CEPD-AEPD Parecer Conjunto 4/2026

sobre a proposta de Regulamento Cibersegurança 2
e a proposta de alterações da Diretiva SRI 2

Adotado em 18 de março de 2026

Índice

Síntese

Em 20 de janeiro de 2026, a Comissão Europeia apresentou uma proposta de regulamento relativo à Agência da União Europeia para a Cibersegurança (ENISA), ao enquadramento europeu para a certificação da cibersegurança e à segurança da cadeia de abastecimento de TIC e que revoga o Regulamento (UE) 2019/881 (Regulamento Cibersegurança 2) e uma proposta de diretiva que altera a Diretiva (UE) 2022/2555 no respeitante a medidas de simplificação e ao alinhamento com a [proposta de Regulamento Cibersegurança 2]. Em 21 de janeiro de 2026, a Comissão consultou formalmente o CEPD e a AEPD, em conformidade com o artigo 42.º, n.º 2, do Regulamento (UE) 2018/1725.

O CEPD e a AEPD recordam que a relação entre a proteção de dados e a cibersegurança tem duas vertentes. Por um lado, a cibersegurança contribui para a proteção dos dados pessoais, ao limitar os riscos de acesso indesejado, alteração ou indisponibilidade desses dados. Por outro lado, algumas medidas de cibersegurança podem interferir com os direitos e liberdades das pessoas, em especial os direitos à privacidade e à proteção de dados. Por conseguinte, embora a eficácia seja um aspeto importante das medidas de cibersegurança, é necessário ter em conta a necessidade e a proporcionalidade.

O CEPD e a AEPD apoiam o objetivo geral das propostas de reforçar o papel da Agência da União Europeia para a Cibersegurança (ENISA) e facilitar a adoção da certificação da cibersegurança, sob reserva das recomendações específicas apresentadas no presente parecer conjunto. Congratulam-se também com o objetivo de estabelecer mecanismos e condições na Diretiva (UE) 2022/2555 para ajudar a facilitar o cumprimento dos requisitos de cibersegurança, tornando assim a aplicação desses requisitos mais coerente e eficaz, bem como com o objetivo de continuar a fazer face aos vários riscos para as cadeias de abastecimento de TIC, incluindo os não técnicos. Apoiam também vivamente o objetivo de criar um ponto de entrada único para a notificação de violações de dados pessoais, uma vez que tal reduziria os encargos administrativos para as organizações, sem afetar o nível de proteção dos titulares dos dados.

O CEPD e a AEPD congratulam-se também com o facto de a proposta de Regulamento Cibersegurança 2 prever uma maior clarificação das modalidades de prestação de apoio por parte da ENISA às diferentes partes interessadas e recomendam que a AEPD seja igualmente incluída como possível requerente de aconselhamento à ENISA. O CEPD e a AEPD apoiam firmemente que esse aconselhamento seja prestado na sequência de um pedido, assegurando uma coordenação clara e uma repartição inequívoca das responsabilidades.

No que respeita à cooperação entre a ENISA e outras entidades da União em geral, o CEPD e a AEPD congratulam-se com as sinergias que esta cooperação pode permitir, em consonância com as respetivas atribuições e mandatos. Recomendam o aditamento de uma referência explícita também à AEPD enquanto organismo da União com o qual a ENISA cooperaria.

O CEPD e a AEPD consideram que, se as futuras atribuições da ENISA enquanto plataforma de informação exigirem um tratamento substancial de dados pessoais, tal deve ser explicitamente especificado nas disposições do ato de base que rege as respetivas atribuições, incluindo os elementos essenciais de qualquer tratamento em grande escala e as garantias adequadas. Em contrapartida, se o objetivo for permitir que a ENISA proceda, principalmente, à recolha e ao tratamento posterior de dados maioritariamente agregados e não pessoais, tal também deverá ser clarificado.

O CEPD e a AEPD recordam que, em princípio, apenas os pormenores (práticos) muito técnicos relacionados com o tratamento de dados pessoais devem ser decididos no âmbito da autonomia administrativa do organismo da UE em causa (neste caso, o Conselho de Administração de uma agência descentralizada). Além disso, recomendam que o artigo 66.º da proposta de Regulamento Cibersegurança 2 preveja uma consulta prévia da AEPD antes da adoção dessas regras.

No que diz respeito ao Quadro Europeu de Competências em Cibersegurança («QECC»), o CEPD e a AEPD recomendam aos colegisladores que alterem o artigo 19.º, n.º 2, da proposta de Regulamento Cibersegurança 2, para que o QECC não se limite exclusivamente aos «profissionais de cibersegurança», mas inclua também perfis para a mão de obra em geral.

Relativamente ao enquadramento europeu para a certificação da cibersegurança, o CEPD e a AEPD recomendam uma maior clarificação do âmbito de aplicação do artigo 80.º, n.º 1, alínea w), do Regulamento Cibersegurança 2 e da sua relação com a certificação ao abrigo do RGPD. Além disso, a fim de assegurar a coerência, o CEPD e a AEPD recomendam que se exija à ENISA que consulte o CEPD antes de adotar um sistema de certificação nos termos do artigo 80.º, n.º 1, alínea w), do Regulamento Cibersegurança 2.

O CEPD e a AEPD salientam a necessidade de ter em conta não só a eficácia das medidas de cibersegurança, mas também a sua necessidade e proporcionalidade. Recomendam que se clarifique que os sistemas de certificação devem, na medida do possível, ter em conta controlos de segurança que possam ajudar a demonstrar o cumprimento dos requisitos do RGPD, em especial quando os sistemas se aplicam a produtos, serviços e processos de TIC e serviços de segurança geridos suscetíveis de serem utilizados em operações de tratamento de dados.

O CEPD e a AEPD congratulam-se ainda com a medida proposta destinada a assegurar um enquadramento para uma cadeia de abastecimento de TIC fiável e a fazer face aos riscos não técnicos em setores de importância crítica.

No que diz respeito à proposta que altera a Diretiva SRI 2, o CEPD e a AEPD congratulam-se com a designação dos fornecedores de carteiras europeias de identidade digital e de carteiras empresariais europeias como «entidades essenciais» e apoiam plenamente o importante objetivo de prevenir futuros ataques de *software* de sequestro (*ransomware*) e de neutralizar e desmantelar as organizações criminosas que os levam a cabo.

O Comité Europeu para a Proteção de Dados e a Autoridade Europeia para a Proteção de Dados

Tendo em conta o artigo 42.º, n.º 2, do Regulamento (UE) 2018/1725, 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,

Adotaram o seguinte parecer conjunto (a seguir designado por «parecer»)

1 CONTEXTO

1. Em 20 de janeiro de 2026, a Comissão Europeia («Comissão») apresentou uma proposta de regulamento relativo à Agência da União Europeia para a Cibersegurança (ENISA), ao enquadramento europeu para a certificação da cibersegurança e à segurança da cadeia de abastecimento de TIC e que revoga o Regulamento (UE) 2019/881 (Regulamento Cibersegurança 2)[1] e uma proposta de diretiva que altera a Diretiva (UE) 2022/2555 no respeitante a medidas de simplificação e ao alinhamento com a [proposta de Regulamento Cibersegurança 2][2] (a seguir designadas por «proposta de Regulamento Cibersegurança 2» e «proposta de alterações da Diretiva SRI 2» e, conjuntamente, por «propostas»). Em 21 de janeiro de 2026, a Comissão consultou formalmente o CEPD e a AEPD, em conformidade com o artigo 42.º, n.º 2, do Regulamento (UE) 2018/1725 («RPDUE»)[3].
2. A proposta de Regulamento Cibersegurança 2 visa substituir o atual Regulamento Cibersegurança[4], a fim de 1) reforçar o papel da ENISA, com destaque para as necessidades das partes interessadas num cenário de ameaças cada vez mais hostil, 2) relançar a aplicação do enquadramento europeu para a certificação da cibersegurança, 3) reduzir a complexidade e a diversidade das políticas relacionadas com a cibersegurança e, 4) continuar a dar resposta aos riscos de segurança das cadeias de abastecimento de TIC[5].
3. A proposta de alterações da Diretiva SRI 2 centra-se, em especial, no terceiro objetivo, introduzindo clarificações e facilitando a conformidade por parte das entidades regulamentadas[6].

[1] COM(2026) 11 final.
[2] COM(2026) 13 final.
[3] 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).
[4] 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, ELI: http://data.europa.eu/eli/reg/2019/881/oj, conforme alterado pelo 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 (JO L, 2025/37, 15.1.2025, ELI: http://data.europa.eu/eli/reg/2025/37/oj).
[5] Exposição de motivos, COM(2026) 11 final, p. 1.
[6] COM(2026) 13 final.

4. O objetivo do presente parecer conjunto consiste em abordar os aspetos pertinentes das propostas que se revestem de especial importância para a proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais.

2 OBSERVAÇÕES DE CARÁTER GERAL

5. A proposta de Regulamento Cibersegurança 2 visa alargar o mandato da ENISA e torná-la mais operacional. O CEPD e a AEPD apoiam o reforço do papel da ENISA e o objetivo de facilitar a adoção da certificação da cibersegurança, ambos sob reserva das recomendações específicas a seguir apresentadas.

6. O CEPD e a AEPD congratulam-se também com o objetivo de estabelecer mecanismos e condições na Diretiva (UE) 2022/2555[7] (a seguir designada por «Diretiva SRI 2») para ajudar a facilitar o cumprimento dos requisitos de cibersegurança, tornando assim a aplicação desses requisitos mais coerente e eficaz, bem como com o objetivo de continuar a fazer face aos vários riscos para as cadeias de abastecimento de TIC, incluindo os não técnicos.

7. Conforme referido no seu parecer conjunto sobre a proposta *Omnibus* Digital[8], o CEPD e a AEPD apoiam vivamente o objetivo de criar um ponto de entrada único para a notificação de violações de dados pessoais, uma vez que tal reduziria os encargos administrativos para as organizações sem afetar o nível de proteção dos titulares dos dados.

8. O artigo 5.º, n.º 1, alínea f), do Regulamento (UE) 2016/679 (RGPD) estabelece a segurança como um dos princípios fundamentais relativos ao tratamento de dados pessoais. O artigo 32.º do RGPD define ainda esta obrigação, aplicável tanto aos responsáveis pelo tratamento como aos subcontratantes, de garantir um nível de segurança adequado. Ambas as disposições deixam claro que a segurança do tratamento de dados pessoais é essencial para o cumprimento da legislação da UE em matéria de proteção de dados.

9. A relação entre a proteção de dados e a cibersegurança tem duas vertentes. Por um lado, a cibersegurança contribui para a proteção dos dados pessoais, ao limitar os riscos de acesso indesejado, alteração ou indisponibilidade desses dados. Por outro lado, algumas medidas de cibersegurança podem interferir com os direitos e liberdades das pessoas, em especial os direitos à privacidade e à proteção de dados[9].

10. O CEPD e a AEPD recordam que o considerando 49 do RGPD reconhece que as medidas de cibersegurança que envolvam o tratamento de dados pessoais constituem um interesse legítimo do responsável pelo tratamento em causa, sublinhando simultaneamente que as medidas devem ser estritamente necessárias e proporcionadas para assegurar a segurança da rede e das informações. Por conseguinte, as medidas de cibersegurança devem não só orientar-se por considerações de eficácia, mas também ponderar se o seu impacto nos direitos fundamentais continua a ser limitado ao que é necessário e proporcionado.

---

[7] 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).

[8] *EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)*, adotado em 10 de fevereiro de 2026.

[9] Ver os seguintes pareceres da AEPD: *Opinion 5/2021 on the Cybersecurity Strategy and the NIS 2.0 Directive*, de 11 de março de 2021, pontos 10-11, *Opinion 7/2022 on the Proposal for a Regulation on information security in the institutions, bodies, offices and agencies of the Union*, de 17 de maio de 2022, pontos 9-10, e *Opinion 2/2024 on the Proposal for a Regulation amending the Cybersecurity Act as regards managed security services*, de 10 de janeiro de 2024, ponto 5.

3 APOIO DA ENISA À EXECUÇÃO DA POLÍTICA E DO DIREITO DA UNIÃO E À COOPERAÇÃO COM OUTRAS ENTIDADES DA UNIÃO

11. Nos termos do artigo 5.º, n.º 1, da proposta de Regulamento Cibersegurança 2, a ENISA deve contribuir para a execução da política e do direito da União em vários domínios, prestando apoio às diferentes partes interessadas enumeradas nesse artigo.

12. Entre elas, em consonância com o artigo 5.º, n.º 1, alínea h), da proposta de Regulamento Cibersegurança 2, a ENISA prestaria aconselhamento, a pedido do Comité Europeu para a Proteção de Dados, sobre a aplicação de aspetos específicos de cibersegurança da política e do direito da União relacionados com a proteção de dados e a privacidade. O CEPD e a AEPD observam que o artigo 5.º, n.º 1, alínea h), da proposta de Regulamento Cibersegurança 2 não é uma disposição inteiramente nova. O artigo 5.º, n.º 5, alínea c), do atual Regulamento Cibersegurança já prevê que a ENISA pode apoiar «[o]s Estados-Membros na aplicação dos aspetos específicos de cibersegurança das políticas e do direito da União em matéria de proteção de dados e privacidade, incluindo através da emissão, a pedido, de parecer dirigido ao Comité Europeu para a Proteção de Dados».

13. O CEPD e a AEPD congratulam-se com o facto de a proposta de Regulamento Cibersegurança 2 prever uma maior clarificação das modalidades de cooperação, mantendo simultaneamente os elementos essenciais do artigo 5.º, n.º 5, alínea c), do Regulamento Cibersegurança. O novo artigo 5.º, n.º 1, alínea h), clarificaria que o CEPD, enquanto organismo da União, tem o direito de solicitar diretamente o aconselhamento da ENISA (sem estar ligado à aplicação, pelos Estados-Membros, de aspetos específicos de cibersegurança da política e do direito da União relacionados com a proteção de dados e a privacidade).

14. Ao mesmo tempo, o CEPD e a AEPD recomendam que se acrescente também a AEPD como possível requerente de aconselhamento no artigo 5.º, n.º 1, alínea h), do Regulamento Cibersegurança 2, tendo em conta o papel desta última enquanto autoridade supervisora do tratamento de dados pessoais pelas instituições, órgãos e organismos da União Europeia. Permitir que tanto o CEPD como a AEPD recorram à competência técnica da ENISA no domínio da cibersegurança pode contribuir para assegurar que as suas orientações e decisões no domínio da proteção de dados se baseiem em conhecimentos de vanguarda em matéria de cibersegurança. Poderá haver vários temas em que o aconselhamento e a cooperação se revelem benéficos, incluindo normas e práticas operacionais em matéria de cibersegurança, bem como a utilização de tecnologias de proteção da privacidade no contexto da cibersegurança.

15. O CEPD e a AEPD apoiam vivamente que o aconselhamento referido no artigo 5.º, n.º 1, alínea h), do Regulamento Cibersegurança 2 só seja prestado após um pedido prévio do CEPD ou, tal como aqui proposto, da AEPD. Ao prever que a ENISA só atue a pedido do CEPD ou da AEPD, o artigo 5.º, n.º 1, alínea h), asseguraria uma coordenação clara e uma repartição inequívoca das responsabilidades[10].

[10] Ao fazer depender o envolvimento da ENISA de um pedido formulado pelas autoridades supervisoras, mantém-se um processo de consulta estruturado, em que a ENISA disponibiliza conhecimentos técnicos especializados, enquanto as autoridades supervisoras conservam pleno controlo sobre as decisões relacionadas com a proteção de dados. Tal assegura igualmente que qualquer intervenção da ENISA é coordenada, cabendo ao CEPD ou à AEPD assumir a liderança e determinar o curso de ação adequado. Este respeito pelos papéis estabelecidos promove a coerência, evita a fragmentação regulamentar e reforça a responsabilização dos organismos de proteção de dados no seu papel de supervisão.

16. O CEPD e a AEPD observam que o artigo 5.º, n.º 1, alínea h), da proposta de Regulamento Cibersegurança 2 parece ser uma manifestação específica de uma obrigação de cooperação mais geral consagrada no artigo 68.º da mesma proposta, que regula a cooperação da ENISA com outras entidades da União. Nos termos do artigo 68.º, a ENISA deve cooperar, em matérias relacionadas com a cibersegurança, com outros organismos da UE, incluindo o Comité Europeu para a Proteção de Dados, a fim de assegurar a coerência, criar sinergias e dar resposta a questões de interesse comum. Essa cooperação pode ser assegurada através do intercâmbio de competências técnicas e de boas práticas; da prestação de aconselhamento e da emissão de orientações sobre questões relacionadas com a cibersegurança; e do estabelecimento de disposições práticas com vista à execução de atribuições específicas, após consulta da Comissão.

17. O CEPD e a AEPD congratulam-se com a cooperação e as sinergias entre a ENISA e outras entidades da União, em consonância com as respetivas atribuições e mandatos. Neste contexto, por razões de clareza jurídica, recomendam a alteração do artigo 68.º da proposta de Regulamento Cibersegurança 2, aditando uma referência explícita também à AEPD enquanto organismo da União com o qual a ENISA cooperaria[11].

4 COOPERAÇÃO OPERACIONAL, CONHECIMENTO SITUACIONAL COMUM EM MATÉRIA DE CIBERSEGURANÇA E PROTEÇÃO DE DADOS PESSOAIS

18. Nos termos dos artigos 10.º e 11.º da proposta de Regulamento Cibersegurança 2, que constituiriam um desenvolvimento do atual artigo 7.º do Regulamento Cibersegurança, a ENISA alargaria o seu papel enquanto plataforma central para a cooperação operacional, incluindo o tratamento de quantidades substanciais de informações sobre ameaças[12]. Por conseguinte, é possível inferir que as informações tratadas pela ENISA no âmbito do seu papel podem incluir dados pessoais, como endereços IP, credenciais de utilizador, registos de utilizador, intercâmbios financeiros ou dados de contas comprometidas.

19. Na sequência dos esclarecimentos prestados pela Comissão Europeia[13], o CEPD e a AEPD entendem que o Regulamento Cibersegurança 2 não se destina a conferir poderes para o tratamento de dados pessoais em grande escala pela ENISA nem a autorizar esse tratamento[14].

---

[11] O CEPD e a AEPD consideram que o artigo 7.º, n.º 2, do atual Regulamento Cibersegurança, que obriga a ENISA a cooperar a nível operacional e a estabelecer sinergias com as instituições, órgãos e organismos da União, nomeadamente com as autoridades supervisoras responsáveis pela proteção da privacidade e dos dados pessoais, a fim de dar resposta a questões de interesse comum, já se estende à AEPD.

[12] Cf. COM(2026) 11 final, Ficha financeira e digital da proposta legislativa, p. 21: «Os novos elementos/atribuições da proposta conferirão valor acrescentado às partes interessadas europeias, que beneficiarão do facto de a ENISA ser uma plataforma de informação, contribuindo para a partilha de informações e fornecendo notificações de alerta aos seus constituintes», e p. 101: «Nos últimos anos, a ENISA tornou-se uma plataforma de informação, que detém informações provenientes de diferentes fontes. Neste sentido, muitas das atribuições da ENISA estão associadas à reutilização e reciclagem de informações para efeitos de várias análises.».

[13] Conforme prestados durante uma reunião *ad hoc* do subgrupo de peritos em tecnologia do CEPD, em 27 de fevereiro de 2026.

[14] A Comissão esclareceu que a ENISA não tem mandato para realizar análises operacionais de incidentes, nem tem acesso aos dados dos próprios incidentes. Em vez disso, os dados tratados serão agregados. Normalmente, os alertas das CSIRT

Embora tomando nota do facto de que a ENISA recolheria e trataria principalmente dados não pessoais agregados, o CEPD e a AEPD recordam, contudo, que se as futuras atribuições da ENISA enquanto plataforma de informação exigirem um tratamento substancial de dados pessoais, tal deve ser explicitamente especificado nas disposições do ato de base que rege as respetivas atribuições, incluindo os elementos essenciais de qualquer tratamento em grande escala e as garantias adequadas. Em contrapartida, se o objetivo for permitir que a ENISA proceda, principalmente, à recolha e ao tratamento posterior de dados agregados e não pessoais, tal deverá também ser clarificado, pelo menos através de um considerando.

20. O CEPD e a AEPD observam que a ENISA continuaria a tratar dados pessoais para fins administrativos[15]. O artigo 66.º, n.º 1, da proposta de Regulamento Cibersegurança 2, à semelhança do atual Regulamento Cibersegurança[16], contém uma referência geral à legislação aplicável em matéria de proteção de dados, ou seja, o RPDUE, sem prever quaisquer outras regras específicas.

21. Na mesma ordem de ideias, o artigo 66.º, n.º 2, da proposta de Regulamento Cibersegurança 2 reproduz o atual artigo 41.º, n.º 2, do Regulamento Cibersegurança, que prevê a possibilidade de o Conselho de Administração da ENISA adotar «medidas adicionais necessárias para a aplicação do Regulamento (UE) 2018/1725» pela Agência[17], sem que daí resulte qualquer obrigação de adoção de medidas específicas por parte do Conselho de Administração. O disposto no artigo 66.º, n.º 2, da proposta de Regulamento Cibersegurança 2 não especifica o âmbito e o tipo de tais medidas adicionais de proteção de dados, nem o procedimento de adoção aplicável. Também não clarifica o papel da AEPD no processo[18].

22. O CEPD e a AEPD entendem que se o Conselho de Administração da ENISA proceder à aplicação do artigo 66.º, n.º 2, da proposta de Regulamento Cibersegurança 2, as suas decisões devem fornecer pormenores adicionais sobre a forma como a ENISA efetua o tratamento de dados pessoais.

nacionais não incluem dados pessoais operacionais, mas dados administrativos, como informações de contacto. Na mesma ordem de ideias, as empresas que se inscrevem para receber alertas precoces podem também fornecer os seus dados de contacto. De acordo com a Comissão Europeia, no caso raro de as informações agregadas sobre ameaças ou incidentes fornecidas à ENISA conterem endereços IP, a ENISA não teria qualquer necessidade operacional e, por conseguinte, qualquer possibilidade jurídica e factual de investigar o assinante por detrás do endereço IP. A Comissão Europeia esclareceu ainda que o serviço de assistência previsto no artigo 13.º é de natureza consultiva, fornecendo, por exemplo, informações sobre a autoridade competente do Estado-Membro a contactar.

[15] Por exemplo, no processo de análise de pedidos de obtenção do estatuto de prestador de atestados autorizado ao abrigo do sistema de atestados individuais europeus de competências de cibersegurança (artigo 22.º), durante o processo de recurso contra decisões tomadas (artigos 36.º e seguintes), no tratamento de reclamações apresentadas por pessoas singulares ou coletivas em relação à certificação de declarações UE de conformidade [artigo 88.º, n.º 6, alínea h)] ou relacionadas com certificações de cibersegurança (artigo 96.º).

[16] Ver o artigo 41.º, n.º 1, do Regulamento (UE) 2019/881.

[17] Em 21 de novembro de 2019, o Conselho de Administração da ENISA adotou uma decisão relativa às normas internas em matéria de limitações de determinados direitos dos titulares de dados em relação ao tratamento de dados pessoais no contexto do funcionamento da ENISA, nos termos do artigo 25.º do RPDUE.

[18] Por exemplo, o artigo 18.º-A, n.º 5, do Regulamento (UE) 2016/794 (Regulamento Europol) prevê que o Conselho de Administração da Europol, deliberando sob proposta do diretor executivo, **após consulta à AEPD**, especifica as condições da transmissão e do tratamento dos dados pessoais [...] (destaque nosso).

23. O CEPD e a AEPD recordam que, em princípio, apenas os pormenores (práticos) muito técnicos relacionados com o tratamento de dados pessoais devem ser decididos no âmbito da autonomia administrativa do organismo da UE em causa, neste caso, o Conselho de Administração de uma agência descentralizada. Tal deve-se ao facto de a autorização de ingerências nos direitos fundamentais dever ser uma matéria preferencialmente reservada ao legislador e, quando muito, à Comissão, por meio de atos de execução ou de atos delegados [19]. Por conseguinte, o exato alcance da expressão «medidas adicionais necessárias para a aplicação do Regulamento (UE) 2018/1725 pela ENISA», constante da segunda frase do projeto de artigo 66.º, n.º 2, deve ser explicitamente clarificado na disposição normativa do regulamento.

24. Se, no entanto, se considerar necessário que o Conselho de Administração tome medidas que vão além dos pormenores técnicos (práticos) do tratamento já previstos na legislação ou em atos delegados ou de execução, para além de o respetivo âmbito de aplicação ser enquadrado de forma mais clara, as medidas a adotar pelo Conselho de Administração devem ser claras e precisas e a sua aplicação deve ser previsível para as pessoas em causa. Tal inclui a divulgação adequada dessas regras que, além disso, devem prever as salvaguardas necessárias para assegurar o cumprimento dos princípios e garantias fundamentais em matéria de proteção de dados, como a limitação da finalidade, a limitação da conservação e a proteção de dados desde a conceção e por defeito. Como salvaguarda adicional importante nesses casos, o CEPD e a AEPD recomendam que o artigo 66.º da proposta de Regulamento Cibersegurança 2 preveja uma consulta prévia da AEPD antes da adoção dessas regras[20].

5 PONTO DE ENTRADA ÚNICO PARA A NOTIFICAÇÃO DE INCIDENTES (ARTIGO 15.º DO REGULAMENTO CIBERSEGURANÇA 2)

25. Nos termos do artigo 15.º da proposta de Regulamento Cibersegurança 2, a ENISA tem de criar, disponibilizar, operar, manter e atualizar, conforme necessário, nomeadamente, a plataforma única de comunicação de informações criada nos termos do artigo 16.º, n.º 1, do Regulamento (UE) 2024/2847 e o ponto de entrada único para a notificação de incidentes criado nos termos do artigo 23.º-A da Diretiva (UE) 2022/2555. Estas ferramentas visam simplificar as diferentes obrigações de comunicação de informações relacionadas com a cibersegurança[21].

[19] Ver *Guidance for co-legislators on key elements of legislative proposals* da AEPD, disponível em https://www.edps.europa.eu/system/files/2025-05/EDPS_Publication_Guidance_for_co-legislators_EN.pdf, ponto 76.
[20] À semelhança do previsto no artigo 18.º-A, n.º 5, do Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho, de 11 de maio de 2016, que cria a Agência da União Europeia para a Cooperação Policial (Europol) e que substitui e revoga as Decisões 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI do Conselho (Regulamento Europol) (JO L 135 de 24.5.2016, p. 53).
[21] Ver artigo 16.º, n.º 1, do Regulamento (UE) 2024/2847 e COM(2025) 837 final, p. 8.

26. Conforme referido no seu parecer conjunto sobre a proposta *Omnibus* Digital[22], o CEPD e a AEPD apoiam vivamente o objetivo de criar um ponto de entrada único para a notificação de violações de dados pessoais, uma vez que tal reduziria os encargos administrativos para as organizações sem afetar o nível de proteção dos titulares dos dados. Na sua Declaração de Helsínquia[23], o CEPD já sublinhou o seu apoio a uma eventual solução europeia de notificação entre reguladores, uma vez que tal ajudaria a facilitar o cumprimento do RGPD. O CEPD e a AEPD recordam igualmente a importância de garantir a segurança das notificações apresentadas e transmitidas através do ponto de entrada único, uma vez que as notificações de violações de dados incluem frequentemente informações sensíveis[24].

6 QUADRO EUROPEU DE COMPETÊNCIAS EM CIBERSEGURANÇA («QECC») (ARTIGO 19.º DO REGULAMENTO CIBERSEGURANÇA 2)

27. O artigo 19.º da proposta de Regulamento Cibersegurança 2 exigiria que a ENISA desenvolvesse e disponibilizasse ao público um Quadro Europeu de Competências em Cibersegurança («QECC»). O QECC ajudaria a assegurar que os profissionais de cibersegurança, os empregadores, os prestadores de formação e as autoridades públicas de todos os Estados-Membros utilizam um entendimento comum das exigências específicas dos empregos no setor da cibersegurança. Apoiaria perfis profissionais claros, requisitos de qualificação transparentes e um melhor alinhamento entre a educação e as necessidades do mercado de trabalho. A ENISA utilizaria o QECC como base para a prestação de formação, em especial para apoiar a aplicação da legislação da UE em matéria de cibersegurança, a cooperação operacional entre os Estados-Membros e as atividades de sensibilização. Tal significa que o QECC funcionaria como uma base para programas estruturados de formação em cibersegurança, especialmente para as autoridades públicas e as entidades abrangidas pela legislação da UE em matéria de cibersegurança.

28. O CEPD e a AEPD congratulam-se com o objetivo de reforçar a mão de obra da UE no domínio da cibersegurança e sublinham que tornar as competências mais transferíveis e reconhecíveis além-fronteiras é importante para o funcionamento do mercado único digital.

[22] *EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)*, adotado em 10 de fevereiro de 2026.
[23] CEPD, *The Helsinki Statement on enhanced clarity, support and engagement*, *A fundamental rights approach to innovation and competitiveness*, adotada em 2 de julho de 2025.
[24] Ver o capítulo 8.3 do *EDPB-EDPS Joint Opinion 2/2026 On the Proposal for a Regulation as regards the simplification of the digital legislative framework (Digital Omnibus)*, adotado em 10 de fevereiro de 2026.

29. Ao mesmo tempo, observam que os perfis definidos no artigo 19.º, n.º 2, da proposta de Regulamento Cibersegurança 2 se limitam atualmente aos profissionais de cibersegurança. A proposta não inclui um perfil das competências necessárias para os cidadãos, funcionários públicos ou trabalhadores não especializados. Tal como reconhecido no considerando 21 da proposta de Regulamento Cibersegurança 2, a literacia digital é essencial para capacitar cidadãos resilientes, contudo, quase metade da população adulta não possui competências digitais básicas, apesar de estas serem um requisito para mais de 90 % dos empregos. Por conseguinte, o QECC deve incluir um perfil de «cibersegurança para generalistas», que abranja as competências mínimas que todos os residentes da UE em idade ativa devem ter para interagir de forma segura no mercado único digital, protegendo-se não só a si próprios, mas também à sua organização e a terceiros, em especial contra a mistificação da interface (*phishing*) assistida por IA, falsificações profundas, usurpação de identidade e ataques de engenharia social. Esse perfil poderia ser utilizado por organizações públicas ou privadas para a formação do seu pessoal, a fim de minimizar os riscos decorrentes do fator humano, reduzindo assim o risco global de violação de dados.

30. O CEPD e a AEPD observam que o considerando 45 da proposta distingue explicitamente o QECC do Quadro Europeu de Competências Digitais (DigComp 3.0), clarificando que este último se destina à vida quotidiana, à participação na sociedade, ao trabalho e à aprendizagem, e pode ser utilizado tanto por adultos como por crianças[25], ao passo que o QECC se destina a um público especializado, oferecendo um quadro simples que identifica as funções relacionadas com a cibersegurança e as tarefas, os conhecimentos e as competências conexos, necessários para as desempenhar.

31. O CEPD e a AEPD apoiam todas as iniciativas referidas, quer sejam executadas pela ENISA ou, no caso do DigComp, pelo Centro Comum de Investigação (JRC) da Comissão Europeia, uma vez que, desde que haja uma adesão suficiente, reduziriam o risco de violações de dados. Por conseguinte, incentivam todas as partes envolvidas a explorarem formas de aumentar o impacto dos quadros.

[25] O CEPD e a AEPD recordam ainda que, entre 2022 e 2024, a Comissão Europeia explorou o desenvolvimento de um Certificado Europeu de Competências Digitais (CECD), com base no DigComp. O certificado ajudaria as pessoas a obter o reconhecimento rápido e fácil das suas competências digitais por parte dos empregadores, dos prestadores de formação, entre outros. Esta iniciativa destinava-se a oferecer um selo de qualidade para a certificação de competências digitais em toda a Europa. Na sequência de um estudo de viabilidade (ver CENTENO, C., COSGROVE, J., CACHIA, R., MORA, T., DI LEGGE, A., VIVARELLI, S., BULIAN, G., MOYES PRELLEZO, N., PIÑA DE SANTISTEBAN, P., SCHULZ, C., HÜSING, T., CUARTAS-ACOSTA, A. e TROIA, S., *European Digital Skills Certificate (EDSC) Feasibility Study*, Serviço das Publicações da União Europeia, Luxemburgo, 2024, doi: 10.2760/958195, JRC138344, https://publications.jrc.ec.europa.eu/repository/handle/JRC138344) e de um projeto-piloto com vários países da UE, a Comissão Europeia concluiu que esse selo de qualidade não traria valor acrescentado suficiente aos cidadãos europeus. No entanto, o DigComp, publicado pela primeira vez em 2013, ainda existe (COSGROVE, J. e CACHIA, R., DigComp 3.0: *European Digital Competence Framework - Fifth Edition*, Serviço das Publicações da União Europeia, Luxemburgo, 2025, https://data.europa.eu/doi/10.2760/0001149, JRC144121). Descreve o que é necessário para se ser digitalmente competente na sociedade atual e apoia o desenvolvimento de competências digitais entre pessoas de todas as idades. Abrange uma vasta gama de níveis de competências, desde o básico ao altamente avançado. Várias competências do DigComp referem-se explicitamente à cibersegurança, como 4.1 «Proteção de dispositivos», 4.2 «Proteção de dados pessoais e privacidade» e até 4.4 «Proteção do ambiente» (evitar a fuga de dados de equipamento fora de uso). Outras áreas também abrangem competências pertinentes, incluindo competências da área 1, essenciais para a defesa contra ataques de engenharia social, contribuem para reduzir os riscos de ameaças internas na área 2 e para prevenir a divulgação acidental de informação, bem como para melhorar a rapidez de deteção de incidentes na área 5.

32. Ao mesmo tempo, o CEPD e a AEPD consideram que o DigComp não substitui um sistema específico de cibersegurança para generalistas[26] e recomendam aos colegisladores que alterem o artigo 19.º, n.º 2, da proposta de Regulamento Cibersegurança 2, para que o QECC não se limite exclusivamente aos «profissionais de cibersegurança», mas inclua também perfis para a mão de obra em geral ou para os cidadãos. Essa alteração deve ser acompanhada de uma alteração correspondente do considerando 45.

33. Além disso, o CEPD e a AEPD consideram que é necessário que os perfis profissionais do QECC integrem um módulo sobre a necessidade de assegurar a conformidade das medidas de cibersegurança com a legislação da UE em matéria de proteção de dados, em especial no que diz respeito à aplicação prática do princípio da proteção de dados desde a conceção e por defeito (artigo 25.º do RGPD), e convidam o colegislador a aditar um considerando com este objetivo.

7 ENQUADRAMENTO EUROPEU PARA A CERTIFICAÇÃO DA CIBERSEGURANÇA (TÍTULO III)

34. O artigo 71.º e o artigo 80.º, n.º 1, alínea w), da proposta de Regulamento Cibersegurança 2 regulam o âmbito da certificação da cibersegurança. O artigo 80.º, n.º 1, alínea w), acrescenta, como objetivo de segurança dos sistemas europeus de certificação da cibersegurança, «assegurar que a entidade seja capaz de garantir a segurança do tratamento de dados pessoais».

35. O CEPD e a AEPD observam que a redação do artigo 80.º, n.º 1, alínea w), da proposta de Regulamento Cibersegurança 2 está muito próxima dos requisitos do RGPD em matéria de segurança do tratamento[27]. Nesse sentido, o âmbito do novo sistema de certificação pode ser interpretado no sentido de incluir requisitos previstos no RGPD. No entanto, o âmbito jurídico e operacional não é totalmente claro, uma vez que a disposição não remete para disposições do RGPD (por exemplo, o artigo 5.º, n.º 1, alínea f), o artigo 32.º e o artigo 25.º do RGPD) e é colocada numa lista de «objetivos de segurança» (artigo 80.º, n.º 1, primeira frase).

36. O CEPD e a AEPD recordam que a segurança ao abrigo do RGPD diz respeito aos riscos para os direitos e liberdades fundamentais das pessoas singulares. Embora a definição jurídica de cibersegurança ao abrigo do direito da União inclua, de um modo geral, a proteção dos utilizadores e de outras pessoas[28], o âmbito das medidas de cibersegurança abrange normalmente todos os tipos de riscos para a organização em causa. Ainda assim, há a oportunidade de estabelecer sinergias para que a avaliação dos riscos possa integrar a proteção dos direitos e liberdades das pessoas singulares.

---

[26] No DigComp, o conteúdo relacionado com segurança encontra-se disperso por 21 competências, não inclui modelos de ameaça explícitos, não operacionaliza os riscos de segurança organizacionais e não estabelece uma correspondência direta com obrigações de conformidade. Embora o QECC, na sua forma atual, se aplicasse às competências dos profissionais de cibersegurança, não existe um quadro estruturado a nível da UE para as pessoas que não trabalham no domínio da cibersegurança. O CEPD e a AEPD recordam que a maioria das violações tem origem na mistificação da interface (*phishing*), na engenharia social, na utilização indevida de credenciais, na má configuração e na utilização de «TI paralela» (*shadow IT*), que são comportamentos generalistas. Um quadro de cibersegurança generalista poderia tornar os riscos explícitos, proporcionar expectativas ajustadas aos diferentes perfis profissionais (por exemplo, recursos humanos, finanças) e apoiar resultados mensuráveis.

[27] Ver o artigo 5.º, n.º 1, alínea f), e o artigo 32.º do RGPD.

[28] Ver o artigo 2.º, n.º 1, da proposta de Regulamento Cibersegurança 2, que é uma disposição já existente e tem a seguinte redação: «"Cibersegurança", as atividades necessárias para proteger de ciberameaças os sistemas de rede e informação, os seus utilizadores e outras pessoas afetadas».

37. O CEPD e a AEPD recordam ainda que o RGPD tem o seu próprio procedimento de certificação (artigos 42.º e 43.º do RGPD) e consideram que a certificação da cibersegurança é distinta da certificação em matéria de proteção de dados nos termos do artigo 42.º do RGPD.

38. Dito isto, o CEPD e a AEPD consideram que podem existir sinergias entre a certificação da cibersegurança e em matéria de proteção de dados. Por exemplo, a certificação no âmbito do Regulamento Cibersegurança 2 pode ser utilizada como prova de apoio para demonstrar que alguns requisitos de uma certificação ao abrigo do RGPD são cumpridos, no que diz respeito à cibersegurança. No entanto, o CEPD e a AEPD observam que o artigo 80.º, n.º 1, alínea w), da proposta de Regulamento Cibersegurança 2 não articula claramente a relação com a certificação ao abrigo dos artigos 42.º e 43.º do RGPD. No interesse da segurança jurídica, o CEPD e a AEPD recomendam uma maior clarificação do âmbito de aplicação do artigo 80.º, n.º 1, alínea w), do Regulamento Cibersegurança 2 e da sua relação com a certificação ao abrigo do RGPD. Além disso, a fim de assegurar a coerência, o CEPD e a AEPD recomendam que se exija à ENISA que consulte o CEPD antes de adotar um sistema de certificação nos termos do artigo 80.º, n.º 1, alínea w), do Regulamento Cibersegurança 2.

39. O CEPD e a AEPD salientam a necessidade de ter em conta não só a eficácia das medidas de cibersegurança, mas também a sua necessidade e proporcionalidade. Determinados controlos de cibersegurança criam riscos específicos em matéria de proteção de dados. Tal pode ocorrer, nomeadamente, no caso da monitorização e do registo, da inspeção profunda de pacotes ou da análise do comportamento dos utilizadores. Um sistema de certificação bem concebido para a segurança do tratamento poderá incluir controlos para assegurar que as medidas de segurança possam ser aplicadas de forma a cumprir as regras de proteção de dados (por exemplo, certos aspetos devem ser configuráveis, como é o caso da granularidade dos dados registados para fins de segurança, uma vez que tal pode permitir ou facilitar o cumprimento, por parte do responsável pelo tratamento, dos princípios da segurança e da minimização de dados previstos no RGPD; na mesma ordem de ideias, os períodos de conservação devem ser configuráveis, de modo a que o responsável pelo tratamento possa decidir, no contexto do tratamento que está a executar, durante quanto tempo os dados pessoais devem ser conservados antes de serem apagados ou anonimizados utilizando técnicas certificadas).

40. Por conseguinte, o CEPD e a AEPD recomendam que se explique num considerando que os sistemas de certificação devem, na medida do possível, ser concebidos, aplicados e mantidos de forma a ter em conta controlos de segurança que possam ajudar a demonstrar o cumprimento dos requisitos do RGPD quando os sistemas se aplicam a produtos, serviços e processos de TIC e serviços de segurança geridos suscetíveis de serem utilizados em operações de tratamento de dados. Importa igualmente salientar que alguns controlos podem ser facilitadores da privacidade e da proteção de dados desde a conceção e por defeito.

8 ENQUADRAMENTO PARA UMA CADEIA DE ABASTECIMENTO DE TIC FIÁVEL (TÍTULO IV)

41. A proposta de Regulamento Cibersegurança 2 acrescenta medidas para a segurança das cadeias de abastecimento de TIC, abordando, em especial, os riscos não técnicos, como os fatores geopolíticos, jurídicos, de propriedade, de dependência e de ingerência estratégica que afetam as cadeias de abastecimento de TIC em setores de importância crítica e noutros setores críticos. Embora essas medidas de segurança da cadeia de abastecimento visem principalmente fazer face a riscos que não estão diretamente relacionados com a proteção de dados, podem também ter um impacto benéfico na proteção dos direitos fundamentais, ao limitar a ingerência estrangeira nos dados dos titulares de dados da UE através de atividades como a espionagem e a vigilância.

42. O CEPD e a AEPD congratulam-se com a medida proposta destinada a assegurar um enquadramento para uma cadeia de abastecimento de TIC fiável e a fazer face aos riscos não técnicos em setores de importância crítica.

9 ENTIDADES ESSENCIAIS ADICIONAIS AO ABRIGO DA PROPOSTA QUE ALTERA A DIRETIVA SRI 2

43. A proposta que altera a Diretiva SRI 2 incluiria os fornecedores de carteiras europeias de identidade digital e de carteiras empresariais europeias como «entidades essenciais», independentemente da sua dimensão. As entidades classificadas como «essenciais» estão sujeitas a todas as obrigações de gestão dos riscos de cibersegurança previstas na SRI 2 e têm de aplicar as medidas de segurança exigidas nos termos do artigo 21.º da SRI 2, nomeadamente as políticas de análise dos riscos e de segurança, o tratamento de incidentes, a continuidade das atividades e a gestão de crises, a segurança da cadeia de abastecimento, o tratamento de vulnerabilidades, as políticas relativas à utilização de criptografia e de cifragem, e o controlo do acesso e gestão de ativos.

44. O CEPD e a AEPD congratulam-se com a designação dos fornecedores de carteiras europeias de identidade digital e de carteiras empresariais europeias como «entidades essenciais». Consideram que as carteiras de identidade digital são uma componente central da infraestrutura digital da UE, pelo que os incidentes que as afetam podem ter um amplo impacto transfronteiriço, dado que estão subjacentes à identificação segura, à autenticação e aos certificados eletrónicos. Para a economia digital, as carteiras empresariais são tão críticas como as carteiras europeias de identidade digital. Por conseguinte, ambos os tipos de fornecedores de carteiras são tratados da mesma forma que os prestadores de serviços de confiança, que já foram designados como «entidades essenciais» ao abrigo da Diretiva SRI 2, e outros operadores de infraestruturas altamente críticas.

10 RECOLHA DE DADOS SOBRE ATAQUES DE *SOFTWARE* DE SEQUESTRO (*RANSOMWARE*)

45. Nos termos do artigo 5.º, n.º 8, da proposta de alterações da Diretiva SRI 2, que propõe o aditamento dos números 12 e 13 ao artigo 23.º da SRI 2, em caso de ataque de *software* de sequestro, pode ser solicitado às entidades em causa que apresentem determinadas informações relativas a incidentes com *software* de sequestro às equipas de resposta a incidentes de segurança informática (CSIRT), nomeadamente se a entidade em causa pagou ou não um resgate e, em caso afirmativo, o montante e o destinatário (criptoativos/prestadores de serviços) e a identidade da pessoa que atua como ponto de contacto.

46. Nos termos do artigo 23.º, n.º 11, da Diretiva SRI 2, a Comissão fica habilitada a adotar atos de execução que especifiquem o tipo de informações, o formato e o procedimento das obrigações de notificação. O âmbito de aplicação desse ato de execução seria alargado para abranger também as novas obrigações de comunicação de informações em caso de ataques de *software* de sequestro.

47. O CEPD e a AEPD apoiam plenamente o importante objetivo de prevenir futuros ataques de *software* de sequestro e neutralizar e desmantelar as organizações criminosas que os levam a cabo. Salientam também que as informações a partilhar sobre ataques de *software* de sequestro podem ser de natureza potencialmente sensível, tal como explicado com mais pormenor pela Comissão no considerando 10 da proposta de alterações da Diretiva SRI 2. Além disso, essa comunicação de informações pode implicar o tratamento de dados pessoais. O CEPD e a AEPD congratulam-se com a abordagem por níveis escolhida nos n.^{os} 12 e 13, em que as informações mais sensíveis referidas no n.º 13 só serão comunicadas a pedido.

48. Ao mesmo tempo, tendo em conta a sensibilidade dos dados comunicados e em consonância com os princípios da necessidade e da proporcionalidade, caso a comunicação de ataques de *software* de sequestro envolva o tratamento de dados pessoais, o CEPD e a AEPD recomendam que se especifiquem no ato de execução nos termos do artigo 23.º, n.º 11, da Diretiva SRI 2 as garantias aplicáveis em matéria de proteção de dados. A este respeito, recordam igualmente o requisito de a Comissão, nos termos do artigo 42.º, n.º 1, do RPDUE, consultar a AEPD sobre os projetos de atos de execução e de atos delegados caso exista um impacto na proteção dos direitos e das liberdades das pessoas singulares no que diz respeito ao tratamento de dados pessoais.