Conselho
da União Europeia

Bruxelas, 17 de dezembro de 2025
(OR. en)

16960/25

CYBER 389
JAI 1924
DATAPROTECT 345
TELECOM 485
MI 1075
CSC 693
CSCI 284
DELACT 198

NOTA DE ENVIO

de:	Secretária-geral da Comissão Europeia, com a assinatura de Martine DEPREZ, diretora
data de receção:	11 de dezembro de 2025
para:	Thérèse BLANCHET, secretária-geral do Conselho da União Europeia
n.° doc. Com.:	C(2025) 8407 final
Assunto:	REGULAMENTO DELEGADO (UE) …/... DA COMISSÃO de 11.12.2025 que completa o Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, ao especificar os termos e condições de aplicação dos motivos relacionados com a cibersegurança no que diz respeito ao adiamento da divulgação de notificações

Envia-se em anexo, à atenção das delegações, o documento C(2025) 8407 final.

Anexo: C(2025) 8407 final

COMISSÃO
EUROPEIA

Bruxelas, 11.12.2025
C(2025) 8407 final

REGULAMENTO DELEGADO (UE) …/... DA COMISSÃO

de 11.12.2025

que completa o Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, ao especificar os termos e condições de aplicação dos motivos relacionados com a cibersegurança no que diz respeito ao adiamento da divulgação de notificações

(Texto relevante para efeitos do EEE)

EXPOSIÇÃO DE MOTIVOS

1. CONTEXTO DO ATO DELEGADO

O Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho («Regulamento de Ciber-Resiliência») exige que os fabricantes de produtos com elementos digitais notifiquem, através de uma plataforma única de comunicação de informações, qualquer vulnerabilidade ativamente explorada ou incidente grave com impacto na segurança de um produto com elementos digitais. Nos termos do artigo 16.º, n.º 2, do referido regulamento, a equipa de resposta a incidentes de segurança informática (CSIRT) designada pelo Estado-Membro como coordenadora que inicialmente recebe a notificação pode, em circunstâncias excecionais e por motivos justificados relacionados com a cibersegurança, adiar a divulgação da notificação às CSIRT de outros Estados-Membros onde o produto com elementos digitais tenha sido disponibilizado.

Por conseguinte, o presente ato delegado destina-se a completar o Regulamento de Ciber-Resiliência, ao especificar os termos e condições de aplicação dos motivos relacionados com a cibersegurança no que diz respeito ao adiamento da divulgação de notificações. Para o efeito, identifica três tipos de motivos pelos quais a CSIRT que recebeu inicialmente a notificação pode decidir que é necessário adiar a divulgação a outras CSIRT. Essa decisão de adiamento pode ser tomada em três circunstâncias:

- à luz de uma avaliação da natureza das informações notificadas,
- caso a CSIRT que recebe a notificação não possa assegurar a confidencialidade das informações,
- se a plataforma única de comunicação de informações tiver sido comprometida ou estiver temporariamente inoperacional.

As obrigações de comunicação de informações previstas no artigo 14.º do Regulamento (UE) 2024/2847 são aplicáveis a partir de 11 de setembro de 2026.

2. CONSULTAS ANTERIORES À ADOÇÃO DO ATO

A rede de CSIRT e a Agência da União Europeia para a Cibersegurança (ENISA) foram consultadas sobre vários projetos do presente ato. Em 26 de março de 2025, realizou-se um debate preliminar com perguntas de orientação, tendo sido dada a possibilidade de apresentar contributos escritos até 11 de abril de 2025. Um primeiro projeto do presente ato foi partilhado com a rede de CSIRT e a ENISA em 16 de maio de 2025, tendo sido realizado um debate em 6 de junho de 2025, com a possibilidade de apresentar contributos escritos até 27 de junho de 2025. Em 23 de julho de 2025, foi partilhado um segundo projeto de ato com a rede de CSIRT e a ENISA, com a possibilidade de apresentar contributos escritos até 1 de setembro de 2025. Um terceiro projeto do presente ato foi partilhado com a rede de CSIRT e a ENISA em 25 de setembro de 2025, tendo sido realizado um debate em 9 de outubro de 2025, com a possibilidade de apresentar contributos escritos até 27 de outubro de 2025.

O projeto de ato foi objeto de uma consulta pública entre 16 de outubro de 2025 e 13 de novembro de 2025, que recebeu 34 respostas de 31 inquiridos (tendo em conta que um mesmo inquirido apresentou quatro contributos diferentes). Destas, 29,41 % provinham de associações empresariais, 26,47 % de empresas, 17,65 % de cidadãos da UE, 14,71 % de

autoridades públicas, 5,88 % de organizações não governamentais (ONG) e 5,88 % de instituições académicas/de investigação[1].

Em 22 de outubro, o projeto foi igualmente debatido com o Grupo de Peritos em Cibersegurança de Produtos com Elementos Digitais (E03967), cujos membros incluem autoridades dos Estados-Membros, a ENISA, peritos nomeados a título pessoal e organizações no sentido lato do termo (por exemplo, empresas, associações ou ONG).

3. ELEMENTOS JURÍDICOS DO ATO DELEGADO

A habilitação para adotar atos delegados está prevista no artigo 14.º, n.º 9, do Regulamento de Ciber-Resiliência, que exige que, até 11 de dezembro de 2025, a Comissão especifique os termos e condições de aplicação dos motivos relacionados com a cibersegurança no que diz respeito ao adiamento da divulgação de notificações.

[1] Estas percentagens não têm em conta o facto de o mesmo inquirido ter apresentado quatro contributos diferentes.

REGULAMENTO DELEGADO (UE) …/... DA COMISSÃO

de 11.12.2025

que completa o Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, ao especificar os termos e condições de aplicação dos motivos relacionados com a cibersegurança no que diz respeito ao adiamento da divulgação de notificações

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o 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)[2], nomeadamente o artigo 14.º, n.º 9,

Considerando o seguinte:

(1) Em circunstâncias excecionais e, em especial, a pedido do fabricante e tendo em conta o grau de sensibilidade das informações notificadas, e por motivos justificados relacionados com a cibersegurança, a equipa de resposta a incidentes de segurança informática (CSIRT) designada como coordenadora que inicialmente recebeu a notificação de uma vulnerabilidade ativamente explorada ou de um incidente grave com impacto na segurança de um produto com elementos digitais (a seguir designada por «CSIRT que recebeu inicialmente a notificação») pode decidir adiar, por um período estritamente necessário, a divulgação da notificação através da plataforma única de comunicação de informações às CSIRT designadas como coordenadoras em cujo território o fabricante que apresenta a notificação indicou que o produto com elementos digitais foi disponibilizado (a seguir designadas por «CSIRT pertinentes»). Desta forma, é necessário estabelecer os termos e condições de aplicação desses motivos. Caso sejam aplicáveis, a CSIRT que recebeu inicialmente a notificação pode adiar a divulgação às CSIRT pertinentes por um período estritamente necessário, mas não é obrigada a fazê-lo. Nos termos do artigo 16.º, n.º 2, do Regulamento (UE) 2024/2847, se uma CSIRT que recebeu inicialmente a notificação decidir invocar esses motivos, deve informar imediatamente a Agência da União Europeia para a Cibersegurança (ENISA) da sua decisão de adiar a notificação, dos motivos que a levaram a fazê-lo e quando tenciona dar seguimento à divulgação da notificação.

(2) Em conformidade com o artigo 16.º, n.º 2, segundo parágrafo, do Regulamento (UE) 2024/2847, os termos e condições de aplicação dos motivos relacionados com a cibersegurança estabelecidos no presente regulamento não se aplicam ao acesso da ENISA às informações notificadas. O acesso da ENISA às informações notificadas só pode ser limitado em circunstâncias particularmente excecionais: se o fabricante indicar na sua notificação que está preenchida uma das três condições referidas no

[2] JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

artigo 16.º, n.º 2, terceiro parágrafo, alíneas a), b) ou c), do Regulamento (UE) 2024/2847, e apenas em relação à notificação de vulnerabilidade no prazo de 72 horas a que se refere o artigo 14.º, n.º 2, alínea b), do Regulamento (UE) 2024/2847. Nesses casos, as únicas informações a disponibilizar simultaneamente à ENISA são a informação de que o fabricante efetuou uma notificação; informações gerais sobre o produto com elementos digitais; informações sobre a natureza geral da exploração; e a informação de que foram invocados motivos relacionados com a segurança.

(3) O acesso às informações notificadas permite às CSIRT ter uma visão geral do ambiente de segurança no seu território e aplicar medidas de atenuação, aumentando o nível global de cibersegurança na União. Por conseguinte, só deverão ser possíveis mais restrições à divulgação de notificações devido à natureza das informações notificadas, nos casos em que, tendo em conta a sensibilidade das informações notificadas, os riscos de cibersegurança decorrentes do prosseguimento da divulgação superem os benefícios de segurança para a União e não possam ser adequadamente atenuados mediante a imposição de restrições ao tratamento e uma maior partilha da notificação através de protocolos específicos utilizados no âmbito da rede de CSIRT, como o protocolo «sinalização luminosa» para a partilha de informações (TLP) ou o protocolo de ações permitidas (PAP). Tal pode ocorrer, por exemplo, se um fabricante tiver informado a CSIRT que recebeu inicialmente a notificação de que espera apresentar em breve uma medida de atenuação (como uma correção). Tal pode igualmente ocorrer quando a CSIRT que recebeu inicialmente a notificação decide partilhar apenas partes de uma notificação, sendo essas partes, todavia, suficientes para que as CSIRT pertinentes possam assegurar a aplicação de medidas adequadas de atenuação dos riscos. Além disso, e para incentivar a cooperação na identificação e divulgação de vulnerabilidades entre os fabricantes, as CSIRT e os investigadores no domínio da segurança, tal pode ocorrer também quando a CSIRT atua como intermediária de confiança para um procedimento de divulgação coordenada de vulnerabilidades em curso, tal como referido no artigo 12.º, n.º 1, da Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho[3]. Nesse caso, quando a CSIRT decide adiar a divulgação de uma notificação, e em conformidade com o artigo 16.º, n.º 6, do Regulamento (UE) 2024/2847, pode adiá-la por um período que não exceda o estritamente necessário e até que as partes envolvidas na divulgação coordenada de vulnerabilidades deem o seu consentimento.

(4) As informações incluídas na notificação ajudarão as CSIRT a desempenhar as suas funções no contexto da atenuação dos riscos e do tratamento de incidentes. No entanto, em casos raros, essas informações podem ser suficientes para permitir a criação de uma técnica de exploração sem investigação adicional, mesmo por agentes com competências e recursos limitados. Se agentes mal-intencionados acedessem a essas informações, a cibersegurança da União seria fortemente afetada, dada a facilidade de exploração. Tal pode ser o caso, por exemplo, quando a versão vulnerável de um *software* difere apenas marginalmente das versões anteriores não vulneráveis. Nesses casos, se a CSIRT que recebeu inicialmente a notificação considerar que os riscos de cibersegurança decorrentes de uma maior divulgação não podem ser atenuados de

[3] 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).

forma adequada através da imposição de restrições ao tratamento e partilha posterior, pode decidir adiar a divulgação até que esteja disponível uma medida eficaz de atenuação dos riscos, como uma atualização de segurança ou orientações para os utilizadores.

(5) Se uma CSIRT pertinente não for capaz de proteger as informações notificadas de forma adequada, os agentes mal-intencionados podem aceder a informações sensíveis e explorar essas informações em todo o mercado único. Por conseguinte, caso existam preocupações sérias quanto à capacidade de uma CSIRT pertinente assegurar a confidencialidade das informações notificadas, a CSIRT que recebeu inicialmente a notificação pode decidir adiar a divulgação de uma notificação apenas a essa CSIRT pertinente até essas preocupações estarem resolvidas. Tal pode ocorrer quando uma CSIRT pertinente é alvo de um incidente de cibersegurança que afeta a sua capacidade de funcionar de forma segura ou quando existem provas ou informações de que foram detetadas deficiências significativas nas capacidades da CSIRT, tais como limitações graves de recursos que comprometam a sua capacidade de desempenhar as suas funções ou o recurso a *software* desatualizado ou vulnerável.

(6) Para evitar que agentes mal-intencionados acedam a informações sensíveis, caso a plataforma única de comunicação de informações criada ao abrigo do artigo 16.º do Regulamento (UE) 2024/2847 tenha sido comprometida por um incidente de cibersegurança, a CSIRT que recebeu inicialmente a notificação deve adiar a divulgação através da plataforma única de comunicação de informações até que a capacidade da plataforma para assegurar a confidencialidade das informações notificadas seja restabelecida.

(7) Em conformidade com o artigo 16.º, n.º 2, primeiro parágrafo, do Regulamento (UE) 2024/2847, a CSIRT que recebeu inicialmente a notificação não tem de divulgar uma notificação a qualquer outra CSIRT pertinente se o fabricante indicar que o produto com elementos digitais só é disponibilizado no mercado do Estado-Membro da CSIRT que recebeu inicialmente a notificação.

(8) A Comissão consultou e procurou obter os pontos de vista das partes interessadas pertinentes aquando da elaboração do projeto de ato delegado e consultou o Grupo de Peritos em Cibersegurança de Produtos com Elementos Digitais.

(9) Em conformidade com o artigo 14.º, n.º 9, do Regulamento (UE) 2024/2847, a Comissão cooperou estreitamente com a rede de CSIRT criada nos termos do artigo 15.º da Diretiva (UE) 2022/2555 e com a ENISA na elaboração do projeto de ato delegado,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Objeto

O presente regulamento especifica os termos e condições de aplicação dos motivos relacionados com a cibersegurança a que se refere o artigo 16.º, n.º 2, do Regulamento (UE) 2024/2847, que permitem à CSIRT designada como coordenadora que inicialmente recebeu uma notificação em conformidade com o artigo 14.º, n.os 1 e 3, e o artigo 15.º, n.os 1 e 2, desse regulamento, adiar a divulgação da notificação às CSIRT designadas como coordenadoras em cujo território o fabricante indicou que o produto com elementos digitais foi disponibilizado.

Artigo 2.º

Definições

Para efeitos do presente regulamento, entende-se por:

1) «CSIRT que recebeu inicialmente a notificação», a CSIRT designada como coordenadora que recebeu inicialmente a notificação nos termos do artigo 14.º, n.os 1 e 3, e do artigo 15.º, n.os 1 e 2, do Regulamento (UE) 2024/2847;

2) «CSIRT pertinente», a CSIRT designada como coordenadora em cujo território o fabricante indicou que o produto com elementos digitais foi disponibilizado.

Artigo 3.º

Termos e condições para a aplicação dos motivos relacionados com a cibersegurança decorrentes da natureza das informações comunicadas

A CSIRT que recebeu inicialmente a notificação pode decidir adiar por um período limitado ao estritamente necessário a divulgação de notificações, ou de partes destas, às CSIRT pertinentes, nos casos em que, tendo em conta a sensibilidade das informações notificadas, os riscos de cibersegurança decorrentes dessa divulgação superem os benefícios de segurança e não possam ser atenuados mediante a imposição de restrições ao tratamento e uma maior partilha da notificação através de protocolos adequados, como o protocolo «sinalização luminosa» para a partilha de informações (TLP) ou o protocolo de ações permitidas (PAP), ou se estiver preenchida pelo menos uma das seguintes condições:

a) O fabricante informou a CSIRT que recebeu inicialmente a notificação de que está prevista a disponibilização de uma medida eficaz de atenuação dos riscos, como uma atualização de segurança ou orientações para os utilizadores, no prazo de 72 horas; se não for disponibilizada uma medida eficaz de atenuação dos riscos dentro deste prazo, a CSIRT que recebeu inicialmente a notificação divulga a notificação às CSIRT pertinentes;

b) As informações incluídas na notificação são consideradas suficientes, tendo em conta a natureza da vulnerabilidade ativamente explorada notificada, para criar uma técnica de exploração, em especial quando a vulnerabilidade pode ser facilmente identificada e explorada por agentes com competências e recursos limitados; assim que estiver disponível uma medida eficaz de atenuação dos riscos, como uma atualização de segurança ou orientações para os utilizadores, a CSIRT que recebeu inicialmente a notificação divulga a notificação às CSIRT pertinentes;

c) A CSIRT que recebeu inicialmente a notificação está em condições de partilhar com as CSIRT pertinentes informações suficientes para assegurar que estas podem aplicar medidas adequadas de atenuação dos riscos; assim que estiver disponível uma medida eficaz de atenuação dos riscos, como uma atualização de segurança ou orientações para os utilizadores, a CSIRT que recebeu inicialmente a notificação divulga a notificação completa às CSIRT pertinentes;

d) A CSIRT que recebeu inicialmente a notificação da vulnerabilidade ativamente explorada foi informada da mesma no âmbito de uma divulgação coordenada de vulnerabilidades para a qual essa CSIRT atua como intermediária de confiança nos termos do artigo 12.º, n.º 1, da Diretiva (UE) 2022/2555; nesse caso, e em conformidade com o artigo 16.º, n.º 6, do Regulamento (UE) 2024/2847, a CSIRT que recebeu inicialmente a notificação divulga-a às CSIRT pertinentes quando um

adiamento já não for estritamente necessário e assim que as partes envolvidas na divulgação coordenada de vulnerabilidades derem o seu consentimento.

Artigo 4.º

Termos e condições para a aplicação dos motivos relacionados com a cibersegurança em relação a uma CSIRT específica

A CSIRT que recebeu inicialmente a notificação pode decidir adiar, por um período estritamente necessário, a divulgação das notificações, ou de partes das mesmas, a uma CSIRT pertinente específica, nos casos em que:

a) A CSIRT pertinente tenha sido afetada por um incidente de cibersegurança que ponha em causa a sua capacidade de assegurar a confidencialidade das informações notificadas;

b) Tenha motivos suficientes para crer que as capacidades da CSIRT pertinente são inadequadas para assegurar a confidencialidade das informações notificadas.

Nos casos a que se refere o primeiro parágrafo, alínea a), a CSIRT que recebeu inicialmente a notificação pode adiar a divulgação até que a CSIRT pertinente tenha informado a rede de CSIRT a que se refere o artigo 15.º da Diretiva 2022/2555 de que a sua capacidade para garantir a confidencialidade das notificações foi restabelecida.

Nos casos a que se refere o primeiro parágrafo, alínea b), a CSIRT que recebeu inicialmente a notificação pode adiar a divulgação à CSIRT pertinente até esta apresentar provas de que corrigiu as deficiências identificadas.

Artigo 5.º

Termos e condições para a aplicação dos motivos relacionados com a cibersegurança em relação à plataforma única de comunicação de informações

A CSIRT que recebeu inicialmente a notificação pode decidir adiar a divulgação das notificações através da plataforma única de comunicação de informações criada pelo artigo 16.º do Regulamento (UE) 2024/2847, caso a ENISA tenha informado a rede de CSIRT, nos termos do artigo 16.º, n.º 4, do referido regulamento, de que a plataforma única de comunicação de informações foi afetada por um incidente de cibersegurança que põe em causa a sua capacidade para assegurar a confidencialidade das informações notificadas. Nestes casos, a CSIRT que recebeu inicialmente a notificação pode adiar a divulgação através da plataforma única de comunicação de informações até que a ENISA tenha informado a rede de CSIRT de que a capacidade da plataforma para assegurar a confidencialidade das notificações foi restabelecida.

Artigo 6.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 11.12.2025

Pela Comissão
A Presidente
Ursula VON DER LEYEN