento, até que seja demonstrada pelo requerente a adoção das medidas necessárias à correção daquela violação.

4.1.2 — O organismo de certificação deve demonstrar que o seu contrato de certificação:

a) Exige que o requerente cumpra também os critérios de certificação aprovados pela CNPD ou pelo Comité Europeu para a Proteção de Dados ([7]);

b) Exige que o requerente garanta a total transparência perante a CNPD no âmbito do procedimento de certificação, em especial o acesso a informação necessária para a verificação do respeito pelo regime de proteção de dados, incluindo informação abrangida por cláusulas contratuais de confidencialidade relativas ao cumprimento do regime de proteção de dados ([8]);

c) Exige que o requerente garanta o acesso para efeito de realização de testemunhos e visitas de controlo por parte do IPAC;

d) Não diminui a responsabilidade do requerente no cumprimento do regime de proteção de dados pessoais e não prejudica as atribuições e os poderes da CNPD;

e) Exige que o requerente garanta ao organismo de certificação o acesso às suas atividades de tratamento e a toda a informação necessário para a tramitação e conclusão do procedimento de certificação ([9]);

f) Exige que o requerente observe os prazos e os procedimentos aplicáveis, designadamente os decorrentes do mecanismo de certificação;

g) Especifica as regras de validade, renovação e de retirada da certificação, incluindo a definição de intervalos adequados para a reavaliação ou revisão ([10]);

h) Legitima o organismo de certificação a disponibilizar à CNPD toda a informação respeitante à fundamentação da concessão da certificação, bem como a fornecer os elementos necessários ao registo público dos procedimentos de certificação pelo Comité Europeu para a Proteção de Dados ([11]);

i) Inclui regras sobre a investigação de reclamações, vinculando o cliente a garantir a transparência e o acesso às regras e procedimentos de gestão de reclamações ([12]);

j) Explicita as consequências da retirada ou suspensão da acreditação para o organismo de certificação, incluindo eventual impacto e consequências para o cliente e as medidas que podem ser subsequentemente adotadas;

k) Exige que o requerente informe, logo que disso tome conhecimento, o organismo de certificação da ocorrência de situações de incumprimento do RGPD e da demais legislação de proteção de dados aplicável, declaradas pela CNPD ou pelos Tribunais, ou de outra certificação de proteção de dados que possa afetar a certificação requerida, bem como de qualquer alteração nos produtos, processos ou serviços a que a certificação diga respeito;

l) Define os métodos de avaliação vinculativos quanto ao objeto da certificação.

4.1.3 — O organismo de certificação só pode usar certificados, marcas e selos que cumpram o disposto nos artigos 42.º e 43.º do RGPD e nas diretrizes sobre acreditação e certificação aprovadas pelo Comité Europeu para a Proteção de Dados ([13]).

4.2 — Gestão da imparcialidade

O organismo de certificação deve demonstrar, de modo satisfatório para a CNPD, que é independente da organização requerente da certificação, conforme exigido na alínea *a*) do n.º 2 do artigo 43.º do RGPD.

Em especial, deve estar em condições de demonstrar que, nem o organismo de certificação, nem as pessoas que estão autorizadas a tomar decisões ou os trabalhadores que intervêm no procedimento de certificação, têm ligações pessoais com o requerente/cliente. O organismo de certificação deve também demonstrar que não tem comparticipação no requerente/cliente nem é por ele comparticipado, nem financiado; da mesma forma, não pode integrar empresas do mesmo grupo societário do requerente/cliente.

Cabe ainda ao organismo de certificação demonstrar que não existe uma relação económica entre ele e o requerente/cliente, em particular uma relação de subcontratação de tratamentos de dados pessoais.

O organismo de certificação deve demonstrar, de modo satisfatório para a CNPD, que as suas funções e obrigações não implicam um conflito de interesses, conforme requerido na alínea *e*) do n.º 2 do artigo 43.º do RGPD.

Para o efeito deve criar procedimentos que permitam detetar e analisar o risco de conflito de interesses decorrentes de atividades ou relações do próprio organismo de certificação e do seu pessoal, definindo regras claras que previnam os conflitos. Por exemplo, assegurando que sempre que um dos seus trabalhadores esteja também a prestar serviços ao requerente/cliente aquele o declare e, consequentemente, seja afastado do concreto procedimento de certificação.

Além disso, deve estabelecer regras claras sobre a gestão de situações de conflitos de interesse concretamente identificadas.

4.3 — Responsabilidade legal e financiamento

O IPAC deve assegurar, com regularidade, que o organismo de certificação adotou adequadas medidas de garantia das suas responsabilidades (v.g., seguro ou fundo de reserva) nas regiões geográficas em que exerce atividade.

4.4 — Condições não discriminatórias

Sem requisitos adicionais.

4.5 — Confidencialidade

Sem requisitos adicionais.

4.6 — Informação publicamente acessível

O organismo de certificação deve ter publicamente acessível:

a) Todas as versões dos critérios de certificação (tanto a vigente, como as anteriores) aprovados pela CNPD conforme o n.º 5 do artigo 42.º do RGPD, bem como todos os procedimentos de certificação, indicando o respetivo período de validade;

b) Informação sobre o procedimento de análise de reclamações e recursos, conforme alínea *d*) do n.º 2 do artigo 43.º do RGPD.

Caso o organismo de certificação disponibilize um sítio eletrónico, a informação que a ISO/IEC 17065 ou o presente regulamento requeiram que seja disponibilizada publicamente deverá ficar acessível no referido sítio, com uma exposição pelo menos igual à usada para publicitar ou listar os seus serviços.

5 — Requisitos estruturais

5.1 — Estrutura organizacional e gestão de topo

O organismo de certificação deve informar antecipadamente a CNPD e o IPAC caso pretenda iniciar ou desenvolver atividades a partir de uma filial, delegação ou outra representação legal instalada noutro país.

5.2 — Mecanismo para salvaguarda da imparcialidade

Sem requisitos adicionais.

6 — Requisitos dos recursos

6.1 — Pessoal do organismo de certificação

a) O organismo de certificação deve demonstrar que o seu pessoal:

i) Goza de independência e imparcialidade em relação à organização que está a ser avaliada, de acordo com as alíneas *a*) e *e*) do n.º 2 do artigo 43.º do RGPD;

ii) Respeita os critérios previstos no n.º 5 do artigo 42.º e na alínea *b*) do n.º 2 do artigo 43.º do RGPD;

iii) Demonstra especialização contínua (conhecimentos e experiência) na proteção de dados, em conformidade com o n.º 1 do artigo 43.º do RGPD, incluindo as seguintes competências mínimas:

(*a*) Conhecimentos adequados e relevantes e experiência na aplicação do regime jurídico de proteção de dados;

(*b*) Conhecimentos adequados e relevantes e experiência quanto a medidas técnicas e organizativas de proteção de dados, sempre que pertinente.

b) O organismo de certificação deve demonstrar que os responsáveis pela gestão dos processos de certificação (incluindo os que planificam auditorias e nomeiam equipas auditoras) têm:

i) Conhecimento adequado e relevante dos procedimentos e dos critérios de certificação em matéria de proteção de dados;

ii) Conhecimento dos procedimentos e dos métodos de avaliação em matéria de proteção de dados;

c) O organismo de certificação deve demonstrar que os responsáveis pelas decisões de certificação (i.e., quem analisa os relatórios de avaliação, avalia e decide sobre não conformidades e decide sobre a concessão, extensão, renovação, suspensão e retirada da certificação) têm as seguintes competências mínimas:

i) Quanto às pessoas com especialização técnica:

(*a*) Conhecimentos e perícia obtidos numa licenciatura em ciências da computação ou outra área científica equivalente (EQF nível 6) ([14]), ou um título reconhecido por ordem profissional em área relevante, ou experiência profissional significativa;

(*b*) Experiência profissional relevante na identificação e aplicação de medidas de proteção de dados técnicas e organizativas;

(*c*) Conhecimento da ISO/IEC 17065 e dos requisitos adicionais de acreditação;

ii) Quanto às pessoas com especialização jurídica:

(*a*) Conhecimentos obtidos numa licenciatura em direito (EQF nível 6) de pelo menos oito semestres, ou grau de mestre ou equivalente, ou experiência profissional significativa;

(*b*) Experiência profissional relevante quanto à legislação de proteção de dados;

(*c*) Conhecimento da ISO/IEC 17065 e dos requisitos adicionais de acreditação.

d) O organismo de certificação deve demonstrar que os responsáveis pelas avaliações têm as seguintes competências mínimas:

i) Quanto às pessoas com especialização técnica:

(*a*) Conhecimentos e perícia obtidos numa licenciatura em ciências da computação ou outra área científica equivalente (EQF nível 6), ou um título reconhecido por ordem profissional em área relevante, ou experiência profissional significativa;

(*b*) Experiência profissional de, pelo menos, 2 (dois) anos na vertente tecnológica de proteção de dados;

(*c*) Conhecimento da ISO/IEC 17065 e dos requisitos adicionais de acreditação;
(*d*) Conhecimento e experiência profissional relevante em procedimentos equivalentes (v.g., certificação e auditoria);

ii) Quanto às pessoas com especialização jurídica:

(*a*) Conhecimentos obtidos numa licenciatura em direito (EQF nível 6) de pelo menos oito semestres, ou grau de mestre ou equivalente, ou experiência profissional significativa;
(*b*) Experiência profissional relevante de, pelo menos, 2 (dois) anos quanto à legislação de proteção de dados;
(*c*) Conhecimento da ISO/IEC 17065 e dos requisitos adicionais de acreditação;
(*d*) Conhecimento e experiência profissional relevante em procedimentos equivalentes (v.g., certificação e auditoria).

e) O organismo de certificação deve definir procedimentos que assegurem e demonstrem que o seu pessoal atualiza periodicamente os seus conhecimentos sobre proteção de dados pessoais, tendo em conta, nomeadamente, as alterações legislativas, a evolução tecnológica e o seu impacto nos riscos para a proteção dos dados e da privacidade, assim como os seus conhecimentos quanto a competências técnicas e de auditoria, quando aplicável.

6.2 — Recursos para a avaliação
Sem requisitos adicionais.
7 — Requisitos procedimentais
7.1 — Generalidades
Nos procedimentos referidos nas alíneas *c*) e *d*) do n.º 2 do artigo 43.º do RGPD, o organismo de certificação deve cumprir os requisitos adicionais de acreditação, em especial de modo a assegurar que as suas atribuições e obrigações não implicam um conflito de interesses ([15]).
Na definição dos critérios de certificação, o organismo de certificação deve:

a) Ter em conta as diretrizes aprovadas pelo Comité Europeu para a Proteção de Dados ([16]);
b) Requerer a aprovação dos critérios de certificação pela CNPD antes de ser acreditado, e requerer nova aprovação pela CNPD sempre que altere, em termos substantivos, os referidos critérios.

No caso de o organismo de certificação pretender atuar noutros Estados-Membros, notificar e, se necessário, obter a aprovação das correspondentes autoridades competentes, incluindo para a utilização de um Selo Europeu de Proteção de Dados, em conformidade com o n.º 5 do artigo 42.º do RGPD.
O organismo de certificação deve também investigar o cliente quanto a violações do regime jurídico de proteção de dados sempre que o cliente lhe dê conhecimento de que está a ser objeto de um processo de averiguações, relacionado com o âmbito e com o objeto da certificação, pela CNPD ou se esta entidade o notificar de tal facto.
Deve ainda cooperar com a CNPD nas investigações em curso sobre os clientes que certificou; o organismo de certificação deve providenciar à CNPD um relatório de apreciação sobre a investigação que realizou, concluindo se o cliente ainda reúne as condições para estar certificado.
Mais, o organismo de certificação deve conservar a documentação da sua atividade (relativa às suas funções e obrigações), para a eventualidade de receber pedidos de informação ou para permitir o contacto no caso de uma reclamação relativa a uma certificação. Além disso, devem ser criados mecanismos procedimentais de comunicação entre o organismo de certificação e o cliente, que agilizem a tramitação e resposta a pedidos de informação sobre o procedimento em curso ou de outras informações pertinentes, e que permitam eventual apreciação pela CNPD das suas respostas e decisões.
7.2 — Candidatura
O organismo de certificação deve exigir que a candidatura à certificação identifique:

a) O âmbito de certificação pretendido, com a descrição completa do objeto de certificação, incluindo eventuais interfaces, comunicações para outros sistemas ou organizações, protocolos e outras disposições vinculativas relativas ao objeto de certificação;

b) A existência de subcontratação do tratamento dos dados e, quando o requerente seja subcontratante, as suas funções e obrigações, devendo em ambos os casos ser apresentada cópia do contrato de subcontratação;

c) A existência de responsabilidade conjunta, devendo, nesse caso, ser apresentada cópia do acordo entre os responsáveis conjuntos; e

d) Quaisquer averiguações ou investigações, relacionadas com o âmbito e o objeto da certificação, efetuadas pela CNPD ao requerente, atuais ou ocorridas desde 25 de maio de 2018.

O organismo de certificação deve notificar, por via eletrónica, a CNPD e o IPAC dos requerimentos admitidos, também para efeito da verificação de existência de averiguações em curso ou de eventuais decisões sancionatórias da CNPD; aquelas entidades públicas asseguram a confidencialidade dos procedimentos, podendo monitorizar as atividades do organismo de certificação.

7.3 — Análise da candidatura

No planeamento e execução da avaliação, o organismo de certificação deve incluir quer a vertente tecnológica, quer a vertente jurídica de proteção dos dados.

7.4 — Avaliação

a) O organismo de certificação deve estabelecer, de forma suficiente e abrangente, os métodos de avaliação a usar para determinar a conformidade do objeto de certificação com os critérios de certificação e o regime jurídico de proteção de dados. Em particular e sempre que aplicável, deve discriminar:

i) O(s) método(s) para avaliar a necessidade e proporcionalidade das operações de tratamento de dados em relação ao fim ou fins declarados e aos dados recolhidos, tendo ainda em conta o universo de titulares de dados;

ii) O(s) método(s) para equacionar a abrangência, a natureza e avaliação dos riscos identificados e considerados pelo responsável ou pelo subcontratante, relativamente às consequências legais previstas nos artigos 30.º, 32.º, 35.º e 36.º do RGPD, e as correspondentes medidas técnicas e organizativas adotadas nos termos dos artigos 24.º, 25.º e 32.º do RGPD, na medida em que tais artigos se apliquem ao objeto da certificação;

iii) O(s) método(s) para avaliar as medidas corretivas, incluindo garantias, salvaguardas e procedimentos para assegurar a proteção dos dados pessoais no contexto dos tratamentos de dados abrangidos pelo objeto da certificação, e para demonstrar que tais medidas estão em conformidade com o regime jurídico de proteção de dados e, especialmente, com as exigências constantes dos critérios de certificação;

iv) Os documentos comprovativos dos procedimentos e o modelo de documento para registo das verificações e avaliação do cumprimento dos critérios de certificação e do regime de proteção de dados pessoais.

b) O organismo de certificação deve utilizar métodos de avaliação padronizados e de aplicação geral para objetos de certificação similares ([17]). Qualquer desvio a este procedimento deve ser fundamentado pelo organismo de certificação.

c) O organismo de certificação deve periodicamente rever os seus métodos de avaliação, incluindo os correspondentes procedimentos, face a alterações do quadro legal ou jurídico, ao desenvolvimento de novas tecnologias, aos riscos relevantes, ao estado da arte e aos custos de execução de medidas técnicas e organizativas.

d) O organismo de certificação deve estabelecer as condições e procedimento para utilizar informação sobre eventual certificação anteriormente obtida de acordo com os artigos 42.º e 43.º do RGPD que o cliente pretenda ver reconhecida ou tida em conta. Note-se que o organismo de certificação deve ser obrigado a avaliar em detalhe essa certificação quanto ao cumprimento dos relevantes critérios de certificação. De todo o modo, tal depende da disponibilidade de um relatório de avaliação completo ou de informação sobre a avaliação da prévia atividade de certificação e dos respetivos resultados.

e) O organismo de certificação deve documentar em procedimento a metodologia de duração das avaliações (avaliador/dia), que deve ser proporcional ao universo e à natureza dos dados

pessoais incluídos no âmbito de certificação, ao universo dos titulares dos dados, ao contexto do tratamento, à complexidade das tecnologias usadas na recolha e subsequente tratamento dos mesmos, e ao recurso a subcontratação pelo cliente.

f) O organismo de certificação pode levar a cabo as suas tarefas de avaliação através de pessoal próprio ou de peritos externos contratados para o efeito, sem prejuízo da utilização da contratação da prestação de serviços tal como definida na ISO/IEC 17065. Em qualquer caso, o organismo de certificação é o responsável pela decisão tomada.

g) Os relatórios das avaliações devem identificar os documentos e registos examinados, processos avaliados, funções desempenhadas pelas pessoas entrevistadas, bem como quaisquer não conformidades em relação aos critérios de certificação, identificando claramente o requisito incumprido e a gravidade do incumprimento.

h) Após a emissão da certificação, no contexto do acompanhamento pelo organismo de certificação, eventuais não conformidades detetadas devem ser corrigidas pelo cliente num prazo proporcional à gravidade da mesma. Para o efeito, o organismo de certificação deve tipificar as não conformidades em função da sua gravidade — nos casos de menor gravidade, o prazo pode atingir um mês, decorrido o qual, na ausência de correção, deve ser iniciado o processo de suspensão da certificação. Nos casos mais graves, além da correção, o organismo de certificação deve requerer ao cliente uma análise das causas da não conformidade, para que (*i*) implemente ações corretivas eficazes que previnam a sua recorrência, e (*ii*) possa determinar se existem outras falhas relacionadas ou similares à detetada e que também devam ser corrigidas.

i) Sempre que a CNPD o solicite, o organismo de certificação garante o acesso a toda a documentação relativa à avaliação.

7.5 — Revisão

Nos termos dos n.os 2 e 3 do artigo 43.º do RGPD, devem ser estabelecidos procedimentos para a emissão, revisão periódica e retirada de certificação. Nos procedimentos de certificação, inclusive os referentes à revisão periódica e retirada da certificação, a fundamentação da decisão deve estar claramente identificada e documentada, com factos e provas objetivos, independentemente de quem a faça.

7.6 — Decisão de certificação

O organismo de certificação deve especificamente definir de que modo é assegurada a sua independência e responsabilidade relativamente às decisões individuais de certificação.

Para garantia da transparência, deve também ter procedimentos implementados para notificar a CNPD previamente a uma tomada de decisão de certificação, de renovação ou de extensão da mesma. A notificação integra um resumo das atividades realizadas para chegar à decisão, incluindo a cópia do relatório de auditoria, do processo de revisão, bem como a fundamentação da decisão, segundo modelo a estabelecer pela CNPD. No caso da concessão, extensão e renovação, deve submeter conjuntamente o projeto de certificado de conformidade ou documentação que o substitua.

O organismo de certificação deve ainda confirmar de novo, imediatamente antes da decisão, se o cliente não é alvo de averiguações pela CNPD que possam pôr em causa a certificação pretendida.

7.7 — Documentação de certificação

De acordo com o n.º 7 do artigo 42.º do RGPD, a certificação não pode ter validade superior a 3 (três) anos.

Deve ficar documentado o período de acompanhamento a que se reporta o ponto 7.9. do presente regulamento.

A descrição do âmbito de certificação tem de incluir a identificação do objeto da certificação, a entidade abrangida pela certificação, bem como a identificação e versão dos critérios de certificação aplicados.

O organismo de certificação deve enviar à CNPD uma cópia das marcas ou selos usados.

7.8 — Diretório de produtos certificados

O organismo de certificação deve tornar publicamente acessível a informação relativa aos produtos, processos e serviços certificados. Caso o organismo de certificação tenha um sítio na Internet, deve aí disponibilizar o diretório relativo às certificações emitidas.

Em especial, deve publicitar um sumário executivo do qual conste o âmbito e o objeto da certificação, o seu período de validade, condições a que está sujeita a certificação, bem como uma síntese dos critérios de certificação aplicados, dos métodos de avaliação adotados e dos resultados obtidos.

Deve ainda informar, por via eletrónica, a CNPD sobre os fundamentos da concessão da certificação, bem como da sua retirada ([18]).

7.9 — Acompanhamento

O organismo de certificação deve estabelecer de forma proporcional e não discriminatória os mecanismos de avaliação periódica durante o período de validade da certificação ([19]).

O organismo de certificação deve estabelecer as condições e o procedimento para utilizar informação sobre eventual certificação anteriormente obtida de acordo com os artigos 42.º e 43.º do RGPD que o cliente pretenda ver reconhecida ou tida em conta.

As atividades de acompanhamento devem ter uma periodicidade anual, não podendo a primeira atividade exceder 12 meses após a data da avaliação realizada para efeito da concessão da certificação, sem prejuízo da sua realização num período de tempo mais curto sempre que o resultado de uma análise de risco o justifique.

7.10 — Alterações que afetam a certificação

As alterações que afetam a certificação, a ser consideradas pelo organismo de certificação, incluem:

a) Notificações de violações de dados pessoais relacionadas com o âmbito e o objeto da certificação ou incumprimento, declarado pela CNPD ou pelos Tribunais, do RGPD ou dos requisitos adicionais;

b) Alterações legislativas em matéria de proteção de dados;

c) Adoção de atos delegados ou de execução pela Comissão Europeia em matéria de proteção de dados ([20]);

d) Documentos relevantes adotados pelo Comité Europeu para a Proteção de Dados;

e) Decisões judiciais em matéria de proteção de dados;

f) Alterações no estado da arte.

Para o efeito, deve prever procedimentos de alteração que incluam períodos de transição, apresentação de requerimento de aprovação junto da CNPD, reavaliação do objeto da certificação e eventuais medidas de retirada de certificação.

7.11 — Anulação, redução, suspensão ou retirada da certificação

Em caso de anulação, redução, suspensão ou retirada da certificação, o organismo de certificação deve notificar ao cliente a decisão e respetivos fundamentos, bem como informar imediatamente a CNPD, incluindo a fundamentação de tal decisão, sem prejuízo da sua comunicação ao IPAC.

O organismo de certificação deve estabelecer sanções proporcionais em caso de omissão, ocultação ou atraso na comunicação, por parte do cliente, de informação relativa a processo de averiguações em curso ou a incumprimento do regime jurídico de proteção de dados.

Se a CNPD entender que os critérios de certificação não são ou já não estão a ser cumpridos, pode ordenar ao organismo de certificação, nos termos da alínea *h*) do n.º 2 do artigo 58.º do RGPD, que não emita ou que retire uma certificação, o qual fica constituído no dever do seu imediato cumprimento.

7.12 — Registos

O organismo de certificação tem de conservar a documentação completa, compreensível, atualizada e auditável.

7.13 — Reclamações e recursos

O organismo de certificação deve estabelecer e disponibilizar os procedimentos de reclamação e recurso, em especial, regras sobre legitimidade, instrução e consulta pelos interessados, bem como tempos de resposta adequados e proporcionais à gravidade e âmbito das reclamações e recursos, assegurando a independência na análise dos mesmos. Deve ainda definir os processos a adotar depois de emitida a decisão sobre a reclamação ou o recurso, designadamente, transmitindo à CNPD as reclamações e recursos pertinentes.

Além disso, o organismo de certificação deve estabelecer regras que garantam a efetiva separação entre as atividades de certificação e a tramitação das reclamações e recursos.

8 — Sistema de gestão

Sempre que no presente regulamento se preveem ou referem obrigações do organismo de certificação, o procedimento e a metodologia adotados para o seu cumprimento têm de ser documentados no respetivo sistema de gestão, de modo a permitir a prossecução eficaz e eficiente dos objetivos visados, bem como a transparência e auditabilidade da aplicação e cumprimento dos requisitos adicionais.

O organismo de certificação deve ainda disponibilizar à CNPD os princípios de gestão e a sua aplicação documentada, durante e após o procedimento de acreditação, sempre que esta entidade o solicite, em qualquer momento, durante uma investigação no âmbito dos poderes conferidos pelo artigo 58.º do RGPD.

([1]) Regulamento Geral sobre a Proteção de Dados, aprovado pelo 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.

([2]) Que assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

([3]) O protocolo entre a CNPD e o IPAC, IP, está disponível nos sítios da Internet de ambas as entidades.

([4]) Diretrizes 4/2018 do Comité Europeu para a Proteção de Dados, relativas à acreditação dos organismos de certificação nos termos do artigo 43.º do Regulamento Geral sobre a Proteção de Dados (2016/679), versão 3.0, de 4 de junho de 2019, acessíveis em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_pt.pdf e Diretrizes 1/2018 do Comité Europeu para a Proteção de Dados, relativas à certificação e à definição dos critérios de certificação em conformidade com os artigos 42.º e 42.º do RGPD, versão 3.0, de 4 de junho de 2019, acessíveis em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf

([5]) Diretrizes 4/2018 do Comité Europeu para a Proteção de Dados., relativas à acreditação dos organismos de certificação nos termos do artigo 43.º do Regulamento Geral sobre a Proteção de Dados (2016/679), versão 3.0, de 4 de junho de 2019, acessíveis em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_pt.pdf e Diretrizes 1/2018 do Comité Europeu para a Proteção de Dados, relativas à certificação e à definição dos critérios de certificação em conformidade com os artigos 42.º e 42.º do RGPD, versão 3.0, de 4 de junho de 2019, acessíveis em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf

([6]) Na ISO/IEC 17065, é usado indistintamente o termo "cliente", independentemente de a certificação ter ou não sido emitida. Atendendo ao ponto 3 do presente Regulamento, o termo "requerente" é usado no seu sentido literal sempre que a certificação ainda não foi emitida e o termo "cliente" quando a organização já detém a certificação.

([7]) Em conformidade com a alínea *b*) do n.º 2 do artigo 43.º e o n.º 5 do artigo 42.º do RGPD.

([8]) De modo a garantir a aplicação do disposto no n.º 7 do artigo 42.º e na alínea *c*) do n.º 1 do artigo 58.º do RGPD.

([9]) Em conformidade com o n.º 6 do artigo 62.º do RGPD.

([10]) Nos termos do n.º 5 do artigo 43.º e do n.º 8 do artigo 42.º do RGPD.

([11]) Nos termos do n.º 5 do artigo 43.º e do n.º 8 do artigo 42.º do RGPD.

([12]) Nos termos do n.º 5 do artigo 43.º e do n.º 8 do artigo 42.º do RGPD.

([13]) Diretrizes 1/2018 do Comité Europeu para a Proteção de Dados, relativas à certificação e à definição dos critérios de certificação em conformidade com os artigos 42.º e 42.º do RGPD, versão 3.0, de 4 de junho de 2019, acessíveis em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf

([14]) Cf. https://ec.europa.eu/ploteus/en/compare?

([15]) Nos termos exigidos pelas alíneas *b*) e *e*) do n.º 2 do artigo 43.º do RGPD.

([16]) Diretrizes 1/2018 do Comité Europeu para a Proteção de Dados, relativas à certificação e à definição dos critérios de certificação em conformidade com os artigos 42.º e 42.º do RGPD, versão 3.0, de 4 de junho de 2019, acessíveis em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201801_v3.0_certificationcriteria_annex2_pt.pdf

([17]) Diretrizes 4/2018 do Comité Europeu para a Proteção de Dados., relativas à acreditação dos organismos de certificação nos termos do artigo 43.º do Regulamento Geral sobre a Proteção de Dados (2016/679), versão 3.0, de 4 de junho de 2019, acessíveis em https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201804_v3.0_accreditationcertificationbodies_annex1_pt.pdf

([18]) De acordo com o n.º 5 do artigo 43.º do RGPD.

([19]) Em conformidade com o disposto na alínea *c*) do n.º 2 do artigo 43.º do RGPD.

([20]) Nos termos dos n.ºs 8 e 9 do artigo 43.º do RGPD.

14 de abril de 2021. — A Presidente da Comissão Nacional de Proteção de Dados, *Filipa Calvão.*

314525693