2025/37

15.1.2025 г.

РЕГЛАМЕНТ (ЕС) 2025/37 НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от 19 декември 2024 година

за изменение на Регламент (ЕС) 2019/881 по отношение на управляваните услуги за сигурност

(текст от значение за ЕИП)

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 114 от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

като взеха предвид становището на Европейския икономически и социален комитет ([1]),

след консултация с Комитета на регионите,

в съответствие с обикновената законодателна процедура ([2]),

като имат предвид, че:

(1) С Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета ([3]) беше определена рамка за създаването на европейски схеми за сертифициране на киберсигурността с цел да се гарантира подходящо ниво на киберсигурност за продуктите на информационните и комуникационните технологии (ИКТ), ИКТ услугите и ИКТ процесите в Съюза, както и с цел да се избегне разпокъсаност на вътрешния пазар по отношение на схемите за сертифициране на киберсигурността в Съюза.

(2) За да се гарантира устойчивостта на Съюза на кибератаки и да бъдат предотвратявани всякакви уязвимости на вътрешния пазар, настоящият регламент има за цел да допълва хоризонталната регулаторна рамка, с която се установяват всеобхватни изисквания за киберсигурност за продукти с цифрови елементи съгласно Регламент (ЕС) 2024/2847 на Европейския парламент и на Съвета ([4]), като се предвидят цели, свързани със сигурността, за управляваните услуги за сигурност, както и прилагането и надеждността на тези услуги.

(3) Управляваните услуги за сигурност се предоставят от доставчиците на управлявани услуги за сигурност съгласно определението в член 6, точка 40 от Директива (ЕС) 2022/2555 на Европейския парламент и на Съвета ([5]). Поради това определението за „управлявани услуги за сигурност“ в настоящия регламент следва да бъде съгласувано с определението за „доставчици на управлявани услуги за сигурност“, съдържащо се в Директива (ЕС) 2022/2555. Тези услуги се състоят от извършване или съдействие за извършване на дейности, свързани с управлението на риска за киберсигурността от страна на съответните клиенти, и придобиват все по-голямо значение за предотвратяването на инциденти или ограничаването на последствията от тях. Съответно доставчиците на тези услуги се считат за съществени или важни субекти, принадлежащи към сектор с висока степен на критичност съгласно Директива (ЕС) 2022/2555. Както гласи съображение 86 от посочената директива, доставчиците на управлявани услуги за сигурност в области като реагиране при инциденти, тестване за проникване, одити за сигурността и консултантски услуги, играят особено важна роля в оценката на усилията на субектите за предотвратяване, идентифициране, реагиране на инциденти или възстановяване от такива. Самите доставчици на управлявани услуги за сигурност обаче също са цел на кибератаки и представляват особен риск, тъй като са тясно свързани с операциите на техните клиенти. Ето защо е важно съществените и важните субекти по смисъла на Директива (ЕС) 2022/2555 да подхождат с повишено внимание към избора на доставчици на управлявани услуги за сигурност.

([1]) ОВ C 349, 29.9.2023 г., стр. 167.

([2]) Позиция на Европейския парламент от 24 април 2024 г. (все още непубликувана в Официален вестник) и решение на Съвета от 2 декември 2024 г.

([3]) Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. 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, 7.6.2019 г., стр. 15).

([4]) 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, за изменение на регламенти (ЕС) № 168/2013 и (ЕС) 2019/1020 и Директива (ЕС) 2020/1828 (Законодателен акт за киберустойчивост) (ОВ L, 2024/2847, 20.11.2024 г., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

([5]) 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).

(4) Определението за управлявани услуги за сигурност съгласно настоящия регламент включва неизчерпателен списък на управляваните услуги за сигурност, които биха могли да отговарят на условията за европейски схеми за сертифициране на киберсигурността, като например справяне с инциденти, тестване на проникването, одити на сигурността и консултантски услуги, свързани с техническата подкрепа. Управляваните услуги за сигурност биха могли да обхващат услуги в областта на киберсигурността, които подпомагат готовността, предотвратяването, откриването, анализа и смекчаването на последиците, реагирането и възстановяването от инциденти. Предоставянето на разузнавателни данни за киберзаплахи и оценката на риска, свързани с техническата подкрепа, също могат да бъдат квалифицирани като управлявани услуги за сигурност. Могат да съществуват отделни европейски схеми за сертифициране на киберсигурността за различни управлявани услуги за сигурност. Европейските сертификати за киберсигурност, издадени в съответствие с такива схеми, следва да се отнасят до конкретни управлявани услуги за сигурност на конкретен доставчик на тези услуги.

(5) Доставчиците на управлявани услуги за сигурност могат също така да играят важна роля във връзка с действията на Съюза в подкрепа на реагирането и първоначалното възстановяване в случаи на значителни инциденти и мащабни киберинциденти, като разчитат на услуги от доверени частни доставчици и на изпитване на критични субекти за потенциални уязвимости въз основа на координирани на равнището на Съюза оценки на риска за сигурността. Сертифицирането на управляваните услуги за сигурност може да играе роля при подбора на доверителни доставчици на управлявани услуги за сигурност съгласно определението в Регламент (ЕС) 2025/38 на Европейския парламент и на Съвета ([6]).

(6) Сертифицирането на управляваните услуги за сигурност не само е от значение за процеса на подбор на резерва на ЕС за киберсигурност, създаден с Регламент (ЕС) 2025/38, но представлява и съществен показател за качество за частните и публичните субекти, които възнамеряват да закупят такива услуги. С оглед на критичността на управляваните услуги за сигурност и чувствителността на обработените данни, сертифицирането може да осигури на потенциалните клиенти важни насоки и гаранции относно надеждността на тези услуги. Европейските схеми за сертифициране на киберсигурността на управляваните услуги за сигурност целят да допринасят да се избегне разпокъсаността на вътрешния пазар. Настоящият регламент има за цел съответно да подобри функционирането на вътрешния пазар.

(7) Европейските схеми за сертифициране на киберсигурността на управлявани услуги за сигурност следва да доведат до използването на тези услуги и до засилена конкуренция между доставчиците на управлявани услуги за сигурност. Без да се засяга целта за осигуряване на достатъчни и подходящи нива на съответните технически познания и професионална почтеност на тези доставчици, тези схеми за сертифициране следва да улесняват навлизането на пазара и предлагането на управлявани услуги за сигурност, като опростяват, доколкото е възможно, потенциалната регулаторна, административна и финансова тежест, която доставчиците, по-специално малките и средните предприятия (МСП), включително микропредприятията, биха могли да срещат при предлагането на управлявани услуги за сигурност. Освен това, за да бъде насърчавано приемането и стимулирането на търсенето на управлявани услуги за сигурност, европейските схеми за сертифициране на киберсигурността следва да допринасят за тяхната достъпност, по-специално за по-малките участници, като например МСП, включително микропредприятията, както и за местните и регионалните органи, които разполагат с ограничен капацитет и ресурси, но за които вероятността да бъдат засегнати от нарушения на киберсигурността с финансови, правни, свързани с репутацията и оперативни последици е по-голяма.

(8) Важно е да се предоставя подкрепа на МСП, включително микропредприятията, при прилагането на настоящия регламент и при набирането на специализирани умения и експертен опит в областта на киберсигурността, необходими за предоставяне на управлявани услуги за сигурност в съответствие с изискванията, определени в настоящия регламент. В програмата „Цифрова Европа“, създадена с Регламент (ЕС) 2021/694 на Европейския парламент и на Съвета ([7]), и в други съответни програми на Съюза се предвижда Комисията да установява финансова и техническа подкрепа, която да дава възможност на тези предприятия да допринасят за растежа на икономиката на Съюза и за укрепването на общото равнище на киберсигурност в Съюза, включително чрез рационализиране на финансовата подкрепа от програмата „Цифрова Европа“ и други съответни програми на Съюза и чрез подпомагане на МСП, включително микропредприятията.

(9) Европейските схеми за сертифициране на киберсигурността на управлявани услуги за сигурност следва да допринасят за наличието на сигурни и висококачествени услуги, които гарантират безопасен цифров преход, както и за постигането на целите, определени в политическа програма „Цифрово десетилетие“ до 2030 г., създадена с Решение (ЕС) 2022/2481 на Европейския парламент и на Съвета ([8]), по-специално по отношение на целта 75 % от

([6]) Регламент (ЕС) 2025/38 на Европейския парламент и на Съвета от 19 декември 2024 г. за определяне на мерки за укрепване на солидарността и способностите на Съюза за откриване, подготовка и реагиране при киберзаплахи и инциденти, и за изменение на Регламент (ЕС) 2021/694 (Законодателен акт в областта на киберсолидарността) (ОВ L, 15.1.2025 г., ELI: http://data.europa.eu/eli/reg/2025/38/oj).

([7]) Регламент (ЕС) 2021/694 на Европейския парламент и на Съвета от 29 април 2021 г. за създаване на програмата „Цифрова Европа“ и за отмяна на Решение (ЕС) 2015/2240 (ОВ L 166, 11.5.2021 г., стр. 1).

([8]) Решение (ЕС) 2022/2481 на Европейския парламент и на Съвета от 14 декември 2022 г. за създаване на политическа програма „Цифрово десетилетие“ до 2030 г. (ОВ L 323, 19.12.2022 г., стр. 4).

предприятията в Съюза да започнат да използват компютърни услуги „в облак“, големи информационни масиви или изкуствен интелект, над 90 % от МСП, включително микропредприятията, да достигнат поне основно равнище на цифров интензитет и ключови обществени услуги да са достъпни онлайн.

(10) Освен че внедряват ИКТ продукти, ИКТ услуги или ИКТ процеси, управляваните услуги за сигурност често осигуряват допълнителни елементи на услугата, които са плод на компетентността, експертните познания и опита на персонала на доставчиците на такива услуги. Част от целите, свързани със сигурността, следва да бъдат осигуряването на много високо равнище на тази компетентност, експертни познания и опит, заедно с подходящи вътрешни процедури, за да се гарантира много високо качество на предоставяните управлявани услуги за сигурност. За да се гарантира, че всички аспекти на управляваните услуги за сигурност могат да бъдат обхванати от специални европейски схеми за сертифициране на киберсигурността, е необходимо Регламент (ЕС) 2019/881 да бъде изменен. Резултатите и препоръките от оценката и прегледа, предвидени в Регламент (ЕС) 2019/881, следва да бъдат взети предвид.

(11) За да се улеснява растежът на надежден вътрешен пазар, като същевременно се създават партньорства с трети държави със сходни възгледи, процесът на сертифициране, установен в европейската рамка за сертифициране на киберсигурността, предвидена от Регламент (ЕС) 2019/881, следва да бъде имплементиран така че да се улеснява международното признаване и привеждането в съответствие с международните стандарти.

(12) Съюзът е изправен пред недостиг на таланти, който се характеризира с недостиг на квалифицирани специалисти, и пред бързо променяща се картина на заплахите, както се признава в съобщението на Комисията от 18 април 2023 г., озаглавено „Преодоляване на недостига на таланти в областта на киберсигурността за повишаване на конкурентоспособността, растежа и устойчивостта на ЕС („Академията на ЕС за киберумения“)“. Образователните ресурси и формите на формално обучение варират и знанията могат да бъдат придобивани по различни начини: формални, например чрез университети или курсове, или неформални, например чрез обучения на работното място или професионален опит в съответната област. Поради това, за да се дава възможност за появата на висококачествени, управлявани услуги за сигурност и за да се придобива по-добър поглед върху състава на работната сила на Съюза в областта на киберсигурността, е важно сътрудничеството между държавите членки, Комисията, Агенцията на Европейския съюз за киберсигурност, създадена с Регламент (ЕС) 2019/881, (ENISA) и заинтересованите лица, включително от частния сектор и академичните среди, да бъде засилвано чрез развитието на публично-частни партньорства, подкрепа за инициативи за научни изследвания и иновации, разработването и взаимното признаване на общи стандарти и сертифицирането на умения в областта на киберсигурността, включително чрез Европейската рамка за умения в областта на киберсигурността. Това сътрудничество следва също така да улеснява мобилността на специалистите в областта на киберсигурността в рамките на Съюза, както и интегрирането на познанията за киберсигурността в програмите за образование и обучение, като същевременно се гарантира достъп до чиракуване и стажове за младите хора, включително за хората, живеещи в региони в неравностойно положение, като например острови, слабо населени, селски и отдалечени райони. Важно е това сътрудничество да има за цел да привлича повече жени и момичета в тази област и да допринася за преодоляване на неравнопоставеността между половете в областта на науката, технологиите, инженерството и математиката, както и частният сектор да се стреми да предоставя обучение на работното място, насочено към най-търсените умения, с участието на публичната администрация и стартиращите предприятия, както и МСП, включително микропредприятията. Важно е също така доставчиците и държавите членки да си сътрудничат и да допринасят за събирането на данни за положението и развитието на пазара на труда в областта на киберсигурността.

(13) ENISA играе важна роля в подготовката на проектите за европейски схеми за сертифициране на киберсигурността. При изготвянето на проекта за общ бюджет на Съюза Комисията следва да прави оценка на бюджетните средства, необходими за щатното разписание на ENISA, в съответствие с процедурата, посочена в член 29 от Регламент (ЕС) 2019/881.

(14) В настоящия регламент се предвиждат целенасочени изменения на Регламент (ЕС) 2019/881, за да се позволи създаването на европейски схеми за сертифициране на киберсигурността за управлявани услуги за сигурност. По този начин в него също така се уточняват и изясняват някои разпоредби от посочения регламент относно подготовката и функционирането на всички европейски схеми за сертифициране на киберсигурността, за да се гарантира тяхната прозрачност и откритост. Последните изменения, които се ограничават до уточняване или изясняване на Регламент (ЕС) 2019/881, по-специално измененията, касаещи информацията, която ENISA трябва да предоставя при предаването на проект на схема, *ad hoc* работните групи, създавани за всеки проект за схема, и информацията и консултациите по отношение на европейските схеми за сертифициране на киберсигурността, не следва по никакъв начин да засягат по-широката оценка и преглед на посочения регламент, изисквани съгласно член 67 от него, по-специално оценката на въздействието, ефективността и ефикасността на дела от посочения регламент, свързан с рамката за сертифициране на киберсигурността. Оценката и прегледът на този дял следва да се основават на широки консултации със заинтересованите страни и пълен и задълбочен анализ на съответните процедури.

(15) Доколкото целта на настоящия регламент, а именно да се способства за създаването на европейски схеми за сертифициране на киберсигурността за управляваните услуги за сигурност, не може да бъде постигната в достатъчна степен от държавите членки, а поради своя обхват и последици може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейския съюз. В съответствие с принципа на пропорционалност, уреден в посочения член, настоящият регламент не надхвърля необходимото за постигането на тази цел.

(16) Европейският надзорен орган по защита на данните беше консултиран в съответствие с член 42, параграф 1 от Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета ([9]) и прие становище на 10 януари 2024 г.,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

Член 1

Изменения на Регламент (ЕС) 2019/881

Регламент (ЕС) 2019/881 се изменя, както следва:

1) В член 1, параграф 1, първа алинея буква б) се заменя със следното:

„б) се определя рамка за създаването на европейски схеми за сертифициране на киберсигурността с цел да се гарантира подходящо ниво на киберсигурност за ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност в Съюза, както и с цел да се избегне разпокъсаност на вътрешния пазар по отношение на схемите за сертифициране на киберсигурността в Съюза.“

2) Член 2 се изменя, както следва:

а) точки 9, 10 и 11 се заменят със следното:

„9) „европейска схема за сертифициране на киберсигурността“ означава определен на равнището на Съюза цялостен набор от правила, технически изисквания, стандарти и процедури, установени на равнище на Съюза и които се прилагат по отношение на сертифицирането или оценката на съответствието на специфични ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност;

10) „национална схема за сертифициране на киберсигурността“ означава цялостен набор от правила, технически изисквания, стандарти и процедури, разработени и приети от национален публичен орган и които се прилагат по отношение на сертифицирането или оценката на съответствието на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност, попадащи в обхвата на конкретната схема;

11) „европейски сертификат за киберсигурност“ означава издаден от съответния орган документ, удостоверяващ, че за даден ИКТ продукт, ИКТ услуга, ИКТ процес или управлявана услуга за сигурност е извършена оценка за съответствие спрямо специфичните изисквания за сигурност, определени в дадена европейска схема за сертифициране на киберсигурността;“;

б) вмъква се следната точка:

„14а) „управлявана услуга за сигурност“ означава услуга, предоставяна на трета страна, по извършване или съдействие за извършване на дейности, свързани с управлението на риска за киберсигурността, като например справяне с инциденти, тестване за проникване, одити на сигурността и консултантски услуги, включително експертни съвети, свързани с техническата подкрепа;“;

в) точки 20, 21 и 22 се заменят със следното:

„20) „техническа спецификация“ означава документ, определящ техническите изисквания, които трябва да бъдат изпълнени от ИКТ продукт, ИКТ услуга или ИКТ процес, или процедурите за оценяване на съответствието, свързани с ИКТ продукт, ИКТ услуга, ИКТ процес или управлявана услуга за сигурност;

([9]) Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета от 23 октомври 2018 г. относно защитата на физическите лица във връзка с обработването на лични данни от институциите, органите, службите и агенциите на Съюза и относно свободното движение на такива данни и за отмяна на Регламент (ЕО) № 45/2001 и Решение № 1247/2002/ЕО (ОВ L 295, 21.11.2018 г., стр. 39).

21) „ниво на увереност“ означава основа за увереност, че даден ИКТ продукт, ИКТ услуга, ИКТ процес или управлявана услуга за сигурност отговаря на изискванията за сигурност на конкретна европейска схема за сертифициране на киберсигурността, и указва на какво ниво е бил оценен ИКТ продуктът, ИКТ услугата, ИКТ процесът или управляваната услуга за сигурност, но само по себе си не измерва сигурността на съответния ИКТ продукт, ИКТ услуга, ИКТ процес или управлявана услуга за сигурност;

22) „самооценяване на съответствието“ означава действие, извършвано от производител или доставчик на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност, с което се оценява дали тези ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност отговарят на изискванията на конкретна европейска схема за сертифициране на киберсигурността.“

3) В член 4 параграф 6 се заменя със следното:

„6. ENISA насърчава използването на европейското сертифициране с оглед на избягването на разпокъсаността на вътрешния пазар. ENISA допринася за създаването и поддържането на европейската рамка за сертифициране на киберсигурността съгласно дял III от настоящия регламент, с цел постигане на повече прозрачност в увереността за киберсигурността на ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност като по този начин се укрепва доверието в цифровия вътрешен пазар и неговата конкурентоспособност.“

4) Член 8 се изменя, както следва:

а) параграф 1 се изменя, както следва:

i) уводната част се заменя със следното:

„1. ENISA насърчава разработването и изпълнението на политиката на Съюза за сертифициране на киберсигурността на ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност, както е предвидено в дял III от настоящия регламент, като:“;

ii) буква б) се заменя със следното:

„б) изготвя проекти за европейски схеми за сертифициране на киберсигурността („проекти за схеми“) на ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност в съответствие с член 49;“;

б) параграф 3 се заменя със следното:

„3. ENISA съставя и публикува насоки и разработва добри практики относно изискванията за киберсигурност за ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност в сътрудничество с националните органи по сертифицирането на киберсигурността и с отрасъла по формален, структуриран и прозрачен начин.“;

в) параграф 5 се заменя със следното:

„5. ENISA улеснява въвеждането и използването на европейски и международни стандарти за управление на риска и за сигурността на ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност.“

5) Член 46 се заменя със следното:

„*Член 46*

Европейска рамка за сертифициране на киберсигурността

1. Европейската рамка за сертифициране на киберсигурността се създава с цел да се подобрят условията за функционирането на вътрешния пазар, като се повиши нивото на киберсигурност в Съюза и се даде възможност за хармонизиран подход на равнището на Съюза спрямо европейските схеми за сертифициране на киберсигурността, с оглед на създаването на цифров единен пазар за ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност.

2. Европейската рамка за сертифициране на киберсигурността предвижда механизъм за създаване на европейски схеми за сертифициране на киберсигурността и удостоверяване, че ИКТ продуктите, ИКТ услугите и ИКТ процесите, които са били оценени в съответствие с такива схеми, отговарят на определени изисквания за сигурност с цел да се защити наличността, автентичността, целостта или поверителността на съхраняваните, предаваните или обработваните данни или на функциите и услугите, предлагани или направени достъпни чрез тези продукти, услуги и процеси през

целия им жизнен цикъл. Освен това тя удостоверява, че управляваните услуги за сигурност, оценени в съответствие с тези схеми, отговарят на определени изисквания за сигурност с цел защита на наличността, автентичността, целостта и поверителността на данните, до които се осъществява достъп, които се обработват, съхраняват или предават във връзка с предоставянето на тези услуги, и че тези услуги се предоставят непрекъснато с необходимата компетентност, експертни познания и опит от персонал с достатъчно и подходящо ниво на съответните технически познания и професионална почтеност.“

6) Член 47 се изменя, както следва:

а) параграф 2 се заменя със следното:

„2. Непрекъснатата работна програма на Съюза включва по-специално списък на ИКТ продуктите, ИКТ услугите, ИКТ процесите и управляваните услуги за сигурност или категориите такива продукти, услуги и процеси, които могат да се възползват от включване в обхвата на дадена европейска схема за сертифициране на киберсигурността.“;

б) параграф 3 се изменя, както следва:

i) уводната част се заменя със следното:

„3. Включването на който и да било конкретен ИКТ продукт, ИКТ услуга, ИКТ процес или управлявана услуга за сигурност или категория такива продукти, услуги или процеси, в непрекъснатата работна програма на Съюза става на едно или повече от следните основания:“;

ii) буква а) се заменя със следното:

„а) наличието и разработването на национални схеми за сертифициране на киберсигурността, които да обхващат някоя конкретна категория ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност и по-специално по отношение на опасността от възникване на разпокъсаност;“;

iii) вмъква се следната буква:

„ва) технологичното развитие и наличието и разработването на международни схеми за сертифициране на киберсигурността и международни и промишлени стандарти;“

7) Член 49 се изменя, както следва:

а) параграфи 1—4 се заменят със следното:

„1. По искане на Комисията съгласно член 48 ENISA изготвя проект за схема, която отговаря на приложимите изисквания, определени в членове 51, 51а, 52 и 54.

2. По искане на Европейската група за сертифициране на киберсигурността съгласно член 48, параграф 2, ENISA може да изготви проект за схема, която отговаря на приложимите изисквания, определени в членове 51, 51а, 52 и 54. Ако ENISA отхвърли такова искане, тя мотивира отказа си. Всяко решение за отхвърляне на такова искане се взема от управителния съвет.

3. При изготвянето на проект за схема ENISA провежда своевременни консултации с всички съответни заинтересовани страни посредством официален, отворен, прозрачен и приобщаващ процес на консултация. При предаването на проекта на схема на Комисията съгласно параграф 6 ENISA предоставя информация за начина, по който е спазила настоящия параграф.

4. За всеки проект за схема ENISA създава *ad hoc* работна група в съответствие с член 20, параграф 4, която да предостави на ENISA конкретни съвети и експертно мнение. Тези *ad hoc* работни групи по целесъобразност и без да се засягат процедурите и свободата на преценка, предвидени в член 20, параграф 4, включват експерти от публичните администрации на държавите членки, институциите, органите, службите и агенциите на Съюза и частния сектор.“;

б) параграф 7 се заменя със следното:

„7. На основата на проекта за схема, изготвен от ENISA, Комисията може да приема актове за изпълнение, с които да установи европейска схема за сертифициране на киберсигурността за ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност, отговаряща на съответните изисквания на членове 51, 51а, 52 и 54. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 66, параграф 2.“

8) Вмъква се следният член:

„*Член 49а*

Информация и провеждане на консултации относно европейските схеми за сертифициране на киберсигурността

1. Комисията прави публично достояние информацията относно своето искане, отправено до ENISA, за изготвяне на проект за схема или за извършване на преглед на съществуваща европейска схема за сертифициране на киберсигурността, както е посочено в член 48.

2. По време на изготвянето на проект за схема от ENISA съгласно член 49 Европейският парламент, Съветът или и двете институции могат да поискат от Комисията в качеството ѝ на председател на Европейската група за сертифициране на киберсигурността и ENISA да представят на всеки три месеца съответната информация относно проекта на проект за схема. По искане на Европейския парламент или на Съвета ENISA, в съгласие с Комисията и без да се засяга член 27, може да предоставя на Европейския парламент и на Съвета съответните части от проекта на проект за схема по начин, съответстващ на изискваното ниво на поверителност, и когато е целесъобразно, по ограничен начин.

3. За да се засилва диалогът между институциите на Съюза и да се допринася за официален, открит, прозрачен и приобщаващ процес на консултации, Европейският парламент, Съветът или и двете институции могат да приканват Комисията и ENISA да обсъждат въпроси, свързани с функционирането на европейските схеми за сертифициране на киберсигурността на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност.

4. При оценката на настоящия регламент съгласно член 67 Комисията взема предвид елементите, произтичащи от становищата, изразени от Европейския парламент и от Съвета по въпросите, посочени в параграф 3 от настоящия член, когато е целесъобразно.“

9) Член 51 се изменя, както следва:

а) заглавието се заменя със следното:

„Цели, свързани със сигурността на европейските схеми за сертифициране на киберсигурността на ИКТ продукти, ИКТ услуги и ИКТ процеси“;

б) уводното изречение се заменя със следното:

„Европейските схеми за сертифициране на киберсигурността на ИКТ продукти, ИКТ услуги или ИКТ процеси се проектират така, че да постигнат, според нуждите, най-малко следните цели, свързани със сигурността:“

10) Вмъква се следният член:

„*Член 51а*

Цели, свързани със сигурността на европейските схеми за сертифициране на киберсигурността на управлявани услуги за сигурност

Европейските схеми за сертифициране на киберсигурността на управлявани услуги за сигурност се проектират така, че да постигнат, според нуждите, най-малко следните цели, свързани със сигурността:

а) управляваните услуги за сигурност да разполагат с необходимата компетентност, експертни познания и опит, включително персоналът, на когото е възложено предоставянето на тези услуги, да притежава достатъчно и подходящо ниво на технически познания и компетентност в конкретната област, достатъчен и подходящ опит и най-висока степен на професионална почтеност;

б) доставчикът да разполага с подходящи вътрешни процедури, за да гарантира, че управляваните услуги за сигурност се предоставят с достатъчно и подходящо качество по всяко време;

в) данните, до които се осъществява достъп и които се съхраняват, предават или обработват по друг начин във връзка с предоставянето на управлявани услуги за сигурност, да са защитени срещу случаен или неразрешен достъп, съхранение, разкриване, унищожаване, друга обработка, загуба, промяна или липса;

г) своевременно да се възстановяват наличието и достъпът до данни, услуги и функции в случай на физически или технически инцидент;

д) оправомощените лица, програми и машини да имат достъп единствено до данните, услугите и функциите, за които се отнасят правата им на достъп;

е) да се пази запис на данните, услугите или функциите, до които е бил осъществен достъп или са били използвани или обработвани по друг начин, кога и от кого, както и този запис да е наличен за оценка;

ж) ИКТ продуктите, ИКТ услугите и ИКТ процесите, внедрени при предоставянето на управляваните услуги за сигурност, да са защитени още при разработването и по подразбиране и, когато е приложимо, да включват последните актуализации на сигурността и да не съдържат публично известни уязвимости.“

11) Член 52 се изменя, както следва:

а) параграф 1 се заменя със следното:

„1. Европейските схеми за сертифициране на киберсигурността могат да предвиждат едно или повече от следните нива на увереност за ИКТ продуктите, ИКТ услугите, ИКТ процесите и управляваните услуги за сигурност: „базово“, „съществено“ или „високо“. Нивото на увереност следва да е съизмеримо със степента на риска, свързан с предвидената употреба на ИКТ продукта, ИКТ услугата, ИКТ процеса или управляваната услуга за сигурност, с оглед на вероятността от инцидент и неговото въздействие.“;

б) параграф 3 се заменя със следното:

„3. Изискванията за сигурност, които отговарят на всяко ниво на увереност се посочват в съответната европейска схема за сертифициране на киберсигурността включително съответните функционалности за сигурност и съответното ниво на стриктност и задълбоченост на оценката, през която трябва да премине даден ИКТ продукт, ИКТ услуга или ИКТ процес и управлявана услуга за сигурност.“;

в) параграфи 5, 6 и 7 се заменят със следното:

„5. Европейският сертификат за киберсигурност или ЕС декларацията за съответствие, посочващи ниво на увереност „базово“, дава увереност, че ИКТ продуктите, ИКТ услугите, ИКТ процесите или управляваните услуги за сигурност, за които този сертификат или тази ЕС декларация за съответствие са издадени, отговарят на съответните изисквания за сигурност, включително функционалности за сигурност, и че са били оценени на ниво, което има за цел да се сведат до минимум известните основни рискове от инциденти и кибератаки. Дейностите по оценка, които трябва да се предприемат, включват най-малко преглед на техническата документация. Когато такъв преглед не е подходящ, се предприемат заместващи дейности с равностоен ефект.

6. Европейският сертификат за киберсигурност, посочващ ниво на увереност „съществено“, дава увереност, че ИКТ продуктите, ИКТ услугите, ИКТ процесите или управляваните услуги за сигурност, за които този сертификат е издаден, отговарят на съответните изисквания за сигурност, включително функционалности за сигурността, и че са били оценени на ниво, което има за цел да се сведат до минимум известните киберрискове, рискове от инциденти и кибератаки, извършвани от субекти с ограничени умения и ресурси. Дейностите по оценка, които трябва да се предприемат, включват най-малко следното: преглед за доказване отсъствие на общоизвестни уязвимости, и изпитване за доказване, че ИКТ продуктите, ИКТ услугите, ИКТ процесите или управляваните услуги за сигурност правилно внедряват необходимите функции за сигурност. Когато такива дейности по оценка не са подходящи, се предприемат заместващи дейности с равностоен ефект.

7. Европейският сертификат за киберсигурност, посочващ ниво на увереност „високо“ дава увереност, че ИКТ продуктите, ИКТ услугите, ИКТ процесите или управляваните услуги за сигурност, за които сертификатът е издаден, отговарят на съответните изисквания за сигурност, включително функционалности за сигурност, и че са били оценени на ниво, което има за цел да се сведе до минимум рискът от най-висш тип кибератаки, извършвани от субекти със значителни умения и ресурси. Дейностите по оценка, които трябва да се предприемат, включват най-малко следното: преглед за доказване отсъствие на общоизвестни уязвимости; изпитване за доказване, че ИКТ продуктите, ИКТ услугите, ИКТ процесите или управляваните услуги за сигурност правилно внедряват необходимите най-съвременни функции за сигурност; и оценяване на устойчивостта им на атаки на умели извършители посредством тестване за проникване. Когато такива дейности по оценка не са подходящи, се предприемат заместващи дейности с равностоен ефект.“

12) В член 53 параграфи 1, 2 и 3 се заменят със следното:

„1. Дадена европейска схема за сертифициране на киберсигурността може да позволява извършване на самооценяване на съответствието, като отговорност за нея носи единствено производителят или доставчикът на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност. Самооценяване на съответствието се разрешава само във връзка с ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност с ниско ниво на риск, съответстващо на ниво на увереност „базово“.

2. Производителят или доставчикът на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност може да издаде ЕС декларация за съответствие, в която заявява, че е изпълнил определените в схемата изисквания. Чрез издаването на такава декларация производителят или доставчикът на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност поема отговорност за съответствието на ИКТ продукта, ИКТ услугата, ИКТ процеса или управляваната услуга за сигурност с определените в схемата изисквания.

3. Производителят или доставчикът на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност съхранява ЕС декларацията за съответствие, техническата документация и всякаква друга съответна информация, отнасяща се до съответствието на ИКТ продуктите, ИКТ услугите, ИКТ процесите или управляваните услуги за сигурност със схемата, която е на разположение на националния орган за сертифициране на киберсигурността, определен съгласно член 58, за срок, определен в съответната европейска схема за сертифициране на киберсигурността. Копие от ЕС декларацията за съответствие се предоставя на националния орган за сертифициране на киберсигурността и на ENISA.“

13) В член 54 параграф 1 се изменя, както следва:

а) буква а) се заменя със следното:

„а) предмет и обхват на схемата за сертифициране, включително вида или категориите ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност, обхванати от нея;“;

б) буква ж) се заменя със следното:

„ж) конкретните критерии и методи за оценка, включително типовете оценки, които да бъдат използвани, с цел да се докаже, че са постигнати посочените в членове 51 и 51а приложими цели, свързани със сигурността;“;

в) буква й) се заменя със следното:

„й) правилата за наблюдение на съответствието на ИКТ продуктите, ИКТ услугите, ИКТ процесите или управляваните услуги за сигурност с изискванията на европейските сертификати за киберсигурност или на ЕС декларациите за съответствие, включително механизми за удостоверяване на трайното съответствие с определените изисквания за киберсигурност;“;

г) буква л) се заменя със следното:

„л) правила относно последиците за ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност, които са били сертифицирани или за които има издадена ЕС декларация за съответствие, но които не съответстват на изискванията на схемата;“;

д) буква о) се заменя със следното:

„о) списък на националните или международни схеми за сертифициране на киберсигурността, които обхващат същия тип или категории ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност, изисквания за сигурност, критерии и методи за оценка и нива на увереност;“;

е) буква р) се заменя със следното:

„р) срока, през който следва да бъде налична ЕС декларацията за съответствие, техническата документация и всякаква друга съответна информация, която трябва да се представи от производителя или доставчика на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност;“

14) Член 56 се изменя, както следва:

а) параграф 1 се заменя със следното:

„1. ИКТ продуктите, ИКТ услугите, ИКТ процесите и управляваните услуги за сигурност, сертифицирани по европейска схема за сертифициране на киберсигурността, приета съгласно член 49, се считат за съответстващи на изискванията на такава схема.“;

б) параграф 3 се изменя, както следва:

i) първата алинея се заменя със следното:

„Комисията прави редовно оценяване на ефективността и използването на приетите европейски схеми за сертифициране на киберсигурността и дали някоя конкретна европейска схема за сертифициране на киберсигурността следва да бъде направена задължителна посредством относимо право на Съюза, така че да се гарантира подходящо ниво на киберсигурност на ИКТ продуктите, ИКТ услугите, ИКТ процесите и от 4 февруари 2025 г. управляваните услуги за сигурност в Съюза и да се подобри функционирането на вътрешния пазар. Първото оценяване се прави до 31 декември 2023 г. и най-малко веднъж на 2 години след това се правят последващи оценявания. Въз основа на резултатите от тези оценявания, Комисията набелязва ИКТ продуктите, ИКТ услугите, ИКТ процесите и управляваните услуги за сигурност, обхванати от съществуваща схема за сертифициране, които следва да бъдат включени в обхвата на задължителна схема за сертифициране.“;

ii) третата алинея се изменя, както следва:

— буква а) се заменя със следното:

„а) отчита въздействието на мерките върху производителите или доставчиците на такива ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност, както и върху ползвателите, от гледна точка на разходите за тези мерки и социалните или икономическите ползи от очакваното повишено ниво на сигурност на ИКТ продуктите, ИКТ услугите, ИКТ процесите или управляваните услуги за сигурност, към които са насочени;“;

— буква г) се заменя със следното:

„г) отчита сроковете за изпълнение, необходимостта от преходни мерки и срокове, по-специално по отношение на възможното въздействие на мярката върху производителите или доставчиците на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност, включително конкретните интереси и потребности на МСП, включително микропредприятията;“;

в) параграфи 7 и 8 се заменят със следното:

„7. Физическото или юридическото лице, което подлага ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност на процедурите за сертифициране, предоставя на националния орган за сертифициране на киберсигурността, определен съгласно член 58, когато този орган е издаващият орган на европейския сертификат за киберсигурност, или на органа за оценяване на съответствието по член 60, цялата необходима информация за провеждане на сертифицирането.

8. Притежателят на европейски сертификат за киберсигурност уведомява органа или институцията, посочени в параграф 7, за всички открити впоследствие уязвимости или нередности във връзка със сигурността на сертифицирания ИКТ продукт, ИКТ услуга, ИКТ процес или управлявана услуга за сигурност, които може да окажат въздействие върху тяхното съответствие с изискванията, свързани със сертифицирането. Органът или институцията изпраща тази информация без излишно забавяне на съответния национален орган за сертифициране на киберсигурността.“

15) В член 57 параграфи 1 и 2 се заменят със следното:

„1. Без да се засягат разпоредбите на параграф 3 от настоящия член, националните схеми за сертифициране на киберсигурността и свързаните с тях процедури за ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност, обхванати от европейска схема за сертифициране на киберсигурността, прекратяват правното си действие от датата, посочена в акта за изпълнение, приет съгласно член 49, параграф 7. Националните схеми за сертифициране на киберсигурността и свързаните с тях процедури за ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност, които не са обхванати от европейска схема за сертифициране на киберсигурността, продължават да съществуват.

2. Държавите членки не въвеждат нови национални схеми за сертифициране на киберсигурността на ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност вече обхванати от европейска схема за сертифициране на киберсигурността, която е в сила.“

16) Член 58 се изменя, както следва:

а) параграф 7 се изменя, както следва:

i) букви а) и б) се заменят със следното:

„а) упражняват надзор и следят за спазването на правилата, включени в европейски схеми за сертифициране на киберсигурността съгласно член 54, параграф 1, буква й), за да наблюдават съответствието на ИКТ продуктите, ИКТ услугите, ИКТ процесите и управляваните услуги за сигурност с изискванията на издадените европейски сертификати за киберсигурност на съответната им територия, в сътрудничество с други съответни органи за надзор на пазара;

б) наблюдават и следят за спазването на задълженията на производителите или доставчиците на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност, които са установени на тяхна територия и които извършват самооценяване на съответствието, и по-специално наблюдават и следят за спазването на задълженията на тези производители или доставчици, посочени в член 53, параграфи 2 и 3 и в съответната европейска схема за сертифициране на киберсигурността;“;

ii) буква з) се заменя със следното:

„з) сътрудничат си с другите национални органи за сертифициране на киберсигурността или други публични органи, включително чрез споделяне на информация за възможни несъответствия на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност с изискванията на настоящия регламент или с изискванията на конкретни европейски схеми за сертифициране на киберсигурността; и“;

б) параграф 9 се заменя със следното:

„9. Националните органи за сертифициране на киберсигурността си сътрудничат помежду си и с Комисията, и по-специално обменят информация, опит и добри практики във връзка със сертифицирането на киберсигурността и техническите въпроси, засягащи киберсигурността на ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност.“

17) В член 59, параграф 3, букви б) и в) се заменят със следното:

„б) процедурите за надзор и изпълнение на правилата за наблюдение на съответствието на ИКТ продуктите, ИКТ услугите, ИКТ процесите и управляваните услуги за сигурност с европейските сертификати за киберсигурност съгласно член 58, параграф 7, буква а);

в) процедурите за наблюдение и изпълнение на задълженията на производителите или доставчиците на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност съгласно член 58, параграф 7, буква б);“

18) В член 67 параграфи 2 и 3 се заменят със следното:

„2. В оценката също така се разглежда въздействието и ефективността на разпоредбите на дял III от настоящия регламент, включително процедурите, водещи до приемането на европейски схеми за сертифициране на киберсигурността и техните набори от доказателства, по отношение на целите за осигуряване на адекватно ниво на киберсигурност на ИКТ продуктите, ИКТ услугите, ИКТ процесите и управляваните услуги за сигурност в Съюза и за подобряване на функционирането на вътрешния пазар.

3. В оценката се преценява дали са необходими съществени изисквания за киберсигурност за достъп до вътрешния пазар, за да се предотврати навлизането на вътрешния пазар на ИКТ продукти, ИКТ услуги, ИКТ процеси и управлявани услуги за сигурност, които не отговарят на базовите изисквания за киберсигурност.“

19) Приложението се изменя в съответствие с приложението към настоящия регламент.

Член 2

Настоящият регламент влиза в сила на двадесетия ден след 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 19 декември 2024 година.

За Европейския парламент	*За Съвета*
Председател	*Председател*
R. METSOLA	BÓKA J.

ПРИЛОЖЕНИЕ

Приложението към Регламент (ЕС) 2019/881 се изменя, както следва:

1) Точки 2—5 се заменят със следното:

„2. Органът за оценяване на съответствието е трета страна, която е независима от организацията или от ИКТ продуктите, ИКТ услугите, ИКТ процесите или управляваните услуги за сигурност, които оценява.

3. Орган, който принадлежи към стопанска асоциация или професионална федерация, представляваща предприятия, участващи в проектирането, производството, доставката, сглобяването, използването или поддръжката на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност, които този орган оценява, може да се счита за орган за оценяване на съответствието, при условие че са доказани неговата независимост и липсата на конфликт на интереси.

4. Органът за оценяване на съответствието, неговото висше ръководство и персоналът, който отговаря за изпълнението на задачите по оценяване на съответствието, не могат да са проектант, производител, доставчик, монтажник, купувач, собственик, ползвател или извършващ поддръжката субект на оценявания ИКТ продукт, ИКТ услуга, ИКТ процес или управлявана услуга за сигурност, или упълномощен представител на някоя от тези страни. Това не изключва използването на оценявани ИКТ продукти, които са необходими за дейностите на органа за оценяване на съответствието, или използването на такива ИКТ продукти за лични цели.

5. Органът за оценяване на съответствието, неговото висше ръководство и персоналът, отговорен за изпълнение на задачите по оценяване на съответствието, не вземат пряко участие в проектирането, производството, конструирането, предоставянето, предлагането на пазара, монтирането, използването или поддръжката на оценяваните ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност, нито представляват страни, ангажирани в тези дейности. Органът за оценяване на съответствието, неговото висше ръководство и персоналът, отговорен за изпълнение на задачите по оценяване на съответствието, не участват в никаква дейност, която може да е в противоречие с тяхната независима преценка или тяхното почтено поведение по отношение на техните дейности по оценяване на съответствието. Тази забрана се прилага по-конкретно за консултантски услуги.“

2) Точка 10 се изменя, както следва:

а) уводната част се заменя със следното:

„10. По всяко време и за всяка процедура за оценяване на съответствието, както и за всеки вид, категория или подкатегория ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност, органът за оценяване на съответствието разполага с необходимите:“;

б) буква в) се заменя със следното:

„в) процедури за изпълнение на дейности, които надлежно отчитат размера на дадено предприятие, отрасъла, в който то осъществява дейността си, неговата структура, степента на сложност на технологията на въпросния ИКТ продукт, ИКТ услуга, ИКТ процес или управлявана услуга за сигурност и масовия или сериен характер на производството.“

3) Точки 19 и 20 се заменят със следното:

„19. Органите за оценяване на съответствието отговарят на изискванията на съответния хармонизиран стандарт, както е определено в член 2, точка 9 от Регламент (ЕО) № 765/2008, за акредитацията на органи за оценяване на съответствието, които извършват сертифициране на ИКТ продукти, ИКТ услуги, ИКТ процеси или управлявани услуги за сигурност.

20. Органите за оценяване на съответствието гарантират, че изпитвателните лаборатории, използвани за целите на оценяването на съответствието, отговарят на изискванията на съответния хармонизиран стандарт, както е определен в член 2, точка 9 от Регламент (ЕО) № 765/2008, за акредитацията на лаборатории, които извършват изпитвания.“

Във връзка с този акт е направено изявление, което може да бъде намерено в ОВ C, C/2025/307, 15.1.2025 г., ELI: http://data.europa.eu/eli/C/2025/307/oj.