Съвет на
Европейския съюз

Брюксел, 17 декември 2025 г.
(OR. en)

16960/25

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

ПРИДРУЖИТЕЛНО ПИСМО

От:	Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор
Дата на получаване:	11 декември 2025 г.
До:	Г-жа Thérèse BLANCHET, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	C(2025) 8407 final
Относно:	ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) .../... НА КОМИСИЯТА от 11.12.2025 година за допълнение на Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета чрез определяне на реда и условията за прилагане на свързаните с киберсигурността основания за забавяне на разпространението на нотификациите

Приложено се изпраща на делегациите документ C(2025) 8407 final.

Приложение: C(2025) 8407 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 11.12.2025 г.
C(2025) 8407 final

ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) .../... НА КОМИСИЯТА

от 11.12.2025 година

за допълнение на Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета чрез определяне на реда и условията за прилагане на свързаните с киберсигурността основания за забавяне на разпространението на нотификациите

(текст от значение за ЕИП)

ОБЯСНИТЕЛЕН МЕМОРАНДУМ

1. КОНТЕКСТ НА ДЕЛЕГИРАНИЯ АКТ

Съгласно Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета (наричан по-нататък „Актът за киберустойчивост“) от производителите на продукти с цифрови елементи се изисква да уведомяват чрез единната платформа за докладване за всяка активно използвана уязвимост или всеки сериозен инцидент, който оказва въздействие върху сигурността на продукт с цифрови елементи. По силата на член 16, параграф 2 от посочения регламент определеният от държавата членка за координатор екип за реагиране при инциденти с компютърната сигурност (ЕРИКС), който първоначално получава нотификацията, може, при изключителни обстоятелства и поради основателни причини, свързани с киберсигурността, да отложи разпространението на нотификацията до ЕРИКС на други държави членки, в които е предоставен продуктът с цифрови елементи.

Поради това настоящият делегиран акт има за цел да допълни Акта за киберустойчивост, като определи реда и условията за прилагане на свързаните с киберсигурността основания за забавяне на разпространението на нотификациите. Това се постига чрез определянето на три вида основания, поради които ЕРИКС, който първоначално получава нотификацията, може да реши, че е необходимо да се отложи по-нататъшното разпространение до други ЕРИКС. Такова решение за забавяне може да бъде взето при някое от следните три изключителни обстоятелства:

- с оглед на оценка на естеството на нотифицираната информация;
- ако ЕРИКС, който получава нотификацията, не е в състояние да гарантира поверителността на съдържащата се в нея информация;
- ако единната платформа за докладване е била компрометирана или временно не функционира.

Предвижда се задълженията за докладване, определени в член 14 от Регламент (ЕС) 2024/2847, да започнат да се прилагат от 11 септември 2026 г.

2. КОНСУЛТАЦИИ ПРЕДИ ПРИЕМАНЕТО НА АКТА

По различни проекти на настоящия акт бяха проведени консултации с мрежата на ЕРИКС и с Агенцията на Европейския съюз за киберсигурност (ENISA). На 26 март 2025 г. беше проведено предварително обсъждане с насочващи въпроси, с възможност за предоставяне на писмен принос до 11 април 2025 г. Първият проект на настоящия акт беше представен на мрежата на ЕРИКС и на ENISA на 16 май 2025 г., а на 6 юни 2025 г. беше проведено обсъждане с възможност за предоставяне на писмен принос до 27 юни 2025 г. Вторият проект на акта беше представен на мрежата на ЕРИКС и на ENISA на 23 юли 2025 г., с възможност за предоставяне на писмен принос до 1 септември 2025 г. Третият проект на акта беше представен на мрежата на ЕРИКС и на ENISA на 25 септември 2025 г., а на 9 октомври 2025 г. беше проведено обсъждане с възможност за предоставяне на писмен принос до 27 октомври 2025 г.

Проектът на акта беше предмет на проведената между 16 октомври 2025 г. и 13 ноември 2025 г. обществена консултация, в рамките на която бяха получени 34 отговора от 31 отделни респонденти (отчитайки факта, че един от респондентите е изпратил обратна информация чрез 4 различни отговора). От тях 29,41 % са получени

от стопански асоциации, 26,47 % — от дружества/предприятия, 17,65 % — от граждани на ЕС, 14,71 % — от публични органи, 5,88 % — от неправителствени организации (НПО), 5,88 % — от академични/научноизследователски институции[1].

На 22 октомври проектът на акта беше обсъден и с експертната група по киберсигурността на продуктите с цифрови елементи (E03967), в която членуват органи на държавите членки, ENISA, отделни експерти, назначени в лично качество, и организации в широкия смисъл на думата (напр. дружества, сдружения, НПО).

3. ПРАВНИ ЕЛЕМЕНТИ НА ДЕЛЕГИРАНИЯ АКТ

Правомощието да се приемат делегирани актове е предвидено в член 14, параграф 9 от Акта за киберустойчивост, съгласно който от Комисията се изисква до 11 декември 2025 г. да определи реда и условията за прилагане на свързаните с киберсигурността основания за забавяне на разпространението на нотификациите.

[1] Тези проценти не отчитат факта, че един от респондентите е изпратил обратна информация чрез 4 различни отговора.

ДЕЛЕГИРАН РЕГЛАМЕНТ (ЕС) .../... НА КОМИСИЯТА

от 11.12.2025 година

за допълнение на Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета чрез определяне на реда и условията за прилагане на свързаните с киберсигурността основания за забавяне на разпространението на нотификациите

(текст от значение за ЕИП)

ЕВРОПЕЙСКАТА КОМИСИЯ,

като взе предвид Договора за функционирането на Европейския съюз,

като взе предвид Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета от 23 октомври 2024 г. относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Акт за киберустойчивост)[2], и по-специално член 14, параграф 9 от него,

като има предвид, че:

(1) При изключителни обстоятелства, по-специално по искане на производителя и с оглед на степента на чувствителност на нотифицираната информация, определеният за координатор екип за реагиране при инциденти с компютърната сигурност (ЕРИКС), който първоначално получава нотификация за активно използвана уязвимост или сериозен инцидент, оказващ въздействие върху сигурността на продукт с цифрови елементи (наричан по-нататък „ЕРИКС, който първоначално получава нотификацията“), може да вземе решение да отложи за период от време, който е строго необходим, разпространението на нотификацията чрез единната платформа за докладване до определените за координатори ЕРИКС, на чиято територия производителят, подаващ нотификацията, е посочил, че е предоставен продуктът му с цифрови елементи (наричани по-нататък „съответните ЕРИКС“). Поради това е необходимо да се определят редът и условията за прилагане на посочените основания. Когато се прилагат посочените основания, ЕРИКС, който първоначално получава нотификацията, има право да отложи разпространението ѝ до съответните ЕРИКС за период от време, който е строго необходим, но не е задължен да го направи. Съгласно член 16, параграф 2 от Регламент (ЕС) 2024/2847, когато ЕРИКС, който първоначално получава нотификацията, реши да се позове на посочените основания, той следва незабавно да информира Агенцията на Европейския съюз за киберсигурност (ENISA) за решението си и за причините, наложили забавянето, както и да посочи кога се предвижда по-нататъшното разпространение нотификацията.

(2) В съответствие с член 16, параграф 2, втора алинея от Регламент (ЕС) 2024/2847 редът и условията за прилагане на основанията, свързани с киберсигурността, посочени в настоящия регламент, не следва да се прилагат за достъпа на ENISA

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

до нотифицираната информация. Достъпът на ENISA до нотифицираната информация може да бъде ограничен само при изключителни обстоятелства: когато производителят посочва в нотификацията, че е изпълнено едно от трите условия, определени в член 16, параграф 2, трета алинея, буква а), б) или в) от Регламент (ЕС) 2024/2847, и то само във връзка със 72-часовата нотификация за уязвимост съгласно член 14, параграф 2, буква б) от горепосочения регламент. В такива случаи единствената информация, която се предоставя едновременно на ENISA, е информацията, че производителят е направил нотификация; обща информация за продукта с цифрови елементи; информация относно общия характер на използването; както и информацията, че е направено позоваване на основания, свързани с киберсигурността.

(3) Достъпът до нотифицираната информация предоставя на ЕРИКС възможността да разполагат с общи сведения относно средата на сигурност на съответните си територии, както и да могат да въвеждат смекчаващи мерки, с което се повишава цялостното равнище на киберсигурността в Съюза. Поради това допълнителни ограничения върху разпространението на нотификации с оглед на естеството на информацията, която се нотифицира, следва да бъдат възможни само в случаите, когато с оглед на чувствителността на нотифицираната информация рисковете за киберсигурността, произтичащи от по-нататъшното разпространение, надхвърлят ползите за сигурността на Съюза, като посочените рискове не могат да бъдат смекчени по подходящ начин чрез налагане на ограничения върху обработването и по-нататъшното споделяне на нотификацията чрез подходящи протоколи, използвани в рамките на мрежата на ЕРИКС, като например Протокола за обмен на информация с цветен код за поверителност (TLP) или Протокола за разрешените действия (PAP). Такъв може да бъде случаят например, когато производителят е информирал ЕРИКС, който първоначално получава нотификацията, че се очаква скоро да бъде предоставена мярка за смекчаване (като например софтуерна поправка). Такъв може да бъде и случаят, когато ЕРИКС, който първоначално получава нотификацията, реши да сподели само части от нея и въпреки това тези части са достатъчни, за да могат съответните ЕРИКС да гарантират, че са в състояние да въведат подходящи мерки за намаляване на риска. Освен това, както и за да се насърчи сътрудничеството в областта на идентифицирането и оповестяването на уязвимости между производителите, ЕРИКС и изследователите в областта на сигурността, такъв може да бъде също и случаят и когато ЕРИКС действа като доверен посредник за текуща процедура за координирано оповестяване на уязвимости, както е посочено в член 12, параграф 1 от Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета[3]. В този случай, в съответствие с член 16, параграф 6 от Регламент (ЕС) 2024/2847, когато ЕРИКС реши да отложи разпространението на нотификация, той трябва да я отложи за срок, не по-дълъг от строго необходимото, и докато не бъде дадено съгласие за оповестяване от участващите страни в координираното оповестяване на уязвимости.

(4) Информацията, включена в нотификацията, ще помогне на ЕРИКС да изпълняват задачите си в контекста на намаляването на риска и действията при

[3] Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 г. относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) № 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148 (Директива МИС 2) (ОВ L 333, 27.12.2022 г., стр. 80—152).

инциденти. В редки случаи обаче посочената информация може да бъде достатъчна, за да позволи дори на участници с ограничени умения и ресурси да разработят без допълнителни изследвания техника за използване на уязвимости. Ако злонамерени участници успеят да осъществят достъп до посочената информация, киберсигурността на Съюза ще бъде сериозно засегната, като се има предвид лесното ѝ използване. Такъв би могъл да бъде случаят например, когато уязвимата версия на даден софтуер се различава незначително от предишните, неуязвими версии. В такива случаи, ако ЕРИКС, който първоначално получава нотификацията, счете, че рисковете за киберсигурността, произтичащи от по-нататъшното разпространение, не могат да бъдат смекчени по подходящ начин чрез налагане на ограничения върху последващото обработване и споделяне, той може да реши да отложи разпространението, докато не бъде въведена ефективна мярка за намаляване на риска, като например актуализация на защитата или насоки за ползвателите.

(5) Ако съответният ЕРИКС не е в състояние да защити по подходящ начин нотифицираната информация, злонамерени участници могат да осъществят достъп до чувствителна информация и да разпространят експлойти в целия единен пазар. Поради това, когато са налице сериозни опасения относно способността на съответния ЕРИКС да гарантира поверителността на нотифицираната информация, ЕРИКС, който първоначално получава нотификацията, може да реши да отложи разпространението на нотификацията само до съответния ЕРИКС, докато тези опасения не бъдат отстранени. Такъв може да бъде случаят в ситуации, когато съответният ЕРИКС е бил засегнат от киберинцидент, който нарушава способността му да работи по сигурен начин, или когато има доказателства или информация, че са били установени значителни недостатъци в способностите на ЕРИКС, като сериозни ограничения на ресурсите, застрашаващи способността му да изпълнява функциите си, или използване на остарял или уязвим софтуер.

(6) В случай че единната платформа за докладване, създадена съгласно член 16 от Регламент (ЕС) 2024/2847, бъде компрометирана от киберинцидент, за да се предотврати достъпът на злонамерени участници до чувствителна информация, ЕРИКС, който първоначално получава нотификацията, следва да отложи разпространението чрез платформата, докато не бъде възстановена способността ѝ да гарантира поверителността на нотифицираната информация.

(7) В съответствие с член 16, параграф 2, първа алинея от Регламент (ЕС) 2024/2847 ЕРИКС, който първоначално получава нотификацията, не е необходимо да разпространява нотификация до друг съответен ЕРИКС, ако производителят посочи, че продуктът с цифрови елементи се предоставя на пазара само на държавата членка на ЕРИКС, който първоначално получава нотификацията.

(8) При изготвянето на проекта на делегиран акт Комисията проведе консултации и потърси становищата на съответните заинтересовани страни и се консултира с експертната група по киберсигурността на продуктите с цифрови елементи.

(9) В съответствие с член 14, параграф 9 от Регламент (ЕС) 2024/2847 при изготвянето на проекта на делегиран акт Комисията си сътрудничи тясно с мрежата на ЕРИКС, създадена съгласно член 15 от Директива (ЕС) 2022/2555, и с ENISA,

ПРИЕ НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Предмет

В настоящия регламент се определят редът и условията за прилагане на основанията, свързани с киберсигурността, посочени в член 16, параграф 2 от Регламент (ЕС) 2024/2847, които позволяват на определения за координатор ЕРИКС, който първоначално получава нотификация в съответствие с член 14, параграфи 1 и 3 и член 15, параграфи 1 и 2 от посочения регламент, да отложи разпространението на нотификацията до определените за координатори ЕРИКС, на чиято територия производителят е посочил, че е предоставен продуктът с цифрови елементи.

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „ЕРИКС, който първоначално получава нотификацията“ означава определеният за координатор ЕРИКС, който първоначално получава нотификацията в съответствие с член 14, параграфи 1 и 3 и член 15, параграфи 1 и 2 от Регламент (ЕС) 2024/2847;

2) „съответен ЕРИКС“ означава ЕРИКС, определен за координатор, на чиято територия производителят е посочил, че е предоставен продуктът с цифрови елементи.

Член 3

Ред и условия за прилагане на основанията, свързани с киберсигурността, произтичащи от естеството на нотифицираната информация

ЕРИКС, който първоначално получава нотификацията, може да реши да отложи за период от време, ограничен до строго необходимото, разпространението на нотификациите или на части от тях до съответните ЕРИКС в случаите, когато с оглед на чувствителността на нотифицираната информация рисковете за киберсигурността, породени от разпространението, надхвърлят ползите за сигурността, като тези рискове не могат да бъдат смекчени чрез налагане на ограничения върху обработването или по-нататъшното споделяне на нотификацията чрез подходящи протоколи, като например Протокола за обмен на информация с цветен код за поверителност (TLP) или Протокола за разрешени действия (PAP), и когато е изпълнено най-малко едно от следните условия:

а) производителят е информирал ЕРИКС, който първоначално получава нотификацията, че в рамките на 72 часа се очаква да бъде предоставена ефективна мярка за намаляване на риска, като например актуализация на защитата или насоки за ползвателите; ако в рамките на този срок не бъде предоставена ефективна мярка за намаляване на риска, ЕРИКС, който първоначално получава нотификацията, я разпространява до съответните ЕРИКС;

б) информацията, включена в нотификацията, се приема за достатъчна от гледна точка на естеството на активно използваната уязвимост за разработването на

техника за използване на уязвимости, особено когато уязвимостта може лесно да бъде идентифицирана и използвана от участници с ограничени умения и ресурси; след като бъде въведена ефективна мярка за намаляване на риска, като например актуализация на защитата или насоки за ползвателите, ЕРИКС, който първоначално получава нотификацията, я разпространява до съответните ЕРИКС;

в) ЕРИКС, който първоначално получава нотификацията, е в състояние да сподели със съответните ЕРИКС достатъчно информация, за да могат съответните ЕРИКС да гарантират, че са в състояние да въведат подходящи мерки за намаляване на риска; след като бъде въведена ефективна мярка за намаляване на риска, като например актуализация на защитата или насоки за ползвателите; ЕРИКС, който първоначално получава нотификацията, разпространява пълната нотификация до съответните ЕРИКС;

г) ЕРИКС, който първоначално получава нотификацията за активно използваната уязвимост, е уведомен за това като част от координирано оповестяване на уязвимости, за което посоченият ЕРИКС действа като доверен посредник в съответствие с член 12, параграф 1 от Директива (ЕС) 2022/2555; в този случай и в съответствие с член 16, параграф 6 от Регламент (ЕС) 2024/2847, ЕРИКС, който първоначално получава нотификацията, разпространява нотификацията до съответните ЕРИКС, когато отлагането вече не е строго необходимо и участващите страни в координираното оповестяване на уязвимости са дали съгласие за оповестяване.

Член 4

Ред и условия за прилагане на основанията, свързани с киберсигурността по отношение на конкретен ЕРИКС

ЕРИКС, който първоначално получава нотификацията, може да реши да отложи за период от време, който е строго необходим, разпространението на нотификациите или на части от тях до съответните ЕРИКС в случаите, когато:

а) съответният ЕРИКС е бил засегнат от киберинцидент, който поставя под съмнение способността му да гарантира поверителността на нотифицираната информация;

б) има достатъчно основания да смята, че способностите на съответния ЕРИКС са недостатъчни, за да се гарантира поверителността на нотифицираната информация.

В случаите, посочени в първа алинея, буква а) ЕРИКС, който първоначално получава нотификацията, може да отложи разпространението, докато съответният ЕРИКС не информира мрежата на ЕРИКС, посочена в член 15 от Директива 2022/2555, че способността му да гарантира поверителността на нотификациите е възстановена.

В случаите, посочени в първа алинея, буква б) ЕРИКС, който първоначално получава нотификацията, може да отложи разпространението до съответния ЕРИКС, докато съответният ЕРИКС не представи доказателства, че е отстранил установените недостатъци.

Член 5

Ред и условия за прилагане на основанията, свързани с киберсигурността, във връзка с единната платформа за докладване

ЕРИКС, който първоначално получава нотификацията, може да реши да отложи разпространението на нотификации чрез единната платформа за докладване, създадена с член 16 от Регламент (ЕС) 2024/2847, когато ENISA е информирала мрежата на ЕРИКС в съответствие с член 16, параграф 4 от посочения регламент, че единната платформа за докладване е била засегната от киберинцидент, който поставя под съмнение способността ѝ да гарантира поверителността на съобщената информация. В такива случаи ЕРИКС, който първоначално получава нотификацията, може да отложи разпространението чрез единната платформа за докладване, докато EINSA не информира мрежата на ЕРИКС, че способността на платформата да гарантира поверителността на нотификациите е възстановена.

Член 6

Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в *Официален вестник на Европейския съюз*.

Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на 11.12.2025 година.

За Комисията
Председател
Ursula VON DER LEYEN