Съвет на
Европейския съюз

Брюксел, 29 март 2022 г.
(OR. en)

7670/22
ADD 7

Междуинституционално досие:
2022/0084(COD)

CSC 128
CSCI 45
CYBER 100
INST 99
INF 40
CODEC 385
IA 34

ПРИДРУЖИТЕЛНО ПИСМО

От:	Генералния секретар на Европейската комисия, подписано от г-жа Martine DEPREZ, директор
Дата на получаване:	22 март 2022 г.
До:	Г-н Jeppe TRANHOLM-MIKKELSEN, генерален секретар на Съвета на Европейския съюз
№ док. Ком.:	SWD(2022) 65 final
Относно:	РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА РЕЗЮМЕ НА ДОКЛАДА ОТ ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО придружаващ Предложение за Регламент на Европейския парламент и на Съвета относно информационната сигурност в институциите, органите, службите и агенциите на Съюза

Приложено се изпраща на делегациите документ SWD(2022) 65 final.

Приложение: SWD(2022) 65 final

ЕВРОПЕЙСКА
КОМИСИЯ

Брюксел, 22.3.2022 г.
SWD(2022) 65 final

РАБОТЕН ДОКУМЕНТ НА СЛУЖБИТЕ НА КОМИСИЯТА

РЕЗЮМЕ НА ДОКЛАДА ОТ ОЦЕНКАТА НА ВЪЗДЕЙСТВИЕТО

придружаващ

Предложение за Регламент на Европейския парламент и на Съвета

относно информационната сигурност в институциите, органите, службите и агенциите на Съюза

{COM(2022) 119 final} - {SWD(2022) 66 final}

Резюме

Оценка на въздействието върху информационната сигурност в институциите, органите, службите и агенциите на Съюза

А. Политически контекст

Стратегическата програма на Европейския съвет за периода 2019—2024 г. призовава институциите да защитават информационните и комуникационните мрежи на ЕС и процесите на вземане на решения от всякакъв вид злонамерени действия, включително киберзаплахи и хибридни заплахи. Вследствие на това през декември 2019 г. Съветът по общи въпроси заключи, че институциите и органите на ЕС следва да разработят и въведат цялостен набор от мерки за гарантиране на своята информационна сигурност.

През юли 2020 г. Комисията прие своята Стратегия на ЕС за Съюза на сигурност, с която се ангажира да допълни националните усилия в областта на сигурността. Като част от тази стратегия Комисията предложи да бъде изготвен минимален набор от правила относно информационната сигурност и киберсигурността във всички институции и органи на Съюза.

Б. Какъв е проблемът?

Основните проблеми са следните: i) значителна разлика между нивото на сигурност в институциите и органите на Съюза в зависимост от техните вътрешни правила за сигурност и ii) липса на координация между институциите и органите на Съюза при изпълнението на техните задачи в областта на сигурността.

Институциите и органите на Съюза имат свои собствени правила за информационна сигурност или изобщо не са приели такива правила. Разпокъсаността на действащата правна рамка доведе до наличието на различни категории некласифицирана информация, различни обозначения и инструкции за боравене. Колкото до класифицираната информация на ЕС, оперативната съвместимост на съответните системи продължава да е ограничена, което възпрепятства безпроблемното предаване на информация между институциите и органите и с държавите членки.

Тази ситуация увеличава риска нападатели да предизвикат нарушение на сигурността в най-слабата връзка и да го използват като отправна точка за още нападения срещу други институции или органи.

В. Какво следва да бъде постигнато?

Общата цел на инициативата е да се създадат правила за информационна сигурност за всички институции и органи на Съюза, за да се гарантира засилена и последователна защита срещу променящите се заплахи за тяхната информация.

Общата цел се изразява в четири конкретни цели:

- Създаване на хармонизирани и изчерпателни категории информация
- Установяване на пропуски в сигурността и прилагане на необходимите мерки
- Установяване на гладко сътрудничество относно информационната сигурност в

институциите и органите на Съюза
- Модернизиране на политиките за информационна сигурност, като се вземат предвид цифровата трансформация и работата от вкъщи

Г. Какви са мненията на различните заинтересовани страни?

Консултираните заинтересованите страни (институциите и органите на Съюза, националните органи на държавите членки по сигурността и експерти от JRC) постигнаха съгласие относно необходимостта от общи стандарти за информационна сигурност за всички институции и органи на Съюза с акцент върху следните въпроси:

- Следва да се вземат предвид разнообразието и различната бизнес среда във всяка институция или орган на Съюза и следва да се позволи решение на местно равнище;
- Макар по-голямата част от институциите и органите да са готови да си сътрудничат със своите колеги в общи органи за целите на информационната сигурност, те не желаят да делегират своите правомощия за вземане на решения;
- Проектът за регламент следва да бъде изготвен при зачитане на междуправителственото споразумение[1] на държавите членки относно защитата на класифицираната информация.

Д. Какво е въздействието на предложението?

Ползи

Чрез създаването на базови правила за информационна сигурност във всички институции и органи на Съюза проектът за регламент ще повиши общите равнища на информационна сигурност, като същевременно ще намали наличните несъответствия. Той ще спомогне за премахването на потенциални слаби връзки, като същевременно защитава информацията, споделяна в рамките на европейската администрация.

От гледна точка на ефективността проектът за регламент следва да доведе до ползи от координираното изпълнение на общи задачи в областта на информационната сигурност (напр. разрешения за достъп до информация, акредитация на комуникационни и информационни системи) и създаването на общи органи за управление (напр. междуинституционалната координационна група, техническите подгрупи).

Икономически последици

За институциите и органите на Съюза се очаква усилията, необходими за прилагането на новото законодателство, да бъдат компенсирани от повишаването на ефективността, като същевременно допълнителните разходи могат да бъдат покрити в рамките на съществуващите програми за подобряване на информационната сигурност на всяка организация. В дългосрочен план те ще спечелят от последователния подход за справяне с постоянно променящите се заплахи за информационната сигурност.

[1] Споразумение между държавите членки на Европейския съюз, заседаващи в рамките на Съвета, относно защитата на класифицирана информация, която се обменя в интерес на Европейския съюз, 2011/C202/05

Европейската комисия следва да осигури постоянния секретариат на междуинституционалната координационна група и да отпусне човешки ресурси за тази задача (един служител степен AD и един служител степен AST). На равнището на администрациите на държавите членки и на частния сектор не се очакват икономически последици.
Е. Последващи действия
Кога ще се извърши преглед на политиката?
На всеки 5 години след датата на прилагане ще се извършва цялостна оценка, за да се преценят последиците и прилагането на проекта за регламент. Комисията представя доклад с констатациите си и го внася до Европейския парламент и на Съвета.