Съвет на Европейския съюз

Брюксел, 22 януари 2026 г.
(OR. en)

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

**5611/26**
**ADD 2**

**CYBER 29**
**JAI 85**
**DATAPROTECT 22**
**TELECOM 29**
**MI 58**
**IND 48**
**CADREFIN 26**
**FIN 100**
**BUDGET 3**
**CODEC 90**

**ПРИДРУЖИТЕЛНО ПИСМО**

| | |
|---|---|
| От: | Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор |
| Дата на получаване: | 21 януари 2026 г. |
| До: | Г-жа Thérèse BLANCHET, генерален секретар на Съвета на Европейския съюз |
| № док. Ком.: | SWD(2026) 12 final |
| Относно: | РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА<br>РЕЗЮМЕ НА ДОКЛАДА ЗА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО, […]<br>придружаващ<br>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)<br>и<br>Предложение за Директива на Европейския парламент и на Съвета за изменение на Директива (ЕС) 2022/2555 по отношение на мерките за опростяване и привеждане в съответствие с [Предложение за Акт за киберсигурността 2] |

Приложено се изпраща на делегациите документ SWD(2026) 12 final.

Приложение: SWD(2026) 12 final

ЕВРОПЕЙСКА
КОМИСИЯ

Страсбург, 20.1.2026 г.
SWD(2026) 12 final

**РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА**

**РЕЗЮМЕ НА ДОКЛАДА ЗА ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО,**

[…]

***придружаващ***

**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)**

**и**

**Предложение за Директива на Европейския парламент и на Съвета за изменение на Директива (ЕС) 2022/2555 по отношение на мерките за опростяване и привеждане в съответствие с [Предложение за Акт за киберсигурността 2]**

{COM(2026) 11 final} - {SEC(2026) 11 final} - {SWD(2026) 11 final}

# Обобщена оценка на въздействието

## Цел

Основната цел на настоящата оценка на въздействието е да се оцени дали в настоящите разпоредби са предвидени адекватни мерки във връзка с развиващите се заплахи за киберсигурността в целия ЕС. В нея се предлага интегриран набор от варианти на политиката, насочен към укрепване на Агенцията на Европейския съюз за киберсигурност (ENISA), реформиране на Европейската рамка за сертифициране на киберсигурността (ЕРСК) и опростяване на съответствието със съществуващата законодателна рамка в областта на киберсигурността. В настоящата оценка се подчертава колко е важно да се модулира управлението на киберпространството с цел хармонизиране с технологичния напредък и търсенето на пазара, като същевременно се гарантира конкурентоспособността и се отчита въздействието върху околната среда.

## Описание на проблема

Въпреки полаганите усилия обстановката по отношение на киберсигурността в ЕС продължава да се характеризира със значителни предизвикателства в контекста на все по-сложни заплахи. Недостатъчната координация между държавите членки и други участници на равнището на ЕС забави въвеждането на инструментите на политиката, а регулаторните пречки и сложността затрудняват ефективното управление на киберсигурността. Тези проблеми пораждат увеличени разходи за предприятията и публичните органи, повишават рисковете от киберинциденти и водят до непоследователни нива на защита на гражданите.

## Обосновка на необходимостта от действие на равнище ЕС

Заплахите за киберсигурността надхвърлят националните граници; поради това прилагането на единен подход е изключително важно за осигуряването на надежден отговор. С намесата на равнището на ЕС се гарантира последователна защита, повишава се конкурентоспособността чрез осигуряване на еднакви условия на конкуренция и се улеснява свободното движение на цифрови услуги и продукти в рамките на единния пазар. Освен това с хармонизирането на равнището на ЕС се намалява административната тежест чрез опростено съответствие и рационализирани процедури.

## Варианти на политиката и предпочитан вариант

В настоящия доклад се анализират четири области на намеса, като във всяка се разглежда набор от варианти на политиката с оглед на постигането на специфичните цели: 1) мандатът на ENISA (също част от действащия Акт за киберсигурността); 2) ЕРСК (също част от действащия Акт за киберсигурността) и 3) целенасочени изменения на Директивата МИС 2 с цел опростяване, които същевременно са тясно свързани с мандата на ENISA и ЕРСК. Всеки от тези набори от варианти представлява самостоятелна област на намеса, като същевременно те са тясно свързани и относими помежду си.

***Варианти за преодоляване на несъответствията в политическата рамка на ЕС за киберсигурност и нуждите на заинтересованите страни в условията на все по-враждебна среда***

Вариант А.1: *Уточняване на мандата на ENISA и въвеждане на приоритизация* — с този вариант се гарантира ясна и стабилна рамка за задачите на ENISA чрез включване на задачите, произтичащи от други законодателни актове.

Вариант А.2: *Реформа на мандата на ENISA* — при този вариант се отменя и заменя Актът за киберсигурността, като се извършва цялостно преструктуриране на мандата на Агенцията.

Вариант А.3: *Реформа на мандата на ENISA със силен акцент върху оперативната подкрепа* — с този вариант се надгражда вариант А.2. В допълнение се предвижда ENISA да разработи способности да оказва пряка подкрепа, по искане на държава членка, на субектите по Директивата МИС 2 при реагиране и възстановяване след инциденти в областта на киберсигурността.

***Варианти за Европейската рамка за сертифициране на киберсигурността***

Вариант Б.1: *Уточняване на обхвата, елементите и целите на ЕРСК и въвеждане на механизъм за поддържане* — при този вариант се предвижда създаването на нов механизъм за поддържане на схемите след приемането им, като това трябва да се извърши от ENISA.

Вариант Б.2: *Реформиране на ЕРСК чрез преразглеждане на процедурите и разширяване на обхвата, за да бъде улеснено опростяването във връзка със спазването на регулаторните изисквания* — при този вариант Актът за киберсигурността ще бъде отменен и заменен с нов регламент. В допълнение към вариант Б.1 ще бъдат преразгледани процедурите, свързани с искането, разработването и приемането на схемите, с цел повишаване на отчетността и ефективността.

Вариант Б.3: *Реформиране на ЕРСК, както е предвидено във вариант Б.2, и въвеждане на задължително сертифициране за състоянието на киберсигурността* — при този вариант се надгражда вариант Б.2, но целта е да се укрепи допълнително въздействието на рамката чрез въвеждане на задължително сертифициране на съществени субекти, обхванати от Директивата МИС 2, като се вземат под внимание конкретни рискови сценарии, вместо да се разчита единствено на доброволното сертифициране на субектите.

***Варианти за опростяване***

Вариант В.1: *Подход на актове с незадължителен характер и незаконодателни инструменти, включително използване на съществуващите оправомощавания (приемане на актове за изпълнение съгласно член 21, параграф 5 и член 23, параграф 11 от Директивата МИС 2)* — при този вариант се предвижда приемане на актове за изпълнение съгласно съществуващите инструменти за оправомощаване по Директивата МИС 2, за да се осигури по-висока степен на хармонизиране на мерките за управление

на рисковете в областта на киберсигурността, на праговете във връзка със задълженията за докладване на инциденти, както и на информацията, форматите и процедурите за уведомяване, успоредно с приемането на набор от насоки с цел повишаване на правната сигурност и хармонизираното прилагане.

Вариант В.2: *Целенасочена намеса — допълнително опростяване на съответствието с приложимата законодателна рамка на Съюза за киберсигурността* — при този вариант се осъществява ограничена намеса чрез изменения в Акта за киберсигурността и Директивата МИС 2 с цел опростяване на конкретни аспекти на рамката за киберсигурност, включително адаптиране на обхвата, въвеждане на максимална степен на хармонизиране за актовете за изпълнение, доказване на съответствието чрез сертифициране и приемане на набора от насоки, предвиден във вариант В.1.

Вариант В.3: *Хармонизиране на предвидените в законодателството на Съюза мерки във връзка с киберсигурността* — при този вариант се надгражда вариант В.2 и се предвижда премахване на всички мерки за управление на рисковете в областта на киберсигурността или на инструментите за оправомощаване, свързани с мерки, включени в секторното законодателство. Вместо това екосистемата на Директивата МИС 2 ще бъде изменена, за да се въведат рационализирани изисквания за всички категории субекти, като по този начин се гарантира по-висока степен на хармонизиране.

## *Варианти за сигурността на веригите за доставки на ИКТ*

Вариант Г.1: *Подход на актове с незадължителен характер за справяне с рисковете в областта на киберсигурността във веригите за доставки на ИКТ* — при този вариант не се предвижда регулаторна намеса на равнището на ЕС. Вместо това Комисията ще увеличи броя на координираните оценки на риска и наборите от инструменти на доброволна основа.

Вариант Г.2: *Ad hoc регулаторна намеса чрез кодифициране на инструментариума в областта на 5G* — при този вариант се предвижда кодифициране на мерките от инструментариума в областта на 5G. С него се въвежда задължение за държавите членки да гарантират, че не се използват компоненти от високорискови доставчици в ключови активи на мрежата.

Вариант Г.3: *Всеобхватна и хоризонтална рамка за справяне с рисковете за киберсигурността на веригите за доставки на ИКТ* — при този вариант се създава хоризонтална, технологично и секторно неутрална регулаторна рамка за справяне с нетехническите рискове за киберсигурността на веригите за доставки на ИКТ.

***След задълбочен анализ предпочитаният пакет на политиката включва:*** вариант А.2 — Реформа на мандата на ENISA; вариант Б.2 — Реформиране на ЕРСК чрез преразглеждане на процедурите и разширяване на обхвата, за да бъде улеснено спазването на регулаторните изисквания, вариант В.2 — Целенасочена намеса — допълнително опростяване на съответствието с приложимата законодателна рамка на

Съюза за киберсигурността и вариант Г.3 — Всеобхватна и хоризонтална рамка за справяне с рисковете за киберсигурността на веригите за доставки на ИКТ.

Тази комбинация предлага добре балансиран отговор на установените предизвикателства пред политиките, като значително повишава ефективността, ефикасността и съгласуваността в целия Съюз.

**Основни въздействия**

**Анализ на разходите и ползите:** преходът към предложената регулаторна рамка ще породи разходи както за ENISA, които се оценяват на до 161,3 милиона евро за период от пет години и са свързани с изпълнението на новите ѝ задачи, така и до разходи за публичните органи в целия ЕС, които се оценяват на до 80 милиона евро за период от пет години (като се отчитат и съответните икономии на разходи) и са свързани с осъществяването на надзор. По отношение на предприятията по време на тригодишния преходен период поетапното извеждане от употреба на специфично високорисково оборудване би могло да доведе до годишни разходи в размер на 3,4—4,3 милиарда евро за операторите на мобилни мрежи, като едновременно с това инвестициите в надеждни доставчици биха могли да нараснат до 2 милиарда евро годишно. Освен това се очаква рационализирането и намаляването на задълженията за спазване на изискванията да насърчат икономии на разходите за предприятията в размер до 14,6 милиарда евро. В допълнение към това подобряването на цялостното състояние на киберсигурността на ЕС и на технологичния му суверенитет и стимулирането на иновациите и конкурентоспособността ще породят значителни ползи за гражданите, публичните органи и бизнеса, като в дългосрочен план се очаква те до голяма степен да компенсират първоначалните разходи.

***Конкурентоспособност:*** чрез намаляване на разпокъсаността на пазара и хармонизиране на разпоредбите с предпочитаните варианти се засилва равнопоставеността при конкуренцията в целия ЕС, като на предприятията се осигуряват по-ясни и предвидими пътища за спазване на изискванията и за иновации.

***Проверка на съответствието по отношение на климата:*** в оценката беше проучено потенциалното въздействие на всеки вариант върху околната среда. Специално внимание беше обърнато на енергийната ефективност, на свързаните с пътуванията емисии и на консолидирането на инфраструктурата. Предпочитаните варианти А.2, Б.2 и В.2 оказват ограничено въздействие върху околната среда, докато вариант Г.3 е неутрален по отношение на околната среда, като се отчитат жизненият цикъл на продуктите и преходните периоди за замяна на ключови активи. Това е съгласувано с ангажимента на ЕС за устойчивост.

***Цифрови по подразбиране:*** акцентът върху оптимизираните цифрови процеси е свидетелство за ангажимента на ЕС да прилага подход с „предимство за цифровите технологии“, при който се осигурява по-бърз и по-надежден обмен на данни и вземане на решения. Вариант Г.3 би могъл да окаже значително въздействие и върху цифровизацията, тъй като в него се предвижда замяната на компоненти на субекти,

установени в трети държави или контролирани от субекти от трети държави, пораждащи опасения за киберсигурността.

***Опростяване и намаляване на тежестта:*** предпочитаните варианти допринасят за опростяването посредством въвеждането на пояснения на обхвата и на мерки за рационализиране на съответствието и надзора, с които се намалява административната тежест. Отчетен е принципът на отмяна на предишни тежести при въвеждане на нови, като се гарантира, че новите задължения се компенсират с намаления в други области.

**Заключение**

С настоящата оценка на въздействието се представя всеобхватна стратегия за повишаване на киберсигурността на ЕС, преодоляване на регулаторната неефективност и подготовка на цифровата среда за бъдещи предизвикателства. В нея се препоръчва подход на сътрудничество и съгласуване, при който реформите на политиката се основават на съществуващите рамки при същевременно адаптиране към новата технологична реалност. Чрез тези мерки ЕС има за цел да гарантира издръжлива, конкурентоспособна и устойчива цифрова икономика.