Съвет на Европейския съюз

Брюксел, 22 май 2026 г.
(OR. en)

9399/26

LIMITE

CYBER 229
JAI 606
DATAPROTECT 161
TELECOM 239
MI 489
IND 342
CADREFIN 220
FIN 697
BUDGET 19
CSC 316
CODEC 937

Междуинституционални досиета:
2026/0011 (COD)
2026/0012 (COD)

БЕЛЕЖКА

От:	Генералния секретариат на Съвета
До:	Комитета на постоянните представители/Съвета
Относно:	Предложение за регламент на Европейския парламент и на Съвета относно Агенцията на Европейския съюз за киберсигурност (ENISA), Европейската рамка за сертифициране на киберсигурността и сигурността на веригите за доставки на ИКТ, както и за отмяна на Регламент (ЕС) 2019/881 (Акт за киберсигурността 2) Предложение за директива на Европейския парламент и на Съвета за изменение на Директива (ЕС) 2022/2555 по отношение на мерки за опростяване и привеждане в съответствие с [предложението за Акт за киберсигурността 2] - Доклад за напредъка

Председателството изготви доклад за напредъка по предложението за регламент на Европейския парламент и на Съвета относно Агенцията на Европейския съюз за киберсигурност (ENISA), Европейската рамка за сертифициране на киберсигурността и сигурността на веригите за доставки на ИКТ, както и за отмяна на Регламент (ЕС) 2019/881 (Акт за киберсигурността 2), за да докладва за работата, извършена от подготвителните органи на Съвета до момента, и за актуалното състояние на разглеждането на предложението.

ВЪВЕДЕНИЕ

1. На 20 януари 2026 г. Комисията предложи нов пакет за киберсигурността, чиято цел е да се укрепят устойчивостта и способностите на ЕС в областта на киберсигурността. Пакетът се състои от **регламент** относно Агенцията на Европейския съюз за киберсигурност (ENISA), Европейската рамка за сертифициране на киберсигурността и сигурността на веригите за доставки на информационни и комуникационни технологии (ИКТ) и отменя Регламент (ЕС) 2019/881 (Акт за киберсигурността). Този регламент (Акт за киберсигурността 2) се допълва от **директива** за изменение на Директива (ЕС) 2022/2555 (Директива МИС 2) по отношение на мерките за опростяване и привеждането в съответствие с [предложението за Акта за киберсигурността].

2. Преди предложението, в заключенията си относно ENISA от 6 декември 2024 г.[1] Съветът прикани Комисията да проучи и допълнително да засили ролята на ENISA в подкрепа на оперативното сътрудничество на равнището на ЕС и между държавите членки за повишаване на киберустойчивостта, като се вземат предвид компетентностите на държавите членки в тази област. Също така Комисията беше призована да осигури целенасочен и ясно определен мандат на ENISA в подкрепа на държавите членки, с конкретни стратегически цели и приоритетни задачи, както и по-прецизно разпределение на задачите и компетентностите по отношение на други участници. Освен това Съветът настойчиво прикани Комисията да използва оценката на Акта за киберсигурността, за да намери начини за по-опростен, основан на риска, както и по-прозрачен и по-бърз подход към разработването на схеми на ЕС за сертифициране на киберсигурността. В допълнение към това, в заключенията си[2] от 21 май 2024 г. относно бъдещето на киберсигурността Съветът подчерта ангажимента си за гарантиране на сигурни вериги за доставки на ИКТ и изтъкна значението на нетехническите рискови фактори, включително неправомерното въздействие на трети държави върху доставчиците и доставчиците на услуги. И накрая, в заключенията на Съвета[3] от 17 октомври 2022 г. относно сигурността на веригите за доставки на ИКТ беше подчертана необходимостта от укрепване на устойчивостта и сигурността на веригите за доставки на ИКТ, като се имат предвид въздействието на геополитическото напрежение и зависимостта от продукти и услуги, свързани с ИКТ.

---

1 16527/24.
2 10133/24.
3 13664/22.

3. Целта на предложението за регламент, което се основава на член 114 от ДФЕС, е да се укрепи рамката на Съюза в областта на киберсигурността. С него се засилват ролята и задачите на Агенцията на Европейския съюз за киберсигурност (ENISA) да подпомага държавите членки и органите на Съюза, за да се постигне високо равнище на киберсигурност, устойчивост и доверие в Съюза. Предложението има за цел да направи Европейската рамка за сертифициране на киберсигурността по-ефективна и по-ефикасна, за да се даде възможност за ускорено разработване и прилагане на схеми. С предложението се създава и надеждна рамка на Съюза за сигурност на веригите за доставки на ИКТ, като се разглеждат нетехническите рискови фактори и зависимостите, засягащи сигурността на критичната инфраструктура и услуги в областта на ИКТ. Предложението е съпътствано от целенасочени мерки, свързани с прилагането на Директивата МИС 2[4] и насочени към опростяване на изискванията за съответствие, намаляване на ненужната административна тежест и повишаване на правната яснота.

4. Предложението е включено като една от приоритетните цели с осезаеми резултати в пътната карта „Една Европа, един пазар“[5], подписана в рамките на неформалната среща на държавните и правителствените ръководители в Кипър на 24 април 2026 г.

5. Европейският парламент определи г-жа Маркета Грегорова (Зелени/ЕСА) за докладчик на водещата комисия по промишленост, изследвания и енергетика (ITRE).

6. На 29 април 2026 г. Европейският икономически и социален комитет прие становището си по предложението[6].

---

4 ОВ L 333, 27.12.2022 г., стр. 80.
5 8473/26.
6 8980/26.

АКТУАЛНО СЪСТОЯНИЕ НА РАБОТАТА В РАМКИТЕ НА ПОДГОТВИТЕЛНИТЕ ОРГАНИ НА СЪВЕТА

7. На заседанието на Хоризонталната работна група по въпроси на кибернетичното пространство (HWPCI) от 26 януари 2026 г. и на заседанието на Комитета на постоянните представители от 28 януари 2026 г. беше направено общо представяне на пакета за киберсигурността.

8. HWPCI започна обсъждането на предложението на 2 февруари 2026 г. с подробно представяне от Комисията. По време на това представяне Комисията представи също констатациите от доклада за оценка, финансовата обосновка и оценката на въздействието.

9. HWPCI започна прочит на предложения регламент на 23 февруари 2026 г.

10. Държавите членки приветстваха предложението и като цяло подкрепиха общите му цели, по-специално засилването на подкрепата на ENISA за оперативното сътрудничество между държавите членки и рационализирането на рамката за сертифициране. Обсъжданията обаче показаха също, че е необходимо няколко аспекта на предложението да бъдат допълнително разгледани. Делегациите поискаха допълнителни разяснения относно засилената оперативна роля и задачи, предвидени за ENISA, например издаването на ранни предупреждения, създаването на бюро за помощ във връзка със софтуера за изнудване и ролята на ENISA в мрежата на ЕРИКС. Няколко делегации поставиха под въпрос отражението върху ресурсите за държавите членки, свързано с предложеното предоставяне на двама командировани национални експерти (КНЕ) от всяка държава членка, които да подпомагат изпълнението на задачите на ENISA. Правилата за гласуване в управителния съвет също трябва да бъдат допълнителни обсъдени. Делегациите изтъкнаха, че са необходими по-голяма яснота и точност по отношение на използваните в предложението определения и понятия. Съставът на бюджета на ENISA, по-специално събирането на такси, също се нуждаеше от допълнителни разяснения.

11. Новите разпоредби за повишаване на ефективността и ефикасността на процеса на сертифициране като цяло бяха приветствани, въпреки че беше установена обща необходимост държавите членки да участват повече в целия процес на сертифициране. Доброволният характер на сертифицирането като цяло беше приветстван. Делегациите обаче поставиха под въпрос някои от предложените срокове съгласно рамката за сертифициране.

12. При обсъжданията на надеждната рамка за веригите за доставки на ИКТ бяха изтъкнати няколко опасения от държавите членки. Делегациите призоваха за допълнителни разяснения относно методиката и процедурите за определяне на ключовите ИКТ активи и високорисковите доставчици, както и относно обхвата и възможното въздействие на предложените мерки. Делегациите подчертаха, че е важно да се осигури подходящо равнище на участие на държавите членки.

13. Няколко делегации внесоха резерви за разглеждане по различни части на предложението, по-специално във връзка с аспектите на управлението, използването на актове за изпълнение и предложения механизъм за определяне на високорискови доставчици и сигурността на веригите за доставки на ИКТ.

14. След обсъжданията в HWPCI държавите членки бяха приканени да представят писмени бележки по разпоредбите, свързани с дял I относно общите разпоредби и дял II относно ENISA. Общо 23 държави членки представиха становища. По-късно държавите членки бяха приканени да представят писмени бележки по дял III относно Европейската рамка за сертифициране на киберсигурността. Общо 20 държави членки използваха възможността да представят своите позиции в писмен вид.

15. Въз основа на тези писмени становища от държавите членки и на работата в HWPCI председателството ще изготви компромисен текст по дял II (ENISA) и дял III (Европейска рамка за сертифициране на киберсигурността), който ще бъде представен на заседанието на HWPCI в началото на юни 2026 г.

16. Няколко държави членки поискаха от Правната служба на Съвета да разгледа целесъобразността на правното основание.

17. Председателството ще започне прочита на текста относно мерките за опростяване на Директивата МИС2 в края на май 2026 г.

18. Като цяло се очаква HWPCI да проведе общо 15 заседания, посветени на предложението за Законодателен акт за киберсигурността 2, по време на кипърското председателство.

19. Въз основа на напредъка, постигнат от кипърското председателство, встъпващото ирландско председателство планира да продължи работата по това важно досие.

20. В контекста на изложеното по-горе Комитетът на постоянните представители и Съветът се приканват да вземат предвид напредъка, постигнат в разглеждането на предложението за регламент.