2025/37

15.1.2025

REGULAMENTO (UE) 2025/37 DO PARLAMENTO EUROPEU E DO CONSELHO

de 19 de dezembro de 2024

que altera o Regulamento (UE) 2019/881 no que diz respeito aos serviços de segurança geridos

(Texto relevante para efeitos do EEE)

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Comité Económico e Social Europeu ([1]),

Após consulta ao Comité das Regiões,

Deliberando de acordo com o processo legislativo ordinário ([2]),

Considerando o seguinte:

(1) O Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho ([3]) estabelece um enquadramento para a criação de sistemas europeus de certificação da cibersegurança com o objetivo de assegurar um nível adequado de cibersegurança para os produtos, os serviços e os processos de tecnologias da informação e comunicação (TIC) na União e de evitar a fragmentação do mercado interno no que toca aos sistemas de certificação da cibersegurança na União.

(2) A fim de assegurar a resiliência da União aos ciberataques e evitar quaisquer vulnerabilidades no mercado interno, o presente regulamento visa complementar o quadro regulamentar horizontal que estabelece requisitos abrangentes em matéria de cibersegurança para os produtos com elementos digitais, nos termos do Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho ([4]), prevendo objetivos de segurança para os serviços de segurança geridos, bem como a aplicação e a fiabilidade desses serviços.

(3) Os serviços de segurança geridos são prestados por prestadores de serviços de segurança geridos, na aceção do artigo 6.º, ponto 40, da Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho ([5]). Por conseguinte, a definição de serviços de segurança geridos no presente regulamento deverá ser coerente com a de prestadores de serviços de segurança geridos na Diretiva (UE) 2022/2555. Esses serviços consistem na realização ou na prestação de assistência para atividades relacionadas com a gestão dos riscos de cibersegurança dos clientes e têm vindo a adquirir uma importância cada vez maior na prevenção e mitigação de incidentes. Por conseguinte, os prestadores desses serviços são considerados entidades essenciais ou importantes pertencentes a um setor de importância crítica nos termos da Diretiva (UE) 2022/2555. Como resulta do considerando 86 da referida diretiva, os prestadores de serviços de segurança geridos em domínios como a resposta a incidentes, os testes de intrusão, as auditorias de segurança e a consultoria desempenham um papel especialmente importante em termos de apoio aos esforços desenvolvidos pelas entidades para evitar e detetar os incidentes, bem como para lhes dar resposta ou recuperar dos mesmos. Porém, os próprios prestadores de serviços de segurança geridos têm sido igualmente alvo de ciberataques e, em virtude da sua estreita integração nas operações dos seus clientes, implicam especial risco. É, por conseguinte, importante que as entidades essenciais e importantes, na aceção da Diretiva (UE) 2022/2555, exerçam diligência acrescida ao selecionarem prestadores de serviços de segurança geridos.

([1]) JO C 349 de 29.9.2023, p. 167.

([2]) Posição do Parlamento Europeu de 24 de abril de 2024 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 2 de dezembro de 2024.

([3]) Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 15).

([4]) Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro de 2024, relativo aos requisitos horizontais de cibersegurança dos produtos com elementos digitais e que altera os Regulamentos (UE) n.º 168/2013 e (UE) 2019/1020 e a Diretiva (UE) 2020/1828 (Regulamento de Ciber-Resiliência) (JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([5]) Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333 de 27.12.2022, p. 80).

(4) A definição de serviços de segurança geridos ao abrigo do presente regulamento inclui uma lista não exaustiva de serviços de segurança geridos que podem ser elegíveis para sistemas europeus de certificação de cibersegurança, nomeadamente o tratamento de incidentes, os testes de intrusão, as auditorias de segurança, e a consultoria relacionados com apoio técnico. Os serviços de segurança geridos podem abranger serviços de cibersegurança que apoiem a preparação, prevenção, deteção, análise e mitigação, resposta e recuperação de incidentes. A prestação de informações sobre ciberameaças e a avaliação dos riscos relacionados com o apoio técnico poderão igualmente ser consideradas serviços de segurança geridos. Poderão existir sistemas europeus de certificação da cibersegurança para diferentes serviços de segurança geridos. Os certificados europeus de cibersegurança emitidos em conformidade com esses sistemas deverão referir-se a serviços de segurança geridos específicos de um determinado prestador desses serviços.

(5) Os prestadores de serviços de segurança geridos podem também desempenhar um papel importante no que diz respeito às ações de apoio à resposta e recuperação inicial em caso de incidentes de cibersegurança significativos e de incidentes de cibersegurança em grande escala, com base em serviços de prestadores privados de confiança e na análise de entidades críticas para detetar potenciais vulnerabilidades com base em avaliações coordenadas a nível da União dos riscos de segurança. A certificação de serviços de segurança geridos poderá desempenhar um papel na seleção de prestadores de serviços de segurança geridos de confiança na aceção do Regulamento (UE) 2025/38 do Parlamento Europeu e do Conselho ([6]).

(6) A certificação dos serviços de segurança geridos não só é relevante no âmbito do processo de seleção para a Reserva de Cibersegurança da UE criada pelo Regulamento (UE) 2025/38, como também constitui um indicador de qualidade essencial para as entidades públicas e privadas que pretendam adquirir esses serviços. Tendo em conta a importância crítica dos serviços de segurança geridos e a sensibilidade dos dados tratados, a certificação pode fornecer aos potenciais clientes orientações e garantias essenciais sobre a fiabilidade desses serviços. Os sistemas europeus de certificação de cibersegurança dos serviços de segurança geridos que visam contribuir para evitar a fragmentação do mercado interno. Por conseguinte, o presente regulamento visa melhorar o funcionamento do mercado interno.

(7) Os sistemas europeus de certificação de cibersegurança para serviços de segurança geridos deverão conduzir à adoção desses serviços e a uma maior concorrência entre os prestadores de serviços de segurança geridos. Sem prejuízo do objetivo de assegurar níveis suficientes e adequados de conhecimentos técnicos relevantes e a integridade profissional desses prestadores, tais sistemas de certificação deverão, por conseguinte, facilitar a entrada no mercado e a oferta de serviços de segurança geridos, simplificando, na medida do possível, os potenciais encargos regulamentares, administrativos e financeiros que os prestadores, em especial as pequenas e médias empresas (PME), incluindo microempresas, poderão enfrentar ao oferecerem serviços de segurança geridos. Ademais, a fim de incentivar a utilização de serviços de segurança geridos, bem como estimular a procura dos mesmos, os sistemas europeus de certificação da cibersegurança deverão contribuir para a sua acessibilidade, em particular para os intervenientes de menor dimensão, como as PME, incluindo microempresas, bem como para as autoridades locais e regionais com capacidades e recursos limitados, mas que são mais propensos a falhas de cibersegurança com implicações financeiras, jurídicas, de reputação e operacionais.

(8) É importante prestar apoio às PME, incluindo microempresas, na aplicação do presente regulamento e no recrutamento das competências e conhecimentos especializados em cibersegurança, necessários para prestar aos serviços de segurança geridos de acordo com os requisitos estabelecidos no presente regulamento. O Programa Europa Digital, criado pelo Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho ([7]), e outros programas pertinentes da União preveem que a Comissão crie um apoio financeiro e técnico que permita a essas empresas contribuir para o crescimento da economia da União e reforçar o nível comum de cibersegurança da União, nomeadamente racionalizando o apoio financeiro do Programa Europa Digital e de outros programas pertinentes da União e apoiando as PME, incluindo microempresas.

(9) Os sistemas europeus de certificação da cibersegurança para serviços de segurança geridos deverá contribuir para a disponibilidade de serviços seguros e de elevada qualidade, que garantam uma transição digital segura, e para a consecução dos objetivos definidos no programa Década Digital para 2030 criado pela Decisão (UE) 2022/2481 do Parlamento Europeu e do Conselho ([8]), em particular no que diz respeito ao objetivo de conseguir que 75 % das empresas da União comecem a utilizar serviços de computação em nuvem, os megadados ou a inteligência artificial,

([6]) Regulamento (UE) 2025/38 do Parlamento Europeu e do Conselho, de 19 de dezembro de 2024, que cria medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ciberameaças e ciberincidentes e que altera o Regulamento (UE) 2021/694 (Regulamento de Cibersolidariedade) (JO L, 2025/38, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Regulamento (UE) 2021/694 do Parlamento Europeu e do Conselho, de 29 de abril de 2021, que cria o Programa Europa Digital e revoga a Decisão (UE) 2015/2240 (JO L 166 de 11.5.2021, p. 1).

([8]) Decisão (UE) 2022/2481 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, que estabelece o programa Década Digital para 2030 (JO L 323 de 19.12.2022, p. 4).

que mais de 90 % das PME, incluindo microempresas, atinjam, pelo menos, um nível básico de intensidade digital e que os serviços públicos essenciais sejam acessíveis em linha.

(10) Para além da implantação de produtos, serviços ou processos de TIC, os serviços de segurança geridos proporcionam frequentemente prestações adicionais que dependem das competências, dos conhecimentos especializados e da experiência do pessoal dos prestadores desses serviços. De modo a garantir que os serviços de segurança geridos prestados possuem um nível de qualidade muito elevada, importa que, entre os objetivos de segurança, estejam competências, conhecimentos especializados e experiência de nível elevado, bem como procedimentos internos adequados. A fim de assegurar que os sistemas europeus de certificação da cibersegurança dedicados possam abranger todos os aspetos dos serviços de segurança geridos, é, por conseguinte, necessário alterar o Regulamento (UE) 2019/881. Os resultados e recomendações da avaliação e revisão previstas no Regulamento (UE) 2019/881 deverão ser tidos em conta.

(11) A fim de facilitar o crescimento de um mercado interno fiável, criando simultaneamente parcerias com países terceiros que partilhem as mesmas ideias, o processo de certificação definido no enquadramento europeu para a certificação de cibersegurança previsto no Regulamento (UE) 2019/881 deverá ser deverá ser aplicado de uma forma que assegure o reconhecimento internacional e o alinhamento pelas normas internacionais.

(12) A União enfrenta um défice de talentos, caracterizado por uma escassez de profissionais qualificados e pela evolução rápida das ameaças, tal como reconhecido na Comunicação da Comissão de 18 de abril de 2023 intitulada «Colmatar o défice de talentos no domínio da cibersegurança para reforçar a competitividade, o crescimento e a resiliência da UE ("Academia de Competências de Cibersegurança")». Os recursos pedagógicos e a formação de natureza formal diferem e os conhecimentos podem ser adquiridos de diversos modos: formalmente, por exemplo, através de universidades ou cursos, ou informalmente, por exemplo, através da formação em contexto de trabalho ou da experiência profissional no domínio em causa. Por conseguinte, a fim de facilitar a emergência de serviços de segurança geridos de elevada qualidade, bem como de obter uma melhor visão geral da composição da mão de obra da União no domínio da cibersegurança, importa reforçar a cooperação entre os Estados-Membros, a Comissão, a Agência da União Europeia para a Cibersegurança (ENISA), criada pelo Regulamento (UE) 2019/881, e as partes interessadas, incluindo do setor privado e do meio académico, através do desenvolvimento de parcerias público-privadas, do apoio a iniciativas de investigação e inovação, do desenvolvimento e do reconhecimento mútuo de normas comuns e da certificação de competências em matéria de cibersegurança, incluindo através do Quadro Europeu de Competências em Cibersegurança. Tal cooperação facilitaria igualmente a mobilidade de profissionais da cibersegurança na União, bem como a integração de conhecimentos e da formação em matéria de cibersegurança nos programas de ensino, assegurando simultaneamente o acesso a programas de aprendizagem e a estágios para os jovens, em particular para pessoas que vivem em regiões desfavorecidas, como as ilhas e as regiões escassamente povoadas, rurais e remotas. É importante que essa cooperação vise atrair mais mulheres e raparigas para este domínio e contribua para colmatar as disparidades entre homens e mulheres nos domínios da ciência, tecnologia, engenharia e matemática, e que o setor privado vise ministrar ações de formação no local de trabalho que abordem as competências mais procuradas, envolvendo a administração pública e as empresas em fase de arranque, bem como as PME, incluindo microempresas. É igualmente importante que os prestadores e os Estados-Membros colaborem e contribuam para a recolha de dados sobre a situação e a evolução do mercado de trabalho da cibersegurança.

(13) A ENISA desempenha um papel importante na preparação de projetos de sistemas europeus de certificação da cibersegurança. A Comissão deverá avaliar os recursos orçamentais necessários para o quadro de pessoal da ENISA, pelo procedimento previsto no artigo 29.º do Regulamento (UE) 2019/881, aquando da elaboração do projeto de orçamento geral da União.

(14) O presente regulamento prevê alterações específicas ao Regulamento (UE) 2019/881 para permitir a criação de sistemas europeus de certificação da cibersegurança para os serviços de segurança geridos. Ao fazê-lo, especifica e clarifica determinadas disposições desse regulamento relativas à preparação e ao funcionamento de todos os sistemas europeus de certificação da cibersegurança, com vista a assegurar a sua transparência e abertura. As alterações mais recentes, que se limitam à especificação ou clarificação do Regulamento (UE) 2019/881, em especial as alterações relativas às informações que a ENISA deve prestar aquando da transmissão de uma proposta de sistema, aos grupos de trabalho ad hoc criados para cada projeto de sistema e à informação e consulta sobre os sistemas europeus de certificação da cibersegurança, não deverão prejudicar de forma alguma a avaliação e revisão mais amplas desse regulamento, exigidas nos termos do artigo 67.º do mesmo, incluindo a avaliação do impacto, da eficácia e da eficiência do título desse regulamento relativo ao enquadramento para a certificação da cibersegurança. A avaliação e revisão do referido título deverá basear-se numa ampla consulta das partes interessadas e numa análise completa e exaustiva dos procedimentos envolvidos.

(15) Atendendo a que o objetivo do presente regulamento, a saber, permitir a criação de sistemas europeus de certificação da cibersegurança dos serviços de segurança geridos, não pode ser suficientemente alcançado pelos Estados-Membros, mas pode, devido à sua dimensão e aos seus efeitos, ser mais bem alcançado ao nível da União, a União pode tomar medidas, em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para alcançar esse objetivo.

(16) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([9]) e emitiu parecer em 10 de janeiro de 2024,

ADOTARAM O PRESENTE REGULAMENTO:

Artigo 1.º

Alteração do Regulamento (UE) 2019/881

O Regulamento (UE) 2019/881 é alterado do seguinte modo:

1) No artigo 1.º, n.º 1, primeiro parágrafo, a alínea b) passa a ter a seguinte redação:

«b) Um enquadramento para a criação de sistemas europeus de certificação da cibersegurança com o objetivo de assegurar um nível adequado de cibersegurança para os produtos, serviços e processos de TIC e os serviços de segurança geridos na União e de evitar a fragmentação do mercado interno no que toca aos sistemas de certificação da cibersegurança na União.»;

2) O artigo 2.º é alterado do seguinte modo:

a) Os pontos 9, 10 e 11 passam a ter a seguinte redação:

«9) "Sistema europeu de certificação da cibersegurança", o conjunto abrangente, de regras, requisitos técnicos, normas e procedimentos estabelecidos a nível da União e aplicáveis à certificação ou à avaliação da conformidade dos produtos, serviços e processos de TIC ou dos serviços de segurança geridos;

10) "Sistema nacional de certificação da cibersegurança", o conjunto abrangente de regras, requisitos técnicos, normas e procedimentos estabelecidos e adotados por uma autoridade pública nacional e aplicáveis à certificação ou à avaliação da conformidade de produtos, serviços ou processos de TIC e de serviços de segurança geridos abrangidos pelo âmbito de aplicação desse sistema específico;

11) "Certificado europeu de cibersegurança", um documento emitido por um organismo competente, que ateste que determinado produto, serviço ou processo de TIC ou determinado serviço de segurança gerido foi avaliado para verificar a sua conformidade com os requisitos de segurança específicos estabelecidos por um sistema europeu de certificação da cibersegurança;»;

b) É inserido o seguinte ponto:

«14-A) "Serviço de segurança gerido", um serviço prestado a um terceiro que consiste na realização ou na prestação de assistência para atividades relacionadas com a gestão dos riscos de cibersegurança, como o tratamento de incidentes, os testes de intrusão, as auditorias de segurança e a consultoria, incluindo aconselhamento especializado, relacionados com apoio técnico;»;

c) Os pontos 20, 21 e 22 passam a ter a seguinte redação:

«20) "Especificação técnica", um documento que define os requisitos técnicos a cumprir pelos produtos, serviços ou processos de TIC ou pelos serviços de segurança geridos, ou os procedimentos de avaliação da conformidade relativos aos mesmos;

([9]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

21) "Nível de garantia", a base da confiança de que um produto, serviço ou processo de TIC ou um serviço de segurança gerido cumpre os requisitos de segurança de um determinado sistema europeu de certificação da cibersegurança, que indica a que nível esse produto, serviço ou processo de TIC ou serviço de segurança gerido foi avaliado, mas não mede, por si só, a segurança dos produtos, serviços ou processos de TIC ou serviços de segurança geridos em si mesmos;

22) "Autoavaliação da conformidade", uma ação realizada por um fabricante de produtos de TIC, o prestador de serviços de TIC, o fornecedor de processos de TIC ou o prestador de serviços de segurança geridos para avaliar se esses produtos, serviços ou processos de TIC ou serviços de segurança geridos cumprem os requisitos de um sistema europeu de certificação da cibersegurança;»;

3) No artigo 4.º, o n.º 6 passa a ter a seguinte redação:

«6. A ENISA promove o recurso a uma certificação europeia da cibersegurança, com vista a evitar a fragmentação do mercado interno. A ENISA contribui para a criação e a manutenção de um enquadramento europeu para a certificação da cibersegurança, nos termos do título III do presente regulamento, a fim de aumentar a transparência no que respeita à cibersegurança dos produtos, serviços e processos de TIC e dos serviços de segurança geridos, reforçando, assim, a confiança no mercado interno digital e a sua competitividade.»;

4) O artigo 8.º é alterado do seguinte modo:

a) O n.º 1 é alterado do seguinte modo:

i) o proémio passa a ter a seguinte redação:

«1. A ENISA apoia e promove a elaboração e a execução da política da União em matéria de certificação da cibersegurança dos produtos, serviços e processos de TIC e dos serviços de segurança geridos, tal como estabelecido no título III do presente regulamento:»,

i) a alínea b) passa a ter a seguinte redação:

«b) Elaborando projetos de sistemas europeus de certificação da cibersegurança (projetos de sistemas) dos produtos, serviços e processos de TIC e dos serviços de segurança geridos, nos termos do artigo 49.º;»,

b) O n.º 3 passa a ter a seguinte redação:

«3. A ENISA compila e publica orientações e desenvolve boas práticas em matéria de requisitos de cibersegurança dos produtos, serviços e processos de TIC e dos serviços de segurança geridos, em cooperação com as autoridades nacionais de certificação da cibersegurança e a indústria, de modo formal, estruturado e transparente.»;

c) O n.º 5 passa a ter a seguinte redação:

«5. A ENISA facilita a elaboração e a adoção de normas europeias e internacionais em matéria de gestão dos riscos e de segurança dos produtos, serviços e processos de TIC e dos serviços de segurança geridos.»;

5) O artigo 46.º passa a ter a seguinte redação:

«*Artigo 46.º*

Enquadramento europeu para a certificação da cibersegurança

1. É criado o enquadramento europeu para a certificação da cibersegurança a fim de melhorar as condições de funcionamento do mercado interno elevando o nível de cibersegurança na União e permitindo a adoção de uma abordagem harmonizada a nível da União relativamente aos sistemas europeus de certificação da cibersegurança, tendo em vista criar um mercado único digital de produtos, serviços e processos de TIC e de serviços de segurança geridos.

2. O enquadramento europeu para a certificação da cibersegurança prevê um mecanismo destinado a criar sistemas europeus de certificação da cibersegurança e a atestar que os produtos, serviços e processos de TIC que tenham sido avaliados de acordo com esses sistemas cumprem os requisitos de segurança especificados, para efeitos da proteção da disponibilidade, autenticidade, integridade ou confidencialidade dos dados armazenados, transmitidos ou tratados, ou as funções ou serviços oferecidos por esses produtos, serviços e processos ou acessíveis por seu intermédio ao longo do

respetivo ciclo de vida. Além disso, atesta que os serviços de segurança geridos que tenham sido avaliados de acordo com esses sistemas cumprem os requisitos de segurança especificados, para efeitos da proteção da disponibilidade, autenticidade, integridade e confidencialidade dos dados consultados, tratados, armazenados ou transmitidos no âmbito da prestação desses serviços, e que esses serviços são continuamente prestados, com a competência, os conhecimentos especializados e a experiência necessários, por pessoal com um nível suficiente e adequado de conhecimentos técnicos pertinentes e integridade profissional.»;

6) O artigo 47.º é alterado do seguinte modo:

a) O n.º 2 passa a ter a seguinte redação:

«2. O programa de trabalho evolutivo da União compreende, designadamente, uma lista dos produtos, serviços e processos de TIC, e dos serviços de segurança geridos, ou das respetivas categorias, que podem beneficiar da inclusão no âmbito de aplicação de um sistema europeu de certificação da cibersegurança.»;

b) O n.º 3 passa a ter a seguinte redação:

i) o proémio passa a ter a seguinte redação:

«3. A inclusão no programa de trabalho evolutivo da União de um determinado produto, serviço ou processo de TIC, ou serviços de segurança geridos, ou das respetivas categorias, deve ser justificada com base num ou mais dos seguintes fundamentos:»,

ii) a alínea a) passa a ter a seguinte redação:

«a) A disponibilidade e o desenvolvimento de sistemas nacionais de certificação da cibersegurança que abranjam uma categoria específica de produtos, serviços e processos de TIC, ou serviços de segurança geridos, em especial no que toca ao risco de fragmentação;»,

iii) é inserida a seguinte alínea:

«c-A) A evolução tecnológica, bem como a disponibilidade e o desenvolvimento de sistemas internacionais de certificação da cibersegurança e de normas internacionais utilizadas pela indústria;»;

7) O artigo 49.º é alterado do seguinte modo:

a) Os n.ºs 1 a 4 passam a ter a seguinte redação:

«1. Na sequência de um pedido da Comissão nos termos do artigo 48.º, a ENISA elabora um projeto de sistema que cumpra os requisitos aplicáveis, estabelecidos nos artigos 51.º, 51.º-A, 52.º e 54.º.

2. Na sequência de um pedido do GECC nos termos do artigo 48.º, n.º 2, a ENISA pode elaborar um projeto de sistema que cumpra os requisitos aplicáveis, estabelecidos nos artigos 51.º, 51.º-A, 52.º e 54.º. Caso a ENISA recuse esse pedido, deve justificar a sua recusa. Todas as decisões de recusa de tais pedidos são tomadas pelo conselho de administração.

3. Durante a elaboração dos projetos de sistema, a ENISA consulta todas as partes interessadas em tempo útil através de um processo de consulta formal, aberto, transparente e inclusivo. Ao transmitir o projeto de sistema à Comissão, nos termos do n.º 6, a ENISA presta informações sobre a forma como cumpriu com o presente número.

4. Para cada projeto de sistema, a ENISA cria um grupo **ad hoc**, nos termos do artigo 20.º, n.º 4, para prestar aconselhamento específico e disponibilizar conhecimentos especializados à ENISA. Esses grupos de trabalho ad hoc incluem, conforme adequado e sem prejuízo dos procedimentos e poderes discricionários previstos no artigo 20.º, n.º 4, peritos das administrações públicas dos Estados-Membros, das instituições, órgãos e organismos da União e do setor privado.»;

b) O n.º 7 passa a ter a seguinte redação:

«7. A Comissão pode, com base no projeto de sistema apresentado pela ENISA, adotar atos de execução que estabeleçam um sistema europeu de certificação da cibersegurança de produtos, serviços e processos de TIC e de serviços de segurança geridos que cumpram os requisitos pertinentes estabelecidos nos artigos 51.º, 51.º-A, 52.º e 54.º. Os referidos atos de execução são adotados pelo procedimento de exame a que se refere o artigo 66.º, n.º 2.»;

8) É inserido o seguinte artigo:

«*Artigo 49.º-A*

Informações e consulta sobre sistemas europeus de certificação da cibersegurança

1. A Comissão disponibiliza ao público as informações sobre o seu pedido à ENISA para a elaboração de um projeto de sistema ou a revisão de um sistema europeu de certificação da cibersegurança existente, a que se refere o artigo 48.º.

2. Durante a elaboração de um projeto de sistema pela ENISA nos termos do artigo 49.º, o Parlamento Europeu e o Conselho, ou ambos, podem solicitar à Comissão, na sua qualidade de presidente GECC, e à ENISA que apresentem trimestralmente informações pertinentes sobre uma proposta de projeto de sistema. A pedido do Parlamento Europeu ou do Conselho, a ENISA, com o acordo da Comissão, e sem prejuízo do artigo 27.º, pode disponibilizar ao Parlamento Europeu e ao Conselho as partes relevantes de uma proposta de projeto de sistema de uma forma adequada ao nível de confidencialidade exigido e, se for caso disso, de forma restrita.

3. A fim de reforçar o diálogo entre as instituições da União e contribuir para um processo de consulta formal, aberto, transparente e inclusivo, o Parlamento Europeu e o Conselho, ou ambos, podem convidar a Comissão e a ENISA a debater questões relativas ao funcionamento dos sistemas europeus de certificação da cibersegurança de produtos, serviços ou processos de TIC ou serviços de segurança geridos.

4. Ao avaliar o presente regulamento em conformidade com o artigo 67.º, a Comissão tem em conta, se for caso disso, os elementos decorrentes dos pontos de vista expressos pelo Parlamento Europeu e pelo Conselho sobre as questões referidas no n.º 3 do presente artigo.»;

9) O artigo 51.º é alterado do seguinte modo:

a) O título passa a ter a seguinte redação:

«Objetivos de segurança dos sistemas europeus de certificação da cibersegurança de produtos, serviços e processos de TIC»;

b) O proémio passa a ter a seguinte redação:

«Os sistemas europeus de certificação da cibersegurança de produtos, serviços e processos de TIC são concebidos de modo a alcançar, conforme aplicável, pelo menos os seguintes objetivos de segurança:»;

10) É inserido o seguinte artigo:

«*Artigo 51.º-A*

Objetivos de segurança dos sistemas europeus de certificação da cibersegurança de serviços de segurança geridos

Os sistemas europeus de certificação da cibersegurança de serviços de segurança geridos são concebidos de modo a alcançar, conforme aplicável, pelo menos os seguintes objetivos de segurança:

a) Que os serviços de segurança geridos sejam prestados com as competências, conhecimentos especializados e experiência necessários, nomeadamente que o pessoal responsável pela prestação desses serviços possua um nível suficiente e adequado de conhecimentos técnicos e competências no domínio específico, experiência suficiente e adequada e a maior integridade profissional;

b) Que o prestador disponha de procedimentos internos adequados para garantir que os serviços de segurança geridos sejam sempre prestados com um nível de qualidade suficiente e adequado;

c) Que os dados consultados, armazenados, transmitidos ou sujeitos a qualquer outro tipo de tratamento no âmbito da prestação de serviços de segurança geridos sejam protegidos, impedindo o acesso, conservação, divulgação, destruição, outro tipo de tratamento, perda, alteração ou indisponibilidade acidentais ou não autorizados;

d) Que a disponibilidade e o acesso aos dados, serviços e funções sejam restabelecidos em tempo útil, em caso de incidente físico ou técnico;

e) Que as pessoas, os programas ou as máquinas autorizadas só possam aceder aos dados, serviços ou funções abrangidos pelos seus direitos de acesso;

f) Que é mantido e está disponível para avaliação um registo dos dados, serviços ou funções que foram consultados, utilizados ou sujeitos a qualquer outro tipo de tratamento, quando e por quem;

g) Que os produtos, serviços e processos de TIC utilizados na prestação dos serviços de segurança geridos sejam seguros desde a conceção e por defeito e, quando aplicável, incluam as atualizações de segurança mais recentes e não contenham vulnerabilidades conhecidas.»;

11) O artigo 52.º é alterado do seguinte modo:

a) O n.º 1 passa a ter a seguinte redação:

«1. Os sistemas europeus de certificação da cibersegurança podem especificar um ou mais dos seguintes níveis de garantia de produtos, serviços e processos de TIC e serviços de segurança geridos: "básico", "substancial" ou "elevado". O nível de garantia é proporcional ao nível do risco associado à utilização prevista do produto, serviço ou processo de TIC ou do serviço de segurança gerido, em termos de probabilidade e impacto de ocorrência de um incidente.»;

b) O n.º 3 passa a ter a seguinte redação:

«3. Os requisitos de segurança que correspondem a cada nível de garantia são fornecidos no sistema europeu de certificação da segurança relevante, incluindo as funcionalidades de segurança e o rigor e a exaustividade correspondentes da avaliação a que deve ser sujeito o produto, serviço ou processo de TIC ou o serviço de segurança gerido.»;

c) Os n.os 5, 6 e 7 passam a ter a seguinte redação:

«5. Um certificado europeu de cibersegurança ou uma declaração UE de conformidade que ateste um nível de garantia "básico" dá garantia de que os produtos, serviços e processos de TIC ou os serviços de segurança geridos objeto desse certificado ou dessa declaração UE de conformidade cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos básicos conhecidos de incidentes e ciberataques. As atividades de avaliação a realizar compreendem, pelo menos, uma análise da documentação técnica. Caso tal análise não seja adequada, são realizadas atividades de avaliação alternativas de efeito equivalente.

6. Um certificado europeu de cibersegurança que ateste um nível de garantia "substancial" dá garantia de que os produtos, serviços e processos de TIC ou os serviços de segurança geridos objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos conhecidos para a cibersegurança e do risco de incidentes e ciberataques levados a cabo por autores com competências e recursos limitados. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público e a realização de ensaios para demonstrar que os produtos, serviços ou processos de TIC ou os serviços de segurança geridos aplicam corretamente as funcionalidades de segurança necessárias. Caso tais atividades de avaliação não sejam adequadas, são realizadas atividades de avaliação alternativas de efeito equivalente.

7. Um certificado europeu de cibersegurança que ateste um nível de garantia "elevado" dá garantia de que os produtos, serviços e processos de TIC ou os serviços de segurança geridos objeto desse certificado cumprem os requisitos de segurança correspondentes, incluindo as funcionalidades de segurança, e de que foram avaliados a um nível que visa a redução ao mínimo dos riscos de ciberataques sofisticados levados a cabo por autores com competências e recursos significativos. As atividades de avaliação a realizar compreendem, pelo menos, o seguinte: uma análise para demonstrar a inexistência de vulnerabilidades que sejam do conhecimento público, a realização de ensaios para demonstrar que os produtos, serviços ou processos de TIC ou os serviços de segurança geridos aplicam corretamente as funcionalidades de segurança necessárias, ao nível tecnológico mais avançado, e uma avaliação da sua resistência a atacantes competentes através de testes de intrusão. Caso tais atividades de avaliação não sejam adequadas, são realizadas atividades de avaliação alternativas de efeito equivalente.»;

12) No artigo 53.º, os n.os 1, 2 e 3 passam a ter a seguinte redação:

«1. Os sistemas europeus de certificação da cibersegurança podem permitir a realização de uma autoavaliação da conformidade sob a exclusiva responsabilidade do fabricante de produtos de TIC, do prestador de serviços de TIC, do fornecedor de processos de TIC ou do prestador de serviços de segurança geridos. A autoavaliação da conformidade é permitida apenas para produtos, serviços e processos de TIC ou serviços de segurança geridos com um nível de risco baixo, correspondente ao nível de garantia "básico".

2. O fabricante de produtos de TIC, o prestador de serviços de TIC, o fornecedor de processos de TIC ou o prestador de serviços de segurança geridos pode emitir uma declaração UE de conformidade que indique que foi demonstrado o cumprimento dos requisitos estabelecidos no sistema. Através da emissão dessa declaração, o fabricante de produtos de TIC, o prestador de serviços de TIC, o fornecedor de processos de TIC ou o prestador de serviços de segurança geridos assume a responsabilidade pela conformidade do produto, serviço ou processo de TIC ou do serviço de segurança gerido com os requisitos previstos nesse sistema.

3. O fabricante de produtos de TIC, o prestador de serviços de TIC, o fornecedor de processos de TIC ou o prestador de serviços de segurança geridos mantém à disposição da autoridade nacional de certificação da cibersegurança designada nos termos do artigo 58.º, pelo período fixado no sistema europeu de certificação da cibersegurança em causa, a declaração UE de conformidade, a documentação técnica e todas as outras informações pertinentes relativas à conformidade dos produtos, serviços e processos de TIC ou dos serviços de segurança geridos com o sistema. É apresentada à autoridade nacional de certificação da cibersegurança e à ENISA uma cópia da declaração UE de conformidade.»;

13) No artigo 54.º, o n.º 1 é alterado do seguinte modo:

a) A alínea a) passa a ter a seguinte redação:

«a) O objeto e o âmbito do sistema de certificação, nomeadamente o tipo ou as categorias de produtos, serviços e processos de TIC e de serviços de segurança geridos abrangidos;»;

b) A alínea g) passa a ter a seguinte redação:

«g) Os critérios e métodos de avaliação específicos, nomeadamente os tipos de avaliação, a utilizar para demonstrar que são alcançados os objetivos de segurança aplicáveis referidos nos artigos 51.º e 51.º-A;»;

c) A alínea j) passa a ter a seguinte redação:

«j) As regras para o controlo da conformidade dos produtos, serviços ou processos de TIC ou dos serviços de segurança geridos com os requisitos dos certificados europeus de cibersegurança ou da declaração UE de conformidade, incluindo mecanismos para demonstrar a conformidade permanente com os requisitos de cibersegurança especificados;»;

d) A alínea l) passa a ter a seguinte redação:

«l) As regras relativas às consequências para os produtos, serviços e processos de TIC ou para os serviços de segurança geridos que tenham sido certificados ou para os quais tenha sido emitida uma declaração UE de conformidade, mas que não cumprem os requisitos do sistema;»;

e) A alínea o) passa a ter a seguinte redação:

«o) A identificação dos sistemas nacionais ou internacionais de certificação da cibersegurança que abranjam os mesmos tipos ou categorias de produtos, serviços e processos de TIC ou de serviços de segurança geridos, requisitos de segurança, critérios e métodos de avaliação e níveis de garantia;»;

f) A alínea q) passa a ter a seguinte redação:

«q) O período de disponibilidade da declaração UE de conformidade, da documentação técnica e de todas as outras informações relevantes a disponibilizar pelo fabricante de produtos de TIC, o prestador de serviços de TIC, o fornecedor de processos de TIC ou o prestador de serviços de segurança geridos;»;

14) O artigo 56.º é alterado do seguinte modo:

a) O n.º 1 passa a ter a seguinte redação:

«1. Presume-se que os produtos, serviços e processos de TIC e os serviços de segurança geridos que tenham sido certificados ao abrigo de um sistema europeu de certificação da cibersegurança adotado nos termos do artigo 49.º cumprem os requisitos desse sistema.»;

b) O n.º 3 é alterado do seguinte modo:

i) o primeiro parágrafo passa a ter a seguinte redação:

«A Comissão avalia regularmente a eficiência e a utilização dos sistemas europeus de certificação da cibersegurança adotados e se algum sistema europeu de certificação da cibersegurança específico deve passar a ser obrigatório por força do direito aplicável da União, a fim de assegurar um nível adequado de cibersegurança dos produtos, serviços e processos de TIC e, a partir de 4 de fevereiro de 2025, dos serviços de segurança geridos na União e melhorar o funcionamento do mercado interno. A primeira dessas avaliações deve ser realizada até 31 de dezembro de 2023 e as avaliações subsequentes devem ser efetuadas pelo menos de dois em dois anos. Com base no resultado dessas avaliações, a Comissão identifica os produtos, serviços e processos de TIC e os serviços de segurança geridos abrangidos por um sistema de certificação existente que devem ser abrangidos por um sistema de certificação obrigatório.»,

ii) o terceiro parágrafo é alterado do seguinte modo:

— a alínea a) passa a ter a seguinte redação:

«a) Toma em consideração o impacto das medidas para os fabricantes de produtos de TIC, os prestadores de serviços de TIC, os fornecedores de processos de TIC e os prestadores de serviços de segurança geridos e para os utilizadores em termos de custos dessas medidas, e os benefícios societais ou económicos decorrentes do reforço previsto do nível de segurança para os produtos, serviços e processos de TIC e os serviços de segurança geridos visados;»,

— a alínea d) passa a ter a seguinte redação:

«d) Toma em consideração os prazos de aplicação, as medidas e os períodos de transição, tendo especialmente em conta o eventual impacto da medida para os fabricantes de produtos de TIC, os prestadores de serviços de TIC, os fornecedores de processos de TIC e os prestadores de serviços de segurança geridos, incluindo os interesses e necessidades específicos das PME, incluindo microempresas;»;

c) Os n.os 7 e 8 passam a ter a seguinte redação:

«7. As pessoas singulares ou coletivas que submetem os seus produtos, serviços ou processos de TIC ou serviços de segurança geridos à certificação disponibilizam à autoridade nacional de certificação da cibersegurança designada nos termos do artigo 58.º, quando essa autoridade for o organismo que emite o certificado europeu de certificação da cibersegurança ou o organismo de avaliação da conformidade a que se refere o artigo 60.º, todas as informações necessárias para efetuar a certificação.

8. O titular de um certificado europeu de cibersegurança informa a autoridade ou o organismo referido no n.º 7 de quaisquer vulnerabilidades ou irregularidades posteriormente detetadas relativas à segurança do produto, serviço ou processo de TIC ou do serviço de segurança gerido certificado que possam ter um impacto na conformidade do produto, serviço ou processo de TIC ou do serviço de segurança gerido com os requisitos relacionados com a certificação. Essa autoridade ou organismo transmite essas informações sem demora injustificada à autoridade nacional de certificação da cibersegurança.»;

15) No artigo 57.º, os n.os 1 e 2 passam a ter a seguinte redação:

«1. Sem prejuízo do disposto no n.º 3 do presente artigo, os sistemas nacionais de certificação da cibersegurança e os procedimentos conexos relativos aos produtos, serviços e processos de TIC e serviços de segurança geridos abrangidos por um sistema europeu de certificação da cibersegurança deixam de produzir efeitos a partir da data estabelecida no ato de execução adotado ao abrigo do artigo 49.º, n.º 7. Os sistemas nacionais de certificação da cibersegurança e os procedimentos conexos relativos aos produtos, serviços e processos de TIC e serviços de segurança geridos que não sejam abrangidos por um sistema europeu de certificação da cibersegurança continuam a existir.

2. Os Estados-Membros não podem introduzir novos sistemas nacionais de certificação da cibersegurança relativos aos produtos, serviços e processos de TIC e serviços de segurança geridos abrangidos por um sistema europeu de certificação da cibersegurança em vigor.»;

16) O artigo 58.º é alterado do seguinte modo:

a) O n.º 7 é alterado do seguinte modo:

i) as alíneas a) e b) passam a ter a seguinte redação:

«a) Supervisionar e fazer aplicar as regras incluídas nos sistemas europeus de certificação da cibersegurança, nos termos do artigo 54.º, n.º 1, alínea j), para efetuar o controlo da conformidade dos produtos, serviços e processos de TIC e dos serviços de segurança geridos com os requisitos dos certificados europeus de cibersegurança emitidos nos respetivos territórios, em cooperação com outras autoridades de fiscalização de mercado competentes;

b) Controlar o cumprimento das obrigações do fabricante de produtos de TIC, do prestador de serviços de TIC, do fornecedor de processos de TIC ou do prestador de serviços de segurança geridos estabelecidos nos respetivos territórios e que efetuem a autoavaliação da conformidade e fazer executar essas obrigações, em especial, as obrigações estabelecidas no artigo 53.º, n.ºs 2 e 3, e no respetivo sistema europeu de certificação da cibersegurança;»,

ii) a alínea h) passa a ter a seguinte redação:

«h) Cooperar com outras autoridades nacionais de certificação da cibersegurança ou outras autoridades públicas, inclusive através da partilha de informações sobre a eventual não conformidade de produtos, serviços e processos de TIC ou de serviços de segurança geridos com os requisitos do presente regulamento ou de sistemas europeus de certificação da cibersegurança específicos; e»;

b) O n.º 9 passa a ter a seguinte redação:

«9. As autoridades nacionais de certificação da cibersegurança cooperam entre si e com a Comissão e, em particular, partilham informações, experiências e boas práticas em matéria de certificação da cibersegurança e de questões técnicas relacionadas com a cibersegurança dos produtos, serviços e processos de TIC e dos serviços de segurança geridos.»;

17) No artigo 59.º, n.º 3, as alíneas b) e c) passam a ter a seguinte redação:

«b) Os procedimentos destinados a supervisionar e controlar a aplicação das regras relativas ao controlo da conformidade dos produtos, serviços e processos de TIC e dos serviços de segurança geridos com os certificados europeus de cibersegurança nos termos do artigo 58.º, n.º 7, alínea a);

c) Os procedimentos destinados a controlar o cumprimento das obrigações dos fabricantes de produtos de TIC, dos prestadores de serviços de TIC, dos fornecedores de processos de TIC e dos prestadores de serviços de segurança geridos nos termos do artigo 58.º, n.º 7, alínea b);»;

18) No artigo 67.º, os n.ºs 2 e 3 passam a ter a seguinte redação:

«2. A avaliação visa igualmente o impacto, a eficácia e a eficiência das disposições do título III do presente regulamento, incluindo os procedimentos conducentes à adoção de sistemas europeus de certificação da cibersegurança e respetivas bases de dados, no que respeita aos objetivos de assegurar um nível adequado de cibersegurança dos produtos, serviços e processos de TIC e dos serviços de segurança geridos na União e de melhorar o funcionamento do mercado interno.

3. A avaliação deve verificar se são necessários requisitos de cibersegurança essenciais para o acesso ao mercado interno, a fim de impedir que produtos, serviços e processos de TIC e serviços de segurança geridos que não cumpram os requisitos básicos de cibersegurança entrem no mercado interno.»;

19) O anexo é alterado em conformidade com o anexo do presente regulamento.

Artigo 2.º

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 19 de dezembro de 2024.

Pelo Parlamento Europeu	*Pelo Conselho*
A Presidente	*O Presidente*
R. METSOLA	BÓKA J.

ANEXO

O anexo do Regulamento (UE) 2019/881 é alterado do seguinte modo:

1) Os pontos 2 a 5 passam a ter a seguinte redação:

«2. Os organismos de avaliação da conformidade devem ser organismos terceiros independentes da organização ou dos produtos, serviços ou processos de TIC ou serviços de segurança geridos que avaliam.

3. Os organismos que pertençam a organizações empresariais ou associações profissionais que representem empresas envolvidas nas atividades de conceção, fabrico, fornecimento, montagem, utilização ou manutenção de produtos, serviços ou processos de TIC ou serviços de segurança geridos por si avaliados podem ser considerados organismos de avaliação da conformidade, desde que demonstrem a respetiva independência e a inexistência de conflitos de interesses.

4. Os organismos de avaliação da conformidade, os seus quadros superiores e o pessoal encarregado de executar as tarefas de avaliação da conformidade não podem ser o projetista, o fabricante, o fornecedor, o instalador, o comprador, o proprietário, o utilizador ou o responsável pela manutenção dos produtos, serviços ou processos de TIC ou do serviço de segurança gerido a avaliar, ou o representante autorizado de uma dessas partes. Esta proibição não obsta à utilização de produtos de TIC avaliados que sejam necessários às atividades do organismo de avaliação da conformidade, nem à utilização desses produtos de TIC para fins pessoais.

5. Os organismos de avaliação da conformidade, os seus quadros superiores e o pessoal encarregado de executar as tarefas de avaliação da conformidade não podem intervir diretamente na conceção, no fabrico ou na construção, no fornecimento, na comercialização, na instalação, na utilização nem na manutenção dos produtos, serviços ou processos de TIC ou serviços de segurança geridos que são objeto da avaliação. Os organismos de avaliação da conformidade, os seus quadros superiores e o pessoal encarregado de executar as tarefas de avaliação da conformidade não podem exercer qualquer atividade suscetível de comprometer a independência do seu julgamento ou a sua integridade no exercício das atividades de avaliação da conformidade. Essa proibição é aplicável, nomeadamente, aos serviços de consultoria.»;

2) O ponto 10 é alterado do seguinte modo:

a) O proémio passa a ter a seguinte redação:

«10. Para cada procedimento de avaliação da conformidade e para cada tipo, categoria ou subcategoria de produtos, serviços ou processos de TIC ou serviços de segurança geridos, os organismos de avaliação da conformidade devem sempre dispor de:»

b) A alínea c) passa a ter a seguinte redação:

«c) Procedimentos que permitam o exercício das suas atividades, tendo devidamente em conta a dimensão, o setor e a estrutura das empresas, o grau de complexidade da tecnologia do produto, serviço ou processo de TIC ou do serviço de segurança gerido em causa e a natureza do processo de produção em massa ou em série.»;

3) Os pontos 19 e 20 passam a ter a seguinte redação:

«19. Os organismos de avaliação da conformidade devem cumprir os requisitos da norma harmonizada aplicável, na aceção do artigo 2.º, ponto 9, do Regulamento (CE) n.º 765/2008, para a acreditação de organismos de avaliação da conformidade que certifiquem produtos, serviços ou processos de TIC ou serviços de segurança geridos.

20. Os organismos de avaliação da conformidade devem assegurar que os laboratórios de ensaio utilizados para fins de avaliação da conformidade cumpram os requisitos da norma harmonizada aplicável, na aceção do artigo 2.º, ponto 9, do Regulamento (CE) n.º 765/2008 para a acreditação de laboratórios que realizem ensaios.».

Foi feita uma declaração relativamente ao presente ato, que pode ser consultada em JO C, C/2025/307, 15.1.2025, ELI: http://data.europa.eu/eli/C/2025/307/oj.