Становище на Европейския икономически и социален комитет относно „Предложение за регламент на Европейския парламент и на Съвета относно хоризонтални изисквания за киберсигурност за продукти с цифрови елементи и за изменение на Регламент (ЕС) 2019/1020“

(COM(2022) 454 final — 2022/0272 (COD))

(2023/C 100/15)

Докладчик: **Maurizio MENSI**

Съдокладчик: **Marinel Dănuț MURESAN**

Искане за консултация	Европейски парламент, 9.11.2022 г.
	Съвет на Европейския съюз, 28.10.2022 г.
Правно основание	Член 114 от Договора за функционирането на Европейския съюз
Компетентна секция	„Единен пазар, производство и потребление“
Приемане от секцията	10.11.2022 г.
Приемане на пленарна сесия	14.12.2022 г.
Пленарна сесия №	574
Резултат от гласуването	
(„за“/„против“/„въздържал се“)	177/0/0

1. **Заключения и препоръки**

1.1. ЕИСК приветства предложението на Комисията за законодателен акт за киберустойчивост (ЗАК) за определяне на по-високи стандарти за киберсигурност, с които да се създаде надеждна система за икономическите оператори и да се гарантира за гражданите на ЕС безопасното използване на продуктите на пазара. Това е инициатива, която е част от европейската стратегия за данните, чрез която се повишава сигурността на данните, включително личните данни, и основните права, които са съществени предпоставки за нашето цифрово общество.

1.2. ЕИСК счита, че е от съществено значение да се засили колективният отговор на кибератаките и да се консолидира процесът на хармонизиране в областта на киберсигурността на национално равнище по отношение на оперативните правила и инструменти, за да се избегне създаването на правна несигурност и юридически пречки чрез наличието на диференцирани национални подходи.

1.3. ЕИСК приветства инициативата на Комисията, която не само ще спомогне за намаляване на значителните разходи за предприятията, причинени от кибератаки, но и ще даде възможност на гражданите/потребителите да се възползват от по-добра защита на основните си права, като например поверителността на личните данни. По-специално Комисията показва, че взема предвид специфичните нужди на МСП по отношение на дейностите на сертифициращите органи; при все това ЕИСК посочва необходимостта от изясняване на критериите, които следва да бъдат прилагани.

1.4. ЕИСК счита за важно да се подчертае, че макар, от една страна, да е похвално, че Законодателният акт за киберустойчивост на практика обхваща почти всички цифрови продукти, от друга страна може да възникнат проблеми при практическото му прилагане, като се има предвид обемната и сложна дейност за проверка и контрол, която той предвижда. Оттук произтича необходимостта от укрепване на инструментите за мониторинг и проверка.

1.5. ЕИСК отбелязва необходимостта от точно изясняване на материалния обхват на ЗАК, по-специално по отношение на продуктите с цифрови елементи и софтуер.

1.6. ЕИСК отбелязва, че производителите ще бъдат задължени да докладват, от една страна, за уязвимостите на продуктите, и от друга — за всички инциденти, свързани със сигурността, като информират агенцията на Европейския съюз за киберсигурност (ENISA). В това отношение е важно на агенцията да бъдат предоставени необходимите ресурси за навременно и ефективно изпълнение на съответните и чувствителни задачи, които ще ѝ бъдат възложени.

1.7. За да се избегне всякаква несигурност при тълкуването, ЕИСК предлага Комисията да изготви насоки, които да ориентират производителите и потребителите относно конкретните приложими правила и процедури, тъй като изглежда, че редица продукти, попадащи в обхвата на предложението, са предмет и на други законодателни актове в областта на киберсигурността. В това отношение би било важно по-специално МСП и ММСП да имат достъп до квалифицирана експертна подкрепа, която да може да предоставя специфични професионални услуги.

1.8. ЕИСК отбелязва, че не са напълно изяснени отношенията между сертифициращите органи съгласно ЗАК, и други органи, оправомощени да сертифицират киберсигурността по силата на други законодателни разпоредби. Съществува риск същият проблем, свързан с оперативната координацията да възникне и между надзорните органи, предвидени в разглежданото предложение, и тези, които вече действат съгласно друго законодателство, приложимо за същите продукти.

1.9. ЕИСК отбелязва, че предложението предвижда значителен брой дейности и отговорности за сертифициращите органи, чието практическо функциониране трябва да бъде гарантирано. Това се прави също, за да не се допусне ЗАК да доведе до увеличаване на бюрократичните тежести, така че да се поставят в неизгодно положение производителите, които ще трябва да преминат през редица допълнителни изисквания за сертифициране, за да могат да продължат дейността си на пазара.

2. **Анализ на предложението**

2.1. С предложението за ЗАК Комисията възнамерява да рационализира и преструктурира по всеобхватен и хоризонтален начин действащото законодателство в областта на киберсигурността, като същевременно го актуализира с оглед на новите технологични иновации.

2.2. ЗАК по същество има четири цели: да гарантира, че производителите подобряват безопасността на продуктите, които имат цифрови елементи на етапа на проектиране и разработване и през целия им жизнен цикъл; да гарантират съгласувана рамка от правила за киберсигурност, улесняваща спазването на изискванията от страна на производителите на хардуер и софтуер; да подобри прозрачността на характеристиките за безопасност на продуктите с цифрови елементи; да даде възможност на предприятията и потребителите да използват тези продукти по безопасен начин. По същество с предложението се въвежда маркировка на ЕС за киберсигурност, като се изисква тази маркировка да се поставя върху всички продукти, обхванати от ЗАК.

2.3. Това е хоризонтална мярка, чрез която Комисията възнамерява съгласувано да регулира цялата сфера, тъй като, на практика, обхваща всички продукти с цифрови компоненти. Изключват се само тези от медицинско естество и свързани с гражданското въздухоплаване, превозните средства и продуктите с военно предназначение. Освен това предложението не обхваща услугите от типа „софтуер като услуга“ — SaaS (в облак), освен ако те не се използват за изработване на продукти с цифрови елементи.

2.4. Определението за „продукти с цифрови елементи“ е много широко и включва всички софтуерни или хардуерни продукти, както и софтуер или хардуер, които не са включени в продукта, но са пуснати на пазара отделно.

2.5. Със законодателството се въвеждат задължителни изисквания за киберсигурност за продукти, които имат цифрови компоненти през целия си жизнен цикъл, но не се заменят вече съществуващите изисквания. Напротив, продуктите, които вече са сертифицирани като съответстващи на вече съществуващи стандарти на ЕС, също ще се считат за „валидни“ по смисъла на новия регламент.

2.6. Основният общ принцип е, че на пазара в Европа се пускат само „сигурни“ продукти, чиито производители правят така, че тези продукти да останат сигурни през целия си жизнен цикъл.

2.7. Даден продукт се счита за „сигурен“, когато е проектиран и произведен по такъв начин, че да има равнище на сигурност, съответстващо на кибернетичните рискове, свързани с употребата му, ако към момента на продажбата му не са известни уязвимости, конфигурацията му е сигурна по подразбиране, защитен е от незаконни свързвания, защитава данните, които събира, и събирането на данни е ограничено до тези, които служат за функционирането му.

2.8. Счита се, че даден производител е пригоден да предлага на пазара своите продукти, когато, наред с другото, предоставя достъп до списъка на различните софтуерни компоненти на своите продукти, незабавно предоставя безплатна помощ в случай на нови уязвимости, оповестява публично и описва подробно слабостите, които открива и отстранява, и редовно проверява „стабилността“ на продуктите, които продава. Тези и други дейности, наложени от ЗАК, трябва да се извършват през целия жизнен цикъл на продукта или в продължение на поне пет години от пускането му на пазара. От производителя се изисква да гарантира отстраняването на уязвимостите чрез редовни актуализации на софтуера.

2.9. Съгласно общ принцип, прилаган в различни сектори, задълженията се възлагат и на вносителите и дистрибуторите.

2.10. ЗАК предвижда макрокатегория на т.нар. „нормални“ продукти и софтуер, за които може да се разчита на самооценката на производителя, както вече се прави при други видове сертифициране на маркировката „ЕС“. Според Комисията 90 % от продуктите на пазара попадат в тази категория.

2.11. Съответните продукти могат да бъдат пуснати на пазара след самооценка на тяхната киберсигурност, извършена от производителя, който представя подходяща документация, както е посочено в насоките на законодателството. Същият производител е длъжен да повтори оценката, ако продуктът бъде променен.

2.12. Останалите 10 % от продуктите са разделени на две други категории (клас I, по-малко опасен и клас II, по-опасен), които изискват по-голямо внимание, за да бъдат пуснати на пазара. Това са така наречените „критични продукти с цифрови елементи“, чийто дефект може да доведе до други опасни и по-разширени нарушения на сигурността.

2.13. За продукти от тези два класа основните самосертифицирания са допустими само ако производителят докаже, че е спазил специфични пазарни стандарти и спецификации за сигурност или сертификати за киберсигурност, които вече са предвидени от ЕС. В противен случай производителят може да получи сертификат за продукт от акредитиран сертифициращ орган, чието удостоверение е задължително за продуктите от клас II.

2.14. Системата за класифициране на продуктите в рискови категории се съдържа и в предложения регламент за ИИ (изкуствен интелект). За да се избегнат съмнения относно приложимите разпоредби, ЗАК взема под внимание продуктите с цифрови елементи, които едновременно са класифицирани и като „високорискови системи с ИИ“ съгласно предложението относно ИИ. Такива продукти обикновено ще трябва да отговарят на процедурата за оценяване на съответствието, определена в Регламента за ИИ, с изключение на „критичните цифрови продукти“, за които правилата на ЗАК за оценяване на съответствието ще се прилагат в допълнение към „съществените изисквания на ЗАК“.

2.15. За да се гарантира спазването на ЗАК се предвижда всяка държава членка да възлага надзорна дейност на даден национален орган. В съответствие със законодателството относно безопасността на други продукти, ако национален орган установи, че характеристиките, свързани с киберсигурността на даден продукт не покриват в достатъчна степен изискванията, предлагането му на пазара може да бъде преустановено във въпросната държава. ENISA е компетентна да оценява подробно посочен продукт и нейните оценки, в случай на установена несигурност на продукта, могат да доведат до спиране на предлагането му на пазара в ЕС.

2.16. Системата за санкции, предвидена в ЗАК, се състои от редица санкции, съответстващи на тежестта на нарушението, които в случай на нарушение на съществените изисквания за киберсигурност на продуктите могат да достигнат до 15 милиона евро или 2,5 % от оборота за предходната данъчна година.

3. **Бележки**

3.1. ЕИСК приветства инициативата на Комисията да включи в по-широката нормативна „мозайка“ в областта на киберсигурността ключов елемент, който е координиран с и директивата за мрежова и информационна сигурност (МИС) ([1]), като я допълва, и същевременно е в допълнение към Законодателния акт за киберсигурност ([2]). Високите стандарти за киберсигурност играят ключова роля за създаването на стабилна система на ЕС за киберсигурност за всички икономически оператори, която е от полза за гарантирането за гражданите на ЕС на безопасно използване на всички продукти на пазара и за засилването на тяхното доверие в цифровия свят.

3.2. Поради това в регламента се разглеждат два въпроса: ниското равнище на киберсигурност на много от продуктите и, преди всичко, факта, че много производители не извършват актуализации, за да се справят с уязвимостите. Докато производителите на продукти с цифрови елементи понякога понасят вреди за репутацията си, когато техните продукти не са сигурни, разходите, свързани с уязвимостта, се поемат главно от професионалните ползватели и потребители. Това ограничава стимулите за производителите да инвестират в проектирането и разработването на безопасни продукти и да предоставят актуализации, свързани със сигурността. Освен това предприятията и потребителите често не разполагат с

([1]) Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 година относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза (ОВ L 194, 19.7.2016 г., стр. 1).

([2]) Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността) (ОВ L 151, 7.6.2019г., стр. 15).

достатъчна и точна информация при избора на сигурни продукти и често не знаят как да гарантират, че продуктите, които купуват, са конфигурирани по сигурен начин. Новите правила разглеждат тези два аспекта, като се спират на въпроса за актуализациите и предоставянето на актуална информация на клиентите. ЕИСК счита, че в този смисъл приложен правилно, предложеният регламент би могъл да се превърне в еталон и модел в международен план в областта на киберсигурността.

3.3. ЕИСК приветства предложението за въвеждане на изисквания за информационна сигурност за продуктите с цифрови елементи. Въпреки това ще бъде важно да се избегне припокриване с друго действащо законодателство по този въпрос, като например новата Директивата за МИС 2 ([3]) и Регламента за ИИ.

3.4. ЕИСК счита за важно да се подчертае, че макар, от една страна, да е похвално, че Законодателният акт за киберустойчивост на практика обхваща почти всички цифрови продукти, от друга страна може да възникнат проблеми при практическото му прилагане, като се има предвид обемната дейност за проверка и контрол, която той предвижда.

3.5. Материалният обхват на ЗАК е широк и обхваща всички продукти с цифрови елементи. Съгласно предложеното определение са обхванати всички софтуерни и хардуерни продукти и свързаните с тях операции по обработка на данни. ЕИСК предлага Комисията да изясни дали целият софтуер попада в обхвата на предложението за регламент.

3.6. Производителите ще бъдат задължени да докладват, от една страна, за уязвимости, които са били активно използвани, и от друга — за инциденти, свързани със сигурността. От тях ще се изисква да информират ENISA за всички активно използвани уязвимости, съдържащи се в продукта, и (отделно) за всеки инцидент, който оказва въздействие върху сигурността на продукта, във всеки случай в рамките на 24 часа от узнаването за него. Във връзка с това ЕИСК изтъква необходимостта ENISA да разполага с подходящи като брой и професионалната подготовка ресурси, за да може ефективно да изпълнява съответните и чувствителни задачи, които са ѝ възложени с регламента.

3.7. Фактът, че редица продукти, попадащи в обхвата на предложението, са предмет и на други регулаторни разпоредби в областта на киберсигурността, би могъл да доведе до несигурност относно приложимото законодателство. Въпреки че се предвижда ЗАК да бъде в съответствие с настоящата регулаторна рамка на ЕС относно продуктите, както и с други предложения, които понастоящем са в ход в контекста на стратегията на ЕС в областта на цифровите технологии, правилата, като например тези за високорисковите продукти с изкуствен интелект, са взаимосвързани с правилата, определени в Регламента относно обработването на лични данни. Във връзка с това ЕИСК предлага на Комисията да изготви насоки, които да ориентират производителите и потребителите за неговото правилно прилагане.

3.8. ЕИСК отбелязва, че не са изяснени отношенията между сертифициращите органи съгласно ЗАК, и евентуално други органи, оправомощени да сертифицират киберсигурността по силата на други приложими законодателни разпоредби.

3.9. Значителната тежест на дейностите и отговорността се поема от същите сертифициращи органи, като трябва да се проверява и гарантира тяхното практическо функциониране, за да не доведе ЗАК до увеличаване на бюрократичната тежест, която вече е предвидена за производителите, извършващи дейност на пазара. В това отношение би било важно по-специално МСП и ММСП да имат достъп до квалифицирана експертна подкрепа, която да може да предоставя специфични професионални услуги.

3.10. ЗАК предвижда сертифициращите органи да вземат предвид специфичните нужди на МСП по отношение на дейностите на сертифициращите органи; при все това ЕИСК посочва необходимостта от изясняване на критериите, които следва да бъдат прилагани.

3.11. Съществува обаче риск да възникне проблем с координацията между надзорните органи, предвидени в разглеждания регламент, и тези, които вече действат съгласно друга правна уредба, приложима за същите продукти. Поради това ЕИСК предлага Комисията да призове държавите членки да наблюдават и, ако е необходимо, да предприемат действия за предотвратяване на този риск.

Брюксел, 14 декември 2022 г.

Председател
на Европейския икономически и социален комитет
Christa SCHWENG

([3]) Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета от 14 декември 2022 година 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).