Съвет на
Европейския съюз

Брюксел, 29 май 2018 г.
(OR. en)

9350/18

Междуинституционално досие:
2017/0225 (COD)

CYBER 115
TELECOM 152
CODEC 860
COPEN 163
COPS 175
COSI 129
CSC 170
CSCI 80
IND 143
JAI 514
JAIEX 55
POLMIL 61
RELEX 463

БЕЛЕЖКА

От:	Председателството
До:	Съвета
№ предх. док.:	8834/18
№ док. Ком.:	12183/17
Относно:	Предложение за РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно ENISA — Агенцията на ЕС за киберсигурност, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“) — Общ подход

I. ВЪВЕДЕНИЕ

1. На 13 септември 2017 г. в контекста на своята стратегия за цифров единен пазар Комисията прие и представи на Съвета и на Европейския парламент посоченото по-горе предложение[1], с правно основание член 114 от ДФЕС. Като част от т.нар. „пакет за киберсигурността“ това предложение цели постигането на високо равнище на киберсигурност, киберустойчивост и доверие в рамките на Съюза с оглед да се гарантира правилното функциониране на вътрешния пазар.

2. В предложения регламент се определят целите, задачите и организационните аспекти на ENISA — Агенцията на Европейския съюз за киберсигурност, и се установява рамка за създаването на европейски схеми за сертифициране на киберсигурността, с цел да се гарантира подходящо ниво на киберсигурността на ИКТ продукти и услуги в Съюза. Предложението на Комисията се придружава от оценка на въздействието, в която се разглеждат определен набор от осем варианта на политиката, които обхващат прегледа на мандата на ENISA и сертифицирането на киберсигурността на ИКТ.

3. Предложеният регламент съдържа две основни направления:

   - постоянен мандат на Агенцията с определен обхват с оглед на потребностите в рамките на новите приоритети и инструменти на политиката и обновен набор от задачи и функции на Агенцията, за да се даде възможност за ефективна и ефикасна подкрепа на усилията на държавите членки, институциите на ЕС и други заинтересовани страни за гарантиране на сигурно киберпространство;

   - Европейска рамка за сертифициране на киберсигурността за ИКТ продукти и услуги и правила относно европейските схеми за сертифициране на киберсигурността, позволяващи издаваните по тези схеми сертификати да бъдат валидни и признати във всички държави членки и да се преодолее съществуващата в момента разпокъсаност на пазара.

[1] Док. 12183/17; Док. 12183/1/17 REV 1; Док. 12183/2/17 REV 2.

4. През октомври 2017 г. Европейският съвет[2] призова предложенията на Комисията във връзка с киберсигурността да се разработват чрез цялостен подход, да се представят своевременно и да се разглеждат без забавяне, въз основа на план за действие, който да бъде изготвен от Съвета.

5. На 12 декември 2017 г. Съветът по общи въпроси прие плана за действие[3] за изпълнение на заключенията на Съвета[4] относно съвместното съобщение[5] до Европейския парламент и Съвета: „Устойчивост, възпиране и отбрана: изграждане на силна киберсигурност за ЕС“. Планът за действие отразява амбицията на Съвета до юни 2018 г. да бъде постигнат общ подход по предложението.

6. В Европейския парламент за докладчик беше определена г-жа Ангелика НИБЛЕР (ITRE, EPP). Гласуването в Комисията по промишленост, изследвания и енергетика е насрочено за 19 юни 2018 г.

7. Европейският икономически и социален комитет прие своето становище на 14 февруари 2018 г.

II. РАБОТА В РАМКИТЕ НА СЪВЕТА

8. Комисията представи това предложение и оценката на въздействието към него на Хоризонталната работна група по въпроси на кибернетичното пространство (наричана по-долу „работната група“) на 26 септември 2017 г., като впоследствие оценката на въздействието беше разгледана в рамките на работната група на 20 октомври 2017 г. Последващите обсъждания бяха съсредоточени върху оперативния капацитет на Агенцията и обхвата на взаимодействието с националните компетентни органи, както и върху въздействието на рамката за сертифициране по отношение на пазара и конкурентоспособността на предприятията. Като цяло отзивите на делегациите бяха положителни както по отношение на предложението, така и на оценката на въздействието.

---

2 EUCO 14/17, точка 11.
3 Док. 15748/17.
4 Док. 14435/17.
5 Док. 12211/17.

9. Обсъждането на самото предложение от работната група започна през ноември 2017 г. по време на естонското председателство и продължи в рамките на българското председателство. По предложението бяха проведени 12 заседания, което доведе до осем негови последователни преработени текста с оглед постигане на общ подход на предстоящото заседание на Съвета по транспорт, телекомуникации и енергетика (Телекомуникации), което ще се проведе на 8 юни 2018 г.

10. Резултатите от обсъжданията в работната група, проведени на 14—15 май 2018 г., както и преработеният компромисен текст на председателството, се съдържат в приложението към настоящата бележка. Съображенията са адаптирани, за да се отразят промените в разпоредбите от постановителната част. Всички промени спрямо предложението на Комисията са обозначени с **получер шрифт** или квадратни скоби [...]. Промените спрямо последния документ на работната група (8834/18) са обозначени с **получер шрифт и подчертаване**, а всички заличавания — с квадратни скоби и подчертаване **[...]**.

III. ЗАКЛЮЧЕНИЕ

11. Приложеният компромисен текст на председателството отразява усилията на председателството и държавите членки за постигане на подходящ баланс в текста.

12. На 25 май 2018 г. Комитетът на постоянните представители постигна споразумение по компромисния текст на председателството, при условие че бъдат приети измененията в член 19, параграф 5 и член 48, параграф 5, изложени в приложението.

13. Поради това Съветът се приканва да приеме общ подход на заседанието си на 8 юни 2018 г. и да даде мандат на председателството за започване на преговори с представителите на Европейския парламент и Европейската комисия по това досие.

ПРИЛОЖЕНИЕ

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно ENISA — *[...] Агенцията на Европейския съюз за киберсигурност*, и за отмяна на Регламент (ЕС) № 526/2013, както и относно сертифицирането на киберсигурността на информационните и комуникационните технологии („Акт за киберсигурността“)

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[6],

като взеха предвид становището на Комитета на регионите[7],

в съответствие с обикновената законодателна процедура,

[6] ОВ С,, стр. .
[7] ОВ С,, стр. .

като имат предвид, че:

(1) Мрежовите и информационните системи и далекосъобщителните мрежи и услуги играят жизненоважна роля за обществото и са се превърнали в основата на икономическия растеж. Информационните и комуникационните технологии са в основата на сложните системи, които поддържат обществената активност, правят възможно функционирането на нашите икономики в основни сектори като здравеопазване, енергетика, финанси и транспорт, и по-специално поддържат функционирането на вътрешния пазар.

(2) Използването на мрежовите и информационните системи от гражданите, предприятията и правителствата в целия Европейския съюз е вече повсеместно. Цифровизацията и свързаността се превръщат в основни характеристики на все по-голям брой продукти и услуги и с навлизането на „интернет на нещата“ се очаква на територията на ЕС през следващото десетилетие да има милиони, дори милиарди, свързани цифрови устройства. Въпреки нарастващия брой на устройствата, свързани към интернет, вграждането на сигурност и устойчивост в тях „още при проектирането“ все още не се извършва в задоволителен мащаб, което води до недостатъчно ниво на киберсигурността. В този контекст, ограниченото използване на сертифицирането води до недостиг на информация за ползвателите (организации и частни лица) относно характеристиките на ИКТ продукти и услуги в областта на киберсигурността, като подкопава доверието в цифровите решения.

(3) Нарастването на цифровизацията и свързаността доведе до увеличаване на рисковете, свързани с киберсигурността, като по този начин обществото като цяло стана по-уязвимо за киберзаплахи и се изостриха опасностите за физически лица, включително уязвими лица, като например деца. С цел да се смекчи този риск за обществото, трябва да бъдат предприети всички необходими действия за подобряване на киберсигурността в ЕС, за по-добра защита срещу киберзаплахи на мрежовите и информационните системи, далекосъобщителните мрежи, цифровите продукти, услуги и устройства, използвани от гражданите, правителствата и предприятията — от МСП до операторите на критични инфраструктури.

(4) Броят на кибератаките нараства, а икономиката и обществото, които са свързани с интернет, са по-уязвими за киберзаплахи и кибератаки и имат нужда от засилени защитни механизми. Независимо от факта обаче, че кибератаките често са трансгранични, политическият отговор на органите по киберсигурността и правоприлагащите правомощия са основно национални. Широкомащабните киберинциденти могат да нарушат предоставянето на важни услуги в целия ЕС. Това изисква ефективен отговор и ефективно управление на кризи на равнището на ЕС, които да се основават на специални политики и по-широкообхватни инструменти за европейска солидарност и взаимопомощ. Освен това редовното оценяване на състоянието на киберсигурността и устойчивостта в Съюза въз основа на надеждни данни на Съюза, както и систематичното прогнозиране на бъдещи развития, предизвикателства и заплахи както на равнище на Съюза, така и на световно равнище, е важно за разработчиците на политики, за промишлеността и ползвателите.

(5) В светлината на предизвикателствата, пред които е изправен Съюзът в областта на киберсигурността, е необходим всеобхватен набор от мерки, който ще се основава на предходни действия на Съюза и ще насърчава взаимно подкрепящите се цели. Това включва необходимостта от допълнително подобряване на способностите и подготвеността на държавите членки и на предприятията, както и от подобряване на сътрудничеството и координацията между държавите членки и институциите, агенциите и органите на ЕС. Освен това, предвид трансграничния характер на киберзаплахите е необходимо да се доразвият способностите на равнището на Съюза, чрез които могат да се допълват действията на държавите членки, по-специално в случаите на мащабни трансгранични киберинциденти и киберкризи. Също така са необходими допълнителни усилия, за да се повиши информираността на гражданите и на предприятията по въпроси, свързани с киберсигурността. Освен това доверието в цифровия единен пазар следва да бъде допълнително подобрено, като се предоставя прозрачна информация за нивото на сигурност на ИКТ продукти и услуги. Това може да бъде улеснено чрез сертифициране на равнище ЕС, като се предоставят общи изисквания относно киберсигурността и общи критерии за оценка, независещи от националните пазари и секторите. През 2004 г.

(6) Европейският парламент и Съветът приеха Регламент (ЕО) № 460/2004[8] относно създаването на ENISA, предназначен да подпомогне целите за осигуряване на високо ниво на мрежова и информационна сигурност в рамките на Съюза и създаване на култура на мрежова и информационна сигурност в полза на гражданите, потребителите, предприятията и държавните администрации. През 2008 г. Европейският парламент и Съветът приеха Регламент (ЕО) № 1007/2008[9] за удължаване на мандата на Агенцията до март 2012 г. С Регламент (ЕС) № 580/2011[10] мандатът на Агенцията беше удължен допълнително до 13 септември 2013 г. През 201 г. Европейският парламент и Съветът приеха Регламент (ЕС) № 526/2013[11] относно ENISA и за отмяна на Регламент (ЕО) № 460/2004, с който мандатът на Агенцията беше удължен до юни 2020 г.

---

[8] Регламент (ЕО) № 460/2004 на Европейския парламент и на Съвета от 10 март 2004 г. относно създаване на Европейската агенция за мрежова и информационна сигурност (ОВ L 77, 13.3.2004 г., стр. 1).

[9] Регламент (ЕО) № 1007/2008 на Европейския парламент и на Съвета от 24 септември 2008 г. за изменение на Регламент (ЕО) № 460/2004 относно създаване на Европейска агенция за мрежова и информационна сигурност по отношение на срока на съществуване на агенцията (ОВ L 293, 31.10.2008 г., стр. 1).

[10] Регламент (ЕС) № 580/2011 на Европейския парламент и на Съвета от 8 юни 2011 г. за изменение на Регламент (ЕО) № 460/2004 относно създаване на Европейската агенция за мрежова и информационна сигурност по отношение на срока на съществуване на агенцията (ОВ L 165, 24.6.2011 г., стр. 3).

[11] Регламент (ЕС) № 526/2013 на Европейския парламент и на Съвета от 21 май 2013 година относно Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) и за отмяна на Регламент (ЕО) № 460/2004 (ОВ L 165, 18.6.2013 г., стр. 41).

(7) Съюзът вече предприе важни стъпки за гарантиране на киберсигурността и за повишаване на доверието в цифровите технологии. През 2013 г. беше приета стратегия на ЕС за киберсигурност, която да направлява политиката на Съюза в отговор на заплахите и рисковете в областта на киберсигурността. В усилията си да защити по-добре европейските граждани в онлайн средата, през 2016 г. Съюзът прие първия законодателен акт в областта на киберсигурността — Директива (ЕС) 2016/1148 относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза („Директива за МИС“). С Директивата за МИС бяха въведени изисквания по отношение на националните способности в областта на киберсигурността, бяха създадени първите механизми за засилване на стратегическото и оперативното сътрудничество между държавите членки и бяха въведени задължения относно мерките за сигурност и уведомяването за инциденти отвъд границите на отделните сектори, които са жизненоважни за икономиката и обществото, като например енергетиката, транспорта, водните ресурси, банковото дело, инфраструктурите на финансовия пазар, здравеопазването, цифровата инфраструктура, както и доставчиците на основни цифрови услуги (интернет търсачки, услуги за изчисления в облак и платформи за онлайн търговия). ENISA получи основна роля в областта на подпомагането на изпълнението на директивата. В допълнение, ефективна борба срещу киберпрестъпността е важен приоритет в Европейската програма за сигурност, като допринася за общата цел за постигане на високо равнище на киберсигурността.

(8) Отчита се, че след приемането на Стратегията на ЕС за киберсигурност от 2013 г. и след последното преразглеждане на мандата на Агенцията общият контекст на политиката се е променил значително, също и във връзка с по-нестабилната и по-несигурна глобална среда. В този смисъл и в рамките на новата политика в областта на киберсигурността на Съюза е необходимо да се направи преглед на мандата на ENISA, за да се определи нейната роля в променената екосистема на киберсигурността и да се гарантира нейният ефективен принос към борбата с предизвикателствата за киберсигурността в Съюза, произтичащи от тази коренно променена картина на заплахите, за които настоящият мандат не е достатъчен, както беше констатирано в оценката на Агенцията.

(9) Агенцията, която се създава с настоящия регламент, следва да бъде правоприемник на агенцията ENISA, създадена с Регламент (ЕС) № 526/2013. Агенцията следва да изпълнява задачите, възложени ѝ с настоящия регламент и правните актове на Съюза в областта на киберсигурността, като, наред с другото, предоставя експертен опит и консултации и действа като център на Съюза за информация и знания. Тя следва да насърчава обмена на добри практики между държавите членки и заинтересовани страни от частния сектор, да предоставя предложения за политики на Европейската комисия и държавите членки, да действа като отправна точка за секторни политически инициативи на Съюза по въпросите на киберсигурността, да насърчава оперативното сътрудничество между държавите членки, както и между тях и европейските институции, агенции и органи.

(10) В рамките на Решение № 2004/97/ЕО, Евратом, прието на заседанието на Европейския съвет на 13 декември 2003 г., представителите на държавите членки решиха, че седалището на ENISA ще бъде в град в Гърция, който ще бъде определен от гръцкото правителство. Приемащата Агенцията държава членка следва да осигури възможно най-добрите условия за безпроблемното и ефективно функциониране на Агенцията. За правилното и ефикасно изпълнение на задачите на Агенцията, за целите на набирането на персонал и задържането му и за подобряване на ефикасността на дейностите за осъществяване на връзки е наложително Агенцията да се установи в подходящо местоположение, което наред с другото да предоставя подходящи транспортни връзки и съоръжения за съпрузите и децата, придружаващи членовете на персонала на Агенцията. Необходимите разпоредби следва да бъдат определени в споразумение между Агенцията и приемащата държава членка, което се сключва след получаване на одобрението на управителния съвет на Агенцията.

(11) Като се има предвид нарастващият брой на предизвикателствата в областта на киберсигурността, пред които е изправен Съюзът, предоставените на Агенцията финансови и човешки ресурси следва да бъдат увеличени, така че да отразяват нейната разширена роля, нейните задачи, както и нейната ключова позиция в екосистемата на организациите, които защитават европейската цифрова екосистема.

(12) Агенцията следва да постигне и запази високо равнище на експертен опит и да функционира като отправна точка, създавайки условия за увереност и доверие в единния пазар благодарение на своята независимост, качеството на предоставяните от нея консултации и разпространяваната от нея информация, на прозрачността на своите процедури и методи на работа, както и на добросъвестното изпълнение на възложените ѝ задачи. Агенцията следва да **подпомага** [...] усилията на национално равнище и да **дава активен принос към** усилията на равнището на Съюза, като същевременно изпълнява своите задачи в пълно сътрудничество с институциите, [...] агенциите **и органите** на Съюза, както и с държавите членки. Освен това работата на Агенцията следва да се основава на приноса и на сътрудничеството с частния сектор и с други заинтересовани страни. В набор от задачи следва да се формулира как Агенцията трябва да постига своите цели и същевременно да ѝ се предоставя възможност за гъвкаво функциониране.

(13) Агенцията следва да подпомага Комисията чрез консултации, становища и анализи по всички въпроси на Съюза, свързани с разработването, актуализирането и преразглеждането на политиката и законодателството в областта на киберсигурността **и специфичните за сектора аспекти с цел засилване на значението на политиките и законодателството на ЕС, свързани с киберсигурността, и осигуряване на последователност при прилагането им на национално равнище** [...]. Агенцията следва да служи като отправна точка за консултации и експертен опит за специфичните секторни политики и правни инициативи на Съюза, когато те включват въпроси, свързани с киберсигурността.

(14) Основната задача на Агенцията е да насърчава последователното прилагане на съответната правна рамка, по-конкретно на ефективното изпълнение на Директивата за МИС, която е от съществено значение за повишаване на киберустойчивостта. С оглед на бързо развиващата се картина на заплахите за киберсигурността е ясно, че държавите членки трябва да бъдат подкрепяни чрез по-широкообхватен подход, надхвърлящ границите на отделните политики, за изграждането на киберустойчивост.

(15) Агенцията следва да подпомага държавите членки и институциите, [...] агенциите **и органите** на Съюза в усилията им да изградят и подобрят способностите си и подготвеността си за предотвратяване, откриване и реагиране на [...] **заплахи** и инциденти в областта на киберсигурността, както и във връзка със сигурността на мрежовите и информационните системи. По-специално, Агенцията следва да подкрепя развитието и укрепването на националните екипи CSIRT с оглед постигане на високо общо равнище на тяхната зрелост в Съюза. **Осъществяваните от ENISA дейности, свързани с оперативния капацитет на държавите членки, следва единствено да допълват действията на държавите членки с цел изпълнение на задълженията им, произтичащи от Директивата за МИС, а не да ги заменят** [...].

(15a) Агенцията следва също да съдейства за разработването и актуализирането на стратегиите на Съюза, а при поискване — на стратегиите на държавите членки, относно сигурността на мрежовите и информационните системи, по-специално в областта на киберсигурността, да насърчава тяхното разпространение и да следи изпълнението им. Също така, Агенцията следва да предлага обучения и образователни материали за публичните органи и, когато е целесъобразно, да „обучава обучаващите“, с цел да подпомогне държавите членки при развитието на техни собствени способности за обучение.

(16) Агенцията следва да подпомага групата за сътрудничество, създадена с Директивата за МИС, в изпълнението на нейните задачи, по-специално чрез предоставяне на експертен опит и консултации, и да улеснява обмена на най-добри практики, по-специално по отношение на определянето на операторите на основни услуги от държавите членки, включително по отношение на трансграничната зависимост във връзка с рисковете и инцидентите.

(17) С оглед на насърчаването на сътрудничеството между обществения и частния сектор и в рамките на частния сектор, [...] **Агенцията следва** да подпомага **обмена на информация в секторите и между тях, по-специално в секторите, изброени в приложение II към Директива (ЕС) 2016/1148, като им предоставя най-добри практики и насоки относно наличните инструменти, процедури, както и насоки относно начините за справяне с нормативните проблеми във връзка с обмена на информация, например чрез улесняване** [...] на създаването на секторни центрове за споделяне и анализ на информация (ISAC) [...].

(18) Агенцията следва да обобщава и анализира **доброволно подадените** национални доклади от CSIRT и CERT-EU **с цел подпомагане на държавите членки** при създаването на общи [...] **процедури**, език и терминология за обмен на информация. Агенцията следва също така да включи частния сектор, в рамките на Директивата за МИС, с която бяха положени основите за доброволен обмен на техническа информация на оперативно равнище [...] **в рамките на** мрежата на CSIRT.

(19) Агенцията следва да допринася за реакцията на равнището на ЕС в случай на мащабни трансгранични инциденти и кризи в областта на киберсигурността. Тази функция следва **да бъде изпълнявана в съответствие с мандата на Агенцията съгласно настоящия регламент и подход, който да бъде съгласуван от държавите членки в контекста на препоръката на Комисията относно координирана реакция на мащабни киберинциденти и кризи. Тя може** да включва събирането на съответна информация и поемането на ролята на посредник между мрежата на CSIRT, техническата общност и отговорните за вземане на решения лица, натоварени с управлението на кризи. Освен това на Агенцията би могла да спомогне за справянето с инциденти в технически аспект, като улесни съответния технически обмен на решения между държавите членки и даде своя принос за публичното осведомяване. Агенцията следва да подкрепя процеса, като проверява как функционира това сътрудничество чрез [...] **редовни** учения в областта на киберсигурността.

(20) [...] **При подпомагане** на оперативното **сътрудничество** [...] Агенцията следва да използва наличния **технически и оперативен** експертен опит на CERT-EU чрез структурирано сътрудничество [...]. [...] Когато е целесъобразно, следва да бъдат сключени специални договорености между двете организации, за да се определи практическото изражение на такова едно сътрудничество **и да се избегне дублирането на дейности**.

(21) В съответствие със [...] задачите си **за подпомагане на оперативното сътрудничество в рамките на мрежата CSIRT** Агенцията следва да е в състояние да оказва подкрепа на държавите членки **по тяхно искане**, например като предоставя консултации **относно начините за подобряване на техния капацитет за предотвратяване, откриване и реагиране на инциденти, като [...] улеснява справянето** [...] в технически аспект **с инциденти със значително или съществено въздействие** [...] или **като** осигурява анализи на заплахите и инцидентите. **Спомагането за справянето в технически аспект с инциденти със значително или съществено въздействие следва да включва по-специално подкрепата от страна на ENISA по отношение на доброволния обмен на технически решения между държавите членки или изготвянето от нейна страна на комбинирана техническа информация, например технически решения, която доброволно се подава от държавите членки.** В препоръката на Комисията за координирана реакция при мащабни инциденти и кризи в областта на киберсигурността се препоръчва държавите членки да си сътрудничат добросъвестно и да обменят информация помежду си и с ENISA относно мащабни инциденти и кризи в областта на киберсигурността без излишно забавяне. Тази информация следва допълнително да помогне на ENISA при [...] **подкрепата на оперативното сътрудничество**.

(22) Като част от редовното сътрудничество на техническо равнище за подпомагане на ситуационната осведоменост на Съюза, Агенцията следва редовно **и в тясно сътрудничество с държавите членки** да изготвя технически доклади за състоянието на киберсигурността в ЕС във връзка с инциденти и заплахи въз основа на публично достъпна информация, свои собствени анализи, както и доклади, подадени от CSIRT на държавите членки [...] или от единните звена за контакт съгласно Директивата за МИС **(и двете на доброволна основа)**, Европейския център за борба с киберпрестъпността към Европол (EC3) към Европол, CERT-EU, и когато е целесъобразно — от Центъра на ЕС за анализ на информация (INTCEN) към Европейската служба за външна дейност (ЕСВД). Докладите следва да се предоставят на съответните служби на Съвета, Комисията, върховния представител на Съюза по въпросите на външните работи и политиката на сигурност и мрежата на CSIRT.

(23) **Подкрепата на Агенцията по отношение на** [...] последващи технически **разследвания** [...] **на** инциденти със значително въздействие [...] по искане [...] на [...] **съответните** държави членки следва да се съсредоточи върху предотвратяването на бъдещи инциденти [...]. **Съответните държави членки следва да предоставят необходимата информация с цел да се позволи на Агенцията ефективно да подпомага техническото разследване.**

(24) [...]

(25) Държавите членки могат да приканят засегнати от инцидента предприятия да сътрудничат, като предоставят необходимата информация и съдействие на Агенцията, без да се накърнява правото им на защита на поверителната търговска информация.

(26) С оглед да се разберат по-добре предизвикателствата в областта на киберсигурността и да се предоставят стратегически дългосрочни препоръки на държавите членки и институциите на Съюза, Агенцията трябва да анализира текущите и нововъзникващи рискове. За тази цел Агенцията, в сътрудничество с държавите членки и, по целесъобразност, със статистически органи и други организации, следва да събира съответната **публично достъпна или доброволно подадена** информация, да извършва анализи на нововъзникващите технологии и да предоставя тематични оценки на очаквани социални, правни, икономически и регулаторни въздействия на дадени технологични иновации в областта на мрежовата и информационната сигурност, по-специално в областта на киберсигурността. Освен това Агенцията следва да подпомага държавите членки и институциите, агенциите и органите на Съюза при установяването на възникващите тенденции и предотвратяването на [...] **инциденти**, свързани с киберсигурността, като извършва анализи на заплахите и инцидентите.

(27) С цел да се повиши устойчивостта на Съюза, Агенцията следва да развие върхов капацитет в областта на **киберс**игурността на **инфраструктурите, подпомагащи по-специално секторите, изброени в приложение II към Директивата за МИС, и инфраструктурите, използвани от доставчиците на цифрови услуги, изброени в приложение III към същата директива,** като предоставя съвети, насоки и най-добри практики. С оглед да се осигури по-лесен достъп до по-добре структурирана информация относно рисковете за киберсигурността и потенциалните средства за защита, Агенцията следва да разработи и поддържа „информационен център“ на Съюза — един вид портал за „обслужване на едно гише“, който осигурява на обществеността информация относно киберсигурността, получена от европейските и националните институции, агенции и органи.

(28) Агенцията следва да допринася за повишаването на обществената осведоменост относно рисковете, свързани с киберсигурността, и да предлага насоки и добри практики за отделните ползватели, насочени към гражданите и организациите. Агенцията следва също така да допринася за насърчаване на най-добрите практики и решения на равнището на отделни лица и организации, като събира и анализира обществено достъпна информация относно значителни инциденти и изготвя доклади, с цел да се предоставят насоки за предприятията и гражданите и да се подобри цялостното ниво на подготвеност и устойчивост. Освен това Агенцията следва да организира, в сътрудничество с институциите, [...] агенциите и **органите** на Съюза и държавите членки, редовни разяснителни и обществени образователни кампании за крайните ползватели, насочени към насърчаването на по-безопасно индивидуално поведение онлайн и повишаване на осведомеността относно потенциалните заплахи в киберпространството, включително относно киберпрестъпления като фишинг, ботмрежи, финансови и данъчни измами, а също така насочени към разпространението на основни съвети относно автентификацията и защитата на данните. Агенцията следва да играе централна роля за по-бързото осведомяване на крайните ползватели относно сигурността на изделията.

(29) За да се подпомогнат предприятията, извършващи дейност в сектора на киберсигурността, както и ползвателите на решения в областта на киберсигурността, Агенцията следва да разработи и поддържа „обсерватория на пазара“, като извършва редовни анализи и разпространява информация за основните тенденции на пазара на киберсигурността, както по отношение на търсенето, така и по отношение на предлагането.

(30) С цел да се гарантира, че Агенцията ще постигне напълно своите цели, тя следва да си сътрудничи със съответните институции, агенции и органи, в това число CERT-EU, Европейския център за борба с киберпрестъпността към Европол (EC3 към Европол), Европейската агенция по отбрана (EDA), Европейската агенция за оперативното управление на широкомащабни информационни системи (eu-LISA), Европейската агенция за авиационна безопасност (ЕААБ), **Европейската агенция за глобални навигационни спътникови системи (Агенция за ГНСС)** и всяка друга агенция на ЕС, която действа в областта на киберсигурността. Тя следва също така да поддържа връзка с органите, които работят в областта на защитата на данните, с цел да обменя с тях ноу-хау и най-добри практики и да предоставя консултации относно аспекти на киберсигурността, които биха могли да окажат влияние върху тяхната работа. Правоприлагащите органи на национално равнище и на равнището на Съюза и органите за защита на данните следва да имат правото да бъдат представлявани в Постоянната група на заинтересованите страни на Агенцията. При сътрудничеството си с правоприлагащите органи по въпроси на мрежовата и информационната сигурност, които биха могли да окажат влияние върху тяхната работа, Агенцията следва да спазва съществуващите информационни канали и изградени мрежи.

(31) Агенцията, **в ролята си** на [...] секретариат на мрежата на CSIRT, следва да подкрепя екипите CSIRT на държавите членки и екипите CERT-EU при оперативното сътрудничество в допълнение към всички съответни задачи на мрежата на CSIRT, както е определено в Директивата за МИС. Наред с това Агенцията следва да насърчава и подкрепя сътрудничеството между съответните екипи CSIRT в случай на инциденти, атаки или нарушения в работата на мрежите или инфраструктурата, управлявани или защитавани от екипите CSIRT, които включват, действително или потенциално, най-малко два екипа CERT, като същевременно взема предвид надлежно стандартните оперативни процедури на мрежата на CSIRT.

(32) С оглед повишаване на подготвеността на Съюза за реагиране на киберинциденти, Агенцията следва да организира [...] **редовни** учения в областта на киберсигурността на равнището на Съюза и да помага на държавите членки и на институциите, агенциите и органите на ЕС, по тяхно искане, при организирането на учения.

(33) Агенцията следва да продължава да развива и поддържа своя експертен опит в областта на сертифицирането на киберсигурността, с цел да подпомага политиките на Съюза в тази област. Агенцията следва да насърчава внедряването на сертифицирането на киберсигурността, включително като допринася за създаването и поддържането на мрежа за сертифициране на киберсигурността на равнище ЕС, с цел повишаване на прозрачността при обезпечаването на ИКТ продукти и услуги и, в крайна сметка, укрепване на доверието в цифровия вътрешен пазар.

(34) Ефективните политики за киберсигурност следва да се основават на добре разработени методи за оценяване на риска както в публичния, така и в частния сектор. Методите за оценка на риска се използват на различни нива, без да има обща практика относно най-добрия начин за тяхното ефикасно прилагане. Популяризирането и развитието на най-добри практики за оценяване на риска и за оперативно съвместими решения за управление на риска в организациите от публичния и частния сектор ще повиши нивото на киберсигурността в Съюза. За целта Агенцията следва да подкрепя сътрудничеството между заинтересовани страни на равнището на Съюза, като улеснява техните усилия, свързани с въвеждането и използването на европейски и международни стандарти за управление на риска и за измерима сигурност на електронните продукти, системи, мрежи и услуги, които заедно със софтуера са елементите, образуващи мрежовите и информационните системи.

(35) Агенцията следва да насърчава държавите членки и доставчиците на услуги да повишават общите си стандарти за сигурност, така че всички ползватели на интернет да вземат необходимите мерки за гарантиране на собствената си киберсигурност. По-специално, доставчиците на услуги и създателите на продукти следва да оттеглят или рециклират продукти и услуги, които не отговарят на стандартите за киберсигурност. В сътрудничество с компетентните органи, ENISA може да разпространява информация относно равнището на киберсигурността на продуктите и услугите, предлагани на вътрешния пазар, и да отправя предупреждения по отношение на доставчиците и производителите и да изисква от тях да подобрят сигурността, включително киберсигурността, на своите продукти и услуги.

(36) Агенцията следва да взема под внимание в пълна степен текущата научноизследователска и развойна дейност и дейностите за оценка на технологиите, по-специално тези, провеждани от различните научноизследователски инициативи на Съюза, за да съветва институциите, [...] агенциите **и органите** на Съюза и, когато е необходимо, държавите членки, по тяхно искане, относно необходимостта от научни изследвания в областта на [...] киберсигурността. **С цел определяне на научноизследователските нужди и приоритети Агенцията следва също така да се консултира със съответните групи ползватели.**

(37) **Заплахите** [...] за киберсигурността представляват глобален проблем. Необходимо е по-тясно международно сътрудничество с цел подобряване на стандартите за **кибер**сигурност, включително определяне на общи норми за поведение, обмен на информация, насърчаване на по-бързи форми на международно сътрудничество при реагиране на проблеми на мрежовата и информационната сигурност, както и общ глобален подход към такива проблеми. За тази цел Агенцията следва да подкрепя по-задълбоченото ангажиране на Съюза и сътрудничеството с трети държави и международни организации, като предоставя, където е уместно, необходимия експертен опит и анализи на съответните институции, [...] агенции **и органи** на Съюза.

(38) Агенцията следва да бъде в състояние да реагира на ad hoc искания за консултации и помощ от страна на държавите членки и институциите, агенциите и органите на ЕС, попадащи в обхвата на нейните цели.

(39) Необходимо е да се прилагат определени принципи по отношение на управлението на Агенцията с цел спазване на съвместното изявление и общия подход, договорени от междуинституционалната работна група за децентрализираните агенции на ЕС през юли 2012 г., чиято цел е усъвършенстването на дейността на агенциите и подобряването на техните резултати. Съвместното изявление и общият подход следва да се отчитат, когато е уместно, в работните програми на Агенцията, нейните оценки, както и в докладването и административната практика на Агенцията.

(40) Управителният съвет, състоящ се от държавите членки и Комисията, следва да определя общата насока на дейността на Агенцията и да гарантира, че тя изпълнява своите задачи в съответствие с настоящия регламент. Управителният съвет следва да получи правомощията, необходими за определяне на бюджета, проверка на неговото изпълнение, приемане на подходящи финансови правила, установяване на прозрачни работни процедури за вземане на решения от страна на Агенцията, приемане на единния програмен документ на Агенцията, приемане на собствен правилник за дейността на Агенцията, назначаване на изпълнителния директор и вземане на решения за удължаване или прекратяване на неговия мандат.

(41) С оглед на правилното и ефективно функциониране на Агенцията Комисията и държавите членки следва да гарантират, че лицата, назначени в управителния съвет, притежават подходяща професионална компетентност, както и опит в областите на работа. Държавите членки и Комисията следва също да положат усилия да намалят текучеството на своите съответни представители в управителния съвет, за да се гарантира непрекъснатост на работата му.

(42) Гладкото функциониране на Агенцията налага нейният изпълнителен директор да се назначава въз основа на неговите заслуги и документирани административни и управленски умения, както и въз основа на неговите компетентност и опит, свързани с киберсигурността, като той трябва да изпълнява задълженията си в условия на пълна независимост. Изпълнителният директор следва да изготви предложение за работна програма на Агенцията след предварителни консултации с Комисията и да предприеме всички необходими стъпки за гарантиране на правилното изпълнение на работната програма на Агенцията. Изпълнителният директор следва да изготвя ежегоден доклад, **включващ изпълнението на годишната работна програма на Агенцията**, който да бъде представян на управителния съвет, да съставя проект на разчета за предвидените приходи и разходи на Агенцията, както и да изпълнява бюджета. Освен това, изпълнителният директор следва да разполага с възможността да сформира ad hoc работни групи за решаване на специфични въпроси, по-специално с научен, технически, правен или социално-икономически характер. Изпълнителният директор следва да гарантира, че членовете на ad hoc работните групи се избират съобразно най-високите стандарти за експертни знания, като надлежно се отчита балансът при представянето, в зависимост от конкретния въпрос, между държавните администрации на държавите членки, институциите на Съюза и частния сектор, включително индустрията, ползвателите и академични експерти в областта на мрежовата и информационната сигурност.

(43) Изпълнителният съвет следва да допринася за ефективното функциониране на управителния съвет. Като част от подготвителната си работа във връзка с решенията на управителния съвет той следва да разглежда подробно съответната информация, да проучва възможните варианти и да предлага консултации и решения за изготвяне на съответните решения на управителния съвет.

(44) Агенцията следва да разполага с Постоянна група на заинтересованите страни в ролята на консултативен орган, за да се гарантира редовен диалог с частния сектор, потребителските организации и други подходящи заинтересовани страни. Постоянната група на заинтересованите страни, сформирана от управителния съвет по предложение на изпълнителния директор, следва да се съсредоточи върху въпроси, засягащи заинтересованите страни, и да насочва вниманието на Агенцията към тях. Съставът на Постоянната група на заинтересованите страни и задачите, които ѝ се възлагат — по-конкретно предоставянето на консултации относно проекта на работната програма — следва да гарантират достатъчна степен на представяне на заинтересованите страни в работата на Агенцията.

(45) Агенцията следва да има правила за предотвратяването и управлението на конфликти на интереси. Агенцията следва също така да прилага съответните разпоредби на Съюза относно публичния достъп до документи, както е посочено в Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета[12]. Агенцията следва да обработва лични данни в съответствие с Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни[13]. Агенцията следва да съблюдава разпоредбите, приложими за институциите на Съюза, както и националното законодателство относно обработката на информация, по-специално на чувствителната некласифицирана информация и на класифицирана информация на ЕС.

---

[12] Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета от 30 май 2001 г. относно публичния достъп до документи на Европейския парламент, на Съвета и на Комисията (ОВ L 145, 31.5.2001 г., стр. 43).

[13] ОВ L 8, 12.1.2001 г., стр. 1.

(46) За да се гарантира пълната автономност и независимост на Агенцията и за да може тя да изпълнява допълнителни и нови задачи, включително непредвидени задачи в спешни случаи, на Агенцията следва да бъде предоставен достатъчен и автономен бюджет, чиито приходи се набавят най-вече чрез вноска на Съюза и вноски на трети държави, вземащи участие в работата на Агенцията. По-голямата част от персонала на Агенцията следва да е пряко ангажирана с оперативното изпълнение на мандата на Агенцията. Приемащата държава членка или всяка друга държава членка следва да могат да правят доброволни вноски към приходите на Агенцията. Бюджетната процедура на Съюза следва да остане приложима по отношение на всякакви субсидии, платими от общия бюджет на Съюза. Освен това Сметната палата следва да одитира финансовите отчети на Агенцията, за да се гарантират прозрачност и отчетност.

(47) [...]

(48) Сертифицирането на киберсигурността играе важна роля за повишаването на доверието в ИКТ продуктите и услугите и на тяхната сигурност. Цифровият единен пазар, и по-конкретно основаващата се на данни икономика и „интернет на нещата“, могат да функционират успешно само ако обществото като цяло е уверено, че тези продукти и услуги предоставят определено ниво на обезпеченост в областта на киберсигурността. Свързаните автомобили и автомобилите с автоматично управление, електронните медицински устройства, системите за управление на промишлената автоматизация или интелигентните енергийни мрежи са само някои от примерите за сектори, в които сертифицирането вече широко се използва или е вероятно да бъде използвано в близко бъдеще. Секторите, регулирани от Директивата за МИС, са също така сектори, в които сертифицирането на киберсигурността е от ключово значение.

(49) В съобщението от 2016 г., озаглавено „Укрепване на отбранителната способност на Европа срещу кибератаки и изграждане на конкурентен и иновативен сектор на киберсигурността“, Комисията описа необходимостта от висококачествени, достъпни и оперативно съвместими продукти и решения, свързани с киберсигурността. Предлагането на ИКТ продукти и услуги в рамките на единния пазар остава обаче силно разпокъсано географски. Това е така, защото развитието на сектора на киберсигурността в Европа се основава главно на търсене от страна на националните правителства. Освен това, липсата на оперативно съвместими решения (технически стандарти), практики и прилагани в целия ЕС механизми за сертифициране е част от другите пропуски, които оказват влияние върху единния пазар на киберсигурността. От една страна, това влошава конкурентоспособността на европейските компании в национален, европейски и световен мащаб. От друга, то ограничава избора на надеждни и приложими технологии за киберсигурност, до които лицата и предприятията имат достъп. Аналогично, в междинния преглед на изпълнението на стратегията за цифровия единен пазар Комисията подчерта необходимостта от безопасни свързани продукти и системи и посочи, че създаването на Европейска рамка за ИКТ сигурност, определяща правила относно организацията на сертифицирането на сигурността на ИКТ в ЕС, би могло да помогне както за запазването на доверието в интернет, така и за преодоляването на настоящата разпокъсаност на пазара за киберсигурност.

(50) Понастоящем сертифицирането на киберсигурността на ИКТ **процеси,** продукти и услуги се използва само в ограничена степен. Ако има такова, то се осъществява предимно на равнището на държавите членки или в рамките на секторно обусловени схеми. В тези условия сертификат, издаден от един национален орган в областта на киберсигурността, по принцип не се признава от другите държави членки. Поради това може да се наложи предприятията да сертифицират своите продукти и услуги в няколко държави членки, в които развиват дейност, например с цел да участват в националните процедури за възлагане на обществени поръчки. Освен това, въпреки че се появяват нови схеми, изглежда няма съгласуван и цялостен подход по отношение на хоризонталните въпроси, свързани с киберсигурността, например в сферата на „интернет на нещата“. Действащите схеми проявяват съществени недостатъци и различия по отношение на продуктовия обхват, нивата на обезпеченост, съществените критерии и фактическото използване.

(51) В миналото бяха положени известни усилия за постигането на взаимно признаване на сертификати в Европа. Те обаче имаха само частичен успех. Най-важният пример в това отношение е споразумението за взаимно признаване (СВП) на Групата на висшите служители по сигурността на информационните системи (SOG-IS). Макар да представлява най-важният модел за сътрудничество и взаимно признаване в областта на сертифицирането на сигурността, [...] SOG-IS включва само част от държавите — членки на Съюза. Това ограничава ефективността на СВП на SOG-IS от гледна точка на вътрешния пазар.

(52) С оглед на посоченото по-горе е необходимо да се въведе Европейска рамка на сертифициране на киберсигурността, която да определя основните хоризонтални изисквания за европейските схеми за сертифициране на киберсигурността, които ще бъдат разработени, и да дава възможност сертификатите и **декларациите на ЕС за съответствие** за ИКТ продукти и услуги да бъдат признавани и използвани във всички държави членки. Европейската рамка следва да има две цели: от една страна, тя следва да спомогне за повишаване на доверието в ИКТ продуктите и услугите, които са били сертифицирани по такива схеми. От друга страна тя следва да предотврати увеличаването на броя на противоречащи си или припокриващи се национални сертификати за киберсигурност и по този начин да намали разходите за предприятията, упражняващи дейност на единния цифров пазар. Схемите следва да бъдат недискриминационни и да се основават на международни стандарти и/или [...] **европейски** стандарти, освен ако тези стандарти са неефективни или неподходящи за изпълнението на легитимните цели на ЕС в това отношение.

(53) Комисията следва да бъде оправомощена да приема европейски схеми за сертифициране на киберсигурността за специфични групи ИКТ **процеси,** продукти и услуги. Тези схеми следва да се прилагат и контролират от национални [...] органи за сертифициране на **киберсигурността**, а сертификатите, издадени в рамките на тези схеми, следва да са валидни и да се признават на цялата територия на Съюза. Схемите за сертифициране, управлявани от промишлеността или от други частни организации, следва да не попадат в обхвата на регламента. Въпреки това, управляващите такива схеми органи могат да предлагат на Комисията да ги разгледа като основа за схеми, които да бъдат одобрени като европейска схема.

(54) Разпоредбите на настоящия регламент не следва да засягат законодателство на Съюза, с което се определят специфични правила за сертифициране на ИКТ продукти и услуги. По-конкретно с Общия регламент относно защитата на данните (ОРЗД) се установяват разпоредби за създаване на механизми за сертифициране и на печати и маркировки за защита на данните, чрез които се доказва съответствието с посочения регламент на операциите по обработката на данни от страна на контрольорите и обработващите тези данни. Тези механизми за сертифициране и тези печати и маркировки за защита на данните следва да позволяват на субектите, предоставящи своите данни, бързо да оценяват нивото на защита на данните на съответните продукти и услуги. Настоящият регламент не засяга сертифицирането на операции по обработката на данни съгласно ОРЗД, включително когато тези операции са включени в продукти и услуги.

(55) Целта на европейските схеми за сертифициране на киберсигурността следва да бъде да се гарантира, че ИКТ **процесите**, продуктите и услугите, сертифицирани по такава схема, съответстват на специфицираните изисквания [...] **с** цел да се [...] **защити** наличността, автентичността, целостта и поверителността на съхраняваните, предавани или обработвани данни, или на свързаните с тях функции или услуги, предлагани от тези продукти, процеси, услуги и системи или достъпни чрез тях **през целия им жизнен цикъл**, по смисъла на настоящия регламент. Не е възможно в настоящия регламент да се определят подробно изискванията във връзка с киберсигурността на всички ИКТ **процеси,** продукти и услуги. ИКТ **процесите,** продуктите и услугите и техните потребности във връзка с киберсигурността са толкова разнообразни, че е много трудно да се формулират общи изисквания в областта на киберсигурността, които да са общовалидни. Поради това е необходимо да се приеме широко и общо понятие за киберсигурността за целите на сертифицирането, което да се допълва от набор от конкретни цели, свързани с киберсигурността, които трябва да бъдат вземани предвид при разработването на европейските схеми за сертифициране на киберсигурността. Условията, при които тези цели ще бъдат постигани при конкретни ИКТ **процеси,** продукти и услуги, следва да бъдат допълнително уточнявани в подробности на нивото на всяка отделна схема за сертифициране, приемана от Комисията, например чрез позоваване на стандарти или технически спецификации**, когато не са налице подходящи стандарти**.

(55а) Следва да се установят техническите спецификации, които да се използват в европейска схема за сертифициране на киберсигурността, като се спазват принципите, установени в приложение II към Регламент (ЕС) 1025/2012. Някои отклонения от тези принципи биха могли обаче да се счетат за необходими в надлежно обосновани случаи, когато тези технически спецификации трябва да се използват в европейска схема за сертифициране на киберсигурността, отнасяща се до високо ниво на обезпеченост. Причините за тези отклонения трябва да бъдат направени обществено достояние.

(55б) Сертифицираното оценяване на съответствието е процесът на оценяване на изпълнението на специфицираните изисквания, свързани с ИКТ процес, продукт или услуга. Този процес се осъществява от независима трета страна, различна от производителя на продукта или доставчика на услугата. След процеса на успешна оценка на ИКТ процес, продукт или услуга следва процесът на издаване на сертификат. Сертификатът следва да се счита за потвърждение, че съответната оценка е извършена правилно. В зависимост от нивото на обезпеченост, европейската схема за сертифициране на киберсигурността следва да предвижда дали сертификатът се издава от частен или публичен орган. Оценяването на съответствието и сертифицирането сами по себе си не могат да гарантират, че сертифицираните ИКТ продукти и услуги са сигурни по отношение на киберзаплахите. Те представляват само процедура и техническа методика за удостоверяване, че ИКТ продуктите и услугите са изпитани и отговарят на определени изисквания, свързани с киберсигурността, които са определени другаде, например в технически стандарти.

(55в) Изборът от страна на ползвателите на сертификати на подходящото равнище на сертифициране и свързаните с него изисквания по отношение на сигурността следва да се основават на анализ на риска по отношение на използването на ИКТ процеса, продукта или услугата. Поради това нивото на обезпеченост на сигурността следва да е съизмеримо със степента на риск, свързана с предвидената употреба на ИКТ процеса, продукта или услугата.

(55г) Дадена европейска схема за сертифициране на киберсигурността може да предвиди оценяване на съответствието при отговорност единствено на производителя или доставчика на ИКТ продукти и услуги (самооценка на съответствието). В такива случаи е достатъчно производителят или доставчикът сам да извърши всички проверки, за да гарантира съответствието на ИКТ процесите, продуктите или услугите със схемата за сертифициране. Този вид оценяване на съответствието следва да се счита за подходяща за ИКТ продукти и услуги с ниска степен на сложност (напр. опростен проект и производствен механизъм), които представляват малък риск за обществения интерес. Освен това единствено ИКТ продукти и услуги, съответстващи на основно ниво на обезпеченост, могат да подлежат на самооценка на съответствието.

(55д) Дадена европейска схема за сертифициране на киберсигурността може да даде възможност както за сертифициране, така и за самооценка на съответствието на ИКТ продукти и услуги. В този случай схемата следва да предоставя ясни и разбираеми способи за потребителите или други ползватели да направят разграничение между продукти и услуги, които са оценени при отговорността на производителя или доставчика, и продукти и услуги, които са сертифицирани от трета страна.

(55е) Производителят или доставчикът на ИКТ продукти и услуги, който прави самооценка на съответствието, следва да изготви и подпише декларация на ЕС за съответствие като част от процедурата за оценяване на съответствието. Декларацията на ЕС за съответствие е документът, в който се посочва, че конкретен ИКТ продукт или услуга отговаря на изискванията на схемата. Чрез изготвянето и подписването на декларация на ЕС за съответствие, производителят или доставчикът поема отговорност за съответствието на ИКТ продукта или услугата с правните изисквания на схемата. Копие от декларацията на ЕС за съответствие следва да се предостави на националния орган за сертифициране на киберсигурността и на ENISA.

(55ж) Производителят или доставчикът на ИКТ продукти и услуги следва да съхранява декларацията на ЕС за съответствие и техническата документация с цялата съответна информация, отнасяща се до съответствието на ИКТ продуктите или услугите с дадена схема, на разположение на компетентния национален орган за сертифициране на киберсигурността за срок, определен в конкретната европейска схема за сертифициране на киберсигурността. Техническата документация следва да определя приложимите изисквания и да обхваща дотолкова, доколкото е необходимо за нуждите на оценяването, проекта, производството и функционирането на ИКТ продукта или услугата. Техническата документация следва да е изготвена така, че да предоставя възможност за оценяване на съответствието на даден ИКТ продукт или услуга със съответните изисквания.

(55з) Държавите членки и организациите на заинтересованите страни следва да имат право да предлагат на Европейската група по сертифициране на киберсигурността изготвяне на проект за схема. Организациите на заинтересованите страни са организации на представители на отрасъла или потребителите, в т.ч. представители на организации на МСП, които имат действителен интерес от разработването на конкретна европейска схема за сертифициране на киберсигурността. Тези предложения следва да се разглеждат в светлината на критериите, разработени от Европейската група по сертифициране на киберсигурността съгласно насоки, основаващи се на принципите на прозрачност, откритост, безпристрастност, консенсус, ефективност, значимост и съгласуваност.

(56) На Комисията **и на Групата** следва да бъде предоставено правомощието да изискват от ENISA да подготвя **без ненужно забавяне** проекти за схеми за конкретни ИКТ **процеси,** продукти или услуги. Комисията следва да бъде оправомощена да приема посредством актове за изпълнение европейски схеми за сертифициране на киберсигурността въз основава на проекти за схеми, предложени от ENISA. Като се вземат предвид общата цел и целите, свързани със сигурността, определени в настоящия регламент, в европейските схеми за сертифициране на киберсигурността, приемани от Комисията, следва да бъде определен минимален набор от елементи по отношение на предмета, обхвата и функционирането на дадена схема. Те следва да включват, наред с другото, обхвата и предмета на сертифицирането на киберсигурността, включително обхванатите категории ИКТ **процеси,** продукти и услуги, подробна спецификация на изискванията в областта на киберсигурността, например чрез позоваване на стандарти или технически спецификации, конкретните критерии и методи за оценка, както и желаното ниво на обезпеченост: основно, значително и/или високо, **и нивата на обезпеченост, когато е приложимо**.

(56a) Обезпечаването чрез европейска схема за сертифициране е предпоставката да се гарантира, че даден ИКТ процес, продукт или услуга отговаря на изискванията за сигурност на конкретна европейска схема за сертифициране на киберсигурността. С цел да се гарантира последователността на рамката за сертифицирани ИКТ процеси, продукти и услуги, дадена европейска схема за сертифициране на киберсигурността може да определи нивата на обезпеченост за европейските сертификати за киберсигурност и декларациите на ЕС за съответствие, издавани в рамките на тази схема. Всеки сертификат може да се отнася до едно от следните нива на обезпеченост: основно, значително или високо, докато декларацията на ЕС за съответствие може да се отнася единствено до основното ниво на обезпеченост. Нивата на обезпеченост предвиждат съответстваща степен на усилия за оценката [...] и се характеризират с позоваване на техническите спецификации, стандарти и процедури, свързани с тях, в т.ч. технически проверки, чиято цел е да се смекчат или предотвратят инциденти в областта на киберсигурността. Всяко ниво на обезпеченост следва да бъде последователно по отношение на различните секторни области, в които се прилага сертифициране.

(56б) Дадена европейска схема за сертифициране на киберсигурността може да определи няколко нива на оценка в зависимост от стриктността и задълбочеността на използваната методика за оценка, които следва да съответстват на едно от нивата на обезпеченост и да бъдат свързани с подходяща комбинация от компоненти на обезпечеността. За всички нива на обезпеченост ИКТ продуктът или услугата следва да съдържа редица сигурни функции, определени от схемата, които могат да включват: сигурна конфигурация в готов вид, подписан код, сигурна актуализация и овладяване на зловреден код, използващ уязвимостите на софтуера, и пълна защита на стековата/динамичната памет. Тези функции следва да бъдат разработени и поддържани, като се използват ориентирани към сигурността подходи за разработване и свързани с това инструменти, за да се гарантира надеждното включване на ефективни механизми (софтуер и хардуер). По отношение на основното ниво на обезпеченост оценката следва да се ръководи най-малко от следните компоненти: оценката следва да включва като минимум преглед на техническата документация на ИКТ продукта или услугата от орган за оценяване на съответствието. Когато сертифицирането включва ИКТ процеси, на технически преглед следва да подлежи и процесът, използван за проектиране, разработване и поддържане на ИКТ продукт или услуга. В случаите, когато дадена европейска схема за сертифициране на киберсигурността предвижда самооценка на съответствието, следва да е достатъчно производителят или доставчикът да е извършил самооценка на съответствието на ИКТ процесите, продуктите или услугите със схемата за сертифициране. По отношение на значителното ниво на обезпеченост оценката следва, в допълнение към основното ниво на обезпеченост, да се ръководи най-малко от проверката на съответствието на функциите по сигурността на ИКТ продукта или услугата с неговата техническа документация. По отношение на високото ниво на обезпеченост оценката следва, в допълнение към значителното ниво на осигуреност, да се ръководи най-малко от изпитване на ефективността, при което се оценява устойчивостта на функциите по сигурността на ИКТ продукт или услуга срещу извършители на сложни кибератаки, притежаващи съществени умения и ресурси.

(56в) При изготвяне на проект за схема ENISA следва да се консултира с всички съответни заинтересовани страни, например европейските организации за стандартизация, съответните национални органи, организациите, основани на споразумения за взаимно признаване като SOG-IS, СВП, МСП, организации на потребителите, както и заинтересовани страни, свързани с околната среда и социалната сфера.

(56г) ENISA следва да поддържа уебсайт, предоставящ информация и повишаващ осведомеността относно европейските схеми за сертифициране на киберсигурността, които следва да включват, наред с другото, исканията за изготвяне на проект за европейска схема за сертифициране на киберсигурността, както и обратната информация, получена в процеса на консултации, проведени от ENISA през етапа на изготвянето. Този уебсайт следва да предоставя и информация относно сертификатите и декларациите на ЕС за съответствие, издавани съгласно настоящия регламент.

(57) Използването на европейското сертифициране за киберсигурност **и декларацията на ЕС за съответствие** следва да остане доброволно, освен ако не е предвидено друго в законодателството на Съюза или в националното законодателство**, прието в съответствие със законодателството на Съюза**. **При липсата на хармонизирано законодателство държавите членки могат да приемат национални технически правила в съответствие с Директива (ЕС) 2015/1535, предвиждащи задължително сертифициране по европейска схема за сертифициране на киберсигурността. Държавите членки могат също да прилагат използването на европейското сертифициране за киберсигурност в контекста на обществените поръчки и Директива 2014/214/ЕС**. [...]

(57а) За да бъдат постигнати целите на настоящия регламент и да се избегне разпокъсване на вътрешния пазар, националните схеми или процедури за сертифициране на киберсигурността за ИКТ продукти и услуги, обхванати от европейска схема за сертифициране на киберсигурността, следва да престанат да пораждат правно действие от датата, определена от Комисията в акта за изпълнение. Освен това държавите членки следва да не въвеждат нови национални схеми за сертифициране на киберсигурността на ИКТ продукти и услуги, които са вече обхванати от съществуваща европейска схема за сертифициране на киберсигурността. Държавите членки не следва обаче да бъдат възпрепятствани да приемат или да запазват национални схеми за сертифициране за целите на националната сигурност.

(58) След като дадена европейски схема за сертифициране на киберсигурността бъде приета, производителите на ИКТ продукти или доставчиците на ИКТ услуги следва да могат да подават заявления за сертифициране на своите продукти или услуги до орган за оценяване на съответствието по техен избор. Органите за оценяване на съответствието следва да се акредитират от орган по акредитация, ако отговарят на конкретни изисквания, определени в настоящия регламент. Акредитацията следва да се издава за максимален срок от пет години и може да бъде подновявана при същите условия, ако органът за оценяване на съответствието отговаря на изискванията. Органите по акредитация следва да **ограничават, временно да прекратяват или да** отнемат акредитацията на органа за оценяване на съответствието, ако условията за акредитация не са били спазени или вече не се спазват, или ако органът за оценяване на съответствието е предприел действия, които нарушават разпоредбите на настоящия регламент.

(59) [...] Държавите членки **[...] следва** да определят един **или повече** [...] **органи** за сертифициране на киберсигурността, които да упражняват надзор по отношение на спазването **на задълженията, произтичащи от настоящия регламент. Ако дадена държава членка счете, че е целесъобразно, задачите могат да бъдат възлагани и на вече съществуващи органи. Освен това държавите членки следва да могат да вземат решение, при взаимно споразумение с друга държава членка, за определянето на един или повече надзорни органи на територията на тази друга държава членка. Органът следва по-специално да наблюдава и налага задълженията на производителя или доставчика на ИКТ продукти и услуги, установен на съответната му територия, във връзка с декларацията на ЕС за съответствие, да подпомага националните орани по акредитация при наблюдението и надзора на дейностите на органите за оценяване на съответствието, като им предоставя експертен опит и имаща отношение информация, да разрешава на органите за оценяване на съответствието да осъществяват задачите си, когато отговарят на допълнителни изисквания, установени в рамките на дадена схема, и да наблюдава съответните промени в областта на сертифицирането на киберсигурността**[...]. Националните органи [...] за сертифициране на **киберсигурността** следва да разглеждат жалбите, подадени от физически или юридически лица по отношение на сертификатите, издадени от тях, **или сертификатите, издадени от органите за оценяване на съответствието, отнасящи се до високо ниво на обезпеченост** [...], да разследват в необходимата степен предмета на жалбата и информират жалбоподателя за напредъка и резултатите от разследването в разумен срок. Освен това те следва да си сътрудничат с други национални [...] органи за сертифициране на **сигурността** или други публични органи, включително чрез споделяне на информация за възможни несъответствия на ИКТ продукти и услуги с изискванията на настоящия регламент или на конкретни европейски схеми за сертифициране на киберсигурността.

(60) За да се гарантира последователно прилагане на Европейската рамка за сертифициране на киберсигурността, следва да се създаде Европейска група за сертифициране на киберсигурността („групата“), състояща се от **представители на** национални [...] органи за сертифициране на **киберсигурността или други съответни национални органи**. Основните задачи на групата следва да са да съветва и подпомага Комисията при работата ѝ за гарантиране на последователното изпълнение и прилагане на Европейската рамка за сертифициране на киберсигурността; да подпомага Агенцията и да си сътрудничи тясно с нея при изготвянето на проекти на схеми за сертифициране на киберсигурността; да препоръчва на Комисията да изиска от Агенцията подготовката на конкретен проект на европейска схема за сертифициране на киберсигурността; и да приема становища, адресирани до **Агенцията във връзка с проекти за схеми и до** Комисията във връзка с поддръжката и преразглеждането на съществуващите европейски схеми за сертифициране на киберсигурността.

(60a) Групата следва да улеснява обмена на добри практики и експертен опит между националните органи за сертифициране на киберсигурността, отговарящи за оправомощаването на органите за оценяване на съответствието и издаването на сертификати. Групата следва да подпомага разработването на механизъм за партньорски проверки в контекста на изготвянето на проект за схема и прилагането му по отношение на органите, издаващи европейски сертификати за киберсигурност за високо ниво на обезпеченост. При тези партньорски проверки следва по-специално да се оценява дали съответните органи притежават подходящия експертен опит и дали изпълняват задачите си хармонизирано. Резултатите от партньорските проверки следва да бъдат обществено достъпни. Тези органи могат да приемат подходящи мерки за адаптиране на своите практики и експертен опит.

(61) С цел да се повиши осведомеността и да се улесни приемането на бъдещи схеми на ЕС за киберсигурност, Европейската комисия може да издава общи или специфични за сектора на насоки за киберсигурност, например относно добри практики в областта на киберсигурността или отговорно поведение по отношение на киберсигурността, които да подчертават положителните ефекти от използването на сертифицирани ИКТ продукти и услуги.

(61a) С цел да се улесни допълнително търговията и като се отчита, че веригите за доставки на ИКТ са глобални, споразуменията за взаимно признаване, отнасящи се до сертификати, издавани чрез схеми, които са създадени съгласно европейската рамка за сертифициране на киберсигурността, могат да бъдат сключвани от Съюза в съответствие с член 218 от ДФЕС. Комисията, като взема предвид консултациите с ENISA и Европейската група за сертифициране на киберсигурността, може да препоръча започване на съответните преговори. Всяка схема следва да предвижда специфични условия за взаимно признаване с трети страни.

(62) [...]

(63) [...]

(64) За да се гарантират еднакви условия за прилагане на настоящия регламент, на Комисията следва да се предоставят изпълнителни правомощия, когато това е предвидено в настоящия регламент. Тези правомощия следва да се упражняват в съответствие с Регламент (ЕС) № 182/2011.

(65) За приемането на актове за изпълнение относно европейските схеми за сертифициране на киберсигурността на ИКТ продукти и услуги следва да се използва процедурата по разглеждане; по отношение на условията за провеждане на [...] **разследвания** от страна на Агенцията; както и по отношение на обстоятелствата, форматите и процедурите за уведомяване на Комисията относно органи за оценяване на съответствието от националните [...] органи за сертифициране на **киберсигурността**.

(66) Дейностите на Агенцията следва да бъдат оценявани от независим орган. При оценката следва да се има предвид постигането на целите от страна на Агенцията, нейните работни практики и значимостта на задачите ѝ. В оценката следва също така да се разглеждат въздействието, ефективността и ефикасността на Европейската рамка за сертифициране на киберсигурността.

(67) Регламент (ЕС) № 526/2013 следва да бъде отменен.

(68) Тъй като целите на настоящия регламент не могат да бъдат постигнати в достатъчна степен от държавите членки и могат да бъдат постигнати по-добре 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, както е определено в споменатия член, настоящият регламент не надхвърля необходимото за постигането на тази цел,

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

ДЯЛ I
ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет и обхват

1. С оглед да се гарантира правилното функциониране на вътрешния пазар, като същевременно се постигне висока степен на киберсигурност, киберустойчивост и доверие в киберпространството в рамките на Съюза, с настоящия регламент се определят:

а) целите, задачите и организационните аспекти на ENISA — Агенцията на [...] **Европейския съюз за киберсигурност**, наричана по-долу „Агенцията“; както и

б) рамка за създаването на европейски схеми за сертифициране на киберсигурността, с цел да се гарантира подходящо ниво на киберсигурността на ИКТ **процеси,** продукти и услуги в Съюза. Тази рамка се прилага, без да се засягат специфичните разпоредби за доброволно или задължително сертифициране, предвидени в други правни актове на Съюза.

2. **Настоящият регламент не засяга компетентността на държавите членки по въпросите на киберсигурността, нито дейностите, свързани с обществената сигурност, отбраната, националната сигурност и дейностите на държавата в областта на наказателното право.**

Член 2

Определения

За целите на настоящия регламент се прилагат следните определения:

(1) „киберсигурност“ обхваща всички дейности, необходими за защита от киберзаплахи на мрежовите и информационните системи, на техните потребители и засегнати лица;

(2) „мрежова и информационна система“ означава система по смисъла на член 4, точка 1 от Директива (ЕС) 2016/1148;

(3) „национална стратегия относно сигурността на мрежовите и информационните системи“ означава рамка по смисъла на член 4, точка 3 от Директива (ЕС) 2016/1148;

(4) „оператор на основни услуги“ означава публичен или частен субект съгласно определението в член 4, точка 4 от Директива (ЕС) № 2016/1148;

(5) „доставчик на цифрови услуги“ означава юридическо лице, предоставящо цифрова услуга, съгласно определението в член 4, точка 6 от Директива (ЕС) 2016/1148;

(6) „инцидент“ означава събитие съгласно определението в член 4, точка 7 от Директива (ЕС) 2016/1148;

(7) „действия при инцидент“ означава всяка процедура съгласно определението в член 4, точка 8 от Директива (ЕС) 2016/1148;

(8) „киберзаплаха“ означава всяко потенциално обстоятелство или събитие, което може да **навреди, наруши или по друг начин** да окаже неблагоприятно въздействие върху мрежови и информационни системи, техните потребители и засегнати лица;

(9) „европейска схема за сертифициране на киберсигурността“ означава цялостен набор от правила, технически изисквания, стандарти и процедури, определени на равнището на Съюза, които се прилагат за сертифициране **или оценяване на съответствието** на **процеси,** продукти и услуги на информационните и комуникационните технологии (ИКТ), които попадат в обхвата на съответната конкретна схема;

(9а) „национална схема за сертифициране на киберсигурността“ означава цялостен набор от правила, технически изисквания, стандарти и процедури, разработени и приети от национален публичен орган, които се прилагат за сертифициране или оценяване на съответствието на ИКТ процеси, продукти и услуги, попадащи в обхвата на съответната конкретна схема;

(10) „европейски сертификат за киберсигурност“ означава документ, [...] удостоверяващ, че по отношение на даден ИКТ **процес,** продукт или услуга [...] **е извършена оценка за съответствие със** специфични изисквания за **сигурност**, определени в съответната европейска схема за сертифициране на киберсигурността;

(11) „ИКТ продукт [...]“ означава елемент или група елементи на мрежовите и информационните системи;

(11а) „ИКТ услуга“ означава всяка услуга, състояща се в изцяло или главно в предаване, съхранение, извличане или обработка на информация посредством мрежови и информационни системи;

(11б) „ИКТ процес“ означава всеки набор от дейности, извършвани с цел проектиране, разработване, предоставяне и поддържане на ИКТ продукт или услуга;

(12) „акредитация“ означава акредитация съгласно определението в член 2, точка 10 от Регламент (ЕО) № 765/2008;

(13) „национален орган по акредитация“ означава национален орган по акредитация съгласно определението в член 2, точка 11 от Регламент (ЕО) № 765/2008;

(14) „оценяване на съответствието“ означава оценяване на съответствието съгласно определението в член 2, точка 12 от Регламент (ЕО) № 765/2008;

(15) „орган за оценяване на съответствието“ означава орган за оценяване на съответствието съгласно определението в член 2, точка 13 от Регламент (ЕО) № 765/2008;

(16) „стандарт“ означава стандарт съгласно определението в член 2, точка 1 от Регламент (ЕС) № 1025/2012**;**

(16а) „техническа спецификация“ означава документ, определящ техническите изисквания, които трябва да са изпълнени от ИКТ процес, продукт или услуга;

(16б) „ниво на обезпеченост“ означава основа, която позволява да се гарантира, че даден ИКТ процес, продукт или услуга отговаря на изискванията за сигурност на конкретна европейска схема за сертифициране на киберсигурността, и посочва на кое ниво е оценен; нивото на обезпеченост не измерва сигурността на самия ИКТ процес, продукт или услуга.

ДЯЛ II

ENISA — *Агенцията на [...] Европейския съюз за киберсигурност*

ГЛАВА I

МАНДАТ И ЦЕЛИ */.../*

Член 3

Мандат

1. Агенцията поема задачите, възложени ѝ с настоящия регламент, с цел да допринесе за постигане на високо равнище на киберсигурност [...] **в целия** Съюз, **по-специално като подпомага държавите членки и институциите, агенциите и органите на Съюза чрез подобряване на киберсигурността**. **Агенцията служи като отправна точка за консултации и експертен опит по киберсигурността за институциите, агенциите и органите на Съюза.**

2. Агенцията изпълнява задачи, поверени ѝ чрез законодателни актове на Съюза, с които се определят мерки за сближаване на законовите, подзаконовите и административните разпоредби на държавите членки, свързани с киберсигурността.

2а. При изпълнение на задачите си Агенцията действа независимо и взема изцяло под внимание националния експертен опит на съответните органи на държавите членки, като същевременно избягва дублирането на дейности.

3. [...]

Член 4

Цели

1. Агенцията функционира като експертен център по въпросите на киберсигурността благодарение на своята независимост, на научното и техническо качество на консултациите, които предоставя, на предлаганата от нея помощ и информация, на прозрачността на процедурите и методите ѝ на работа, както и на добросъвестното изпълнение на възложените ѝ задачи.

2. Агенцията подпомага институциите, агенциите и органите на Съюза, както и държавите членки, при разработването и прилагането на политиките **на Съюза**, свързани с киберсигурността, **включително секторните политики в областта на киберсигурността**.

3. Агенцията подпомага изграждането на капацитет и подготвеността в целия Съюз, като съдейства на **институциите, агенциите и органите** на Съюза, **както и на** държавите членки и заинтересованите страни от публичния и частния сектор, с цел засилване на защитата на техните мрежи и информационни системи, развитие **и подобряване на киберустойчивостта и капацитета за реагиране [...] и развиване** на уменията и знанията в областта на киберсигурността [...].

4. Агенцията насърчава сътрудничеството и координацията между държавите членки на равнището на Съюза, неговите институции, агенции и органи и съответните заинтересовани страни от **публичния и частния** сектор по въпросите на киберсигурността.

5. Агенцията **допринася за повишаване** [...] на способностите в областта на киберсигурността на равнището на Съюза, за да **съдейства** на държавите членки за предотвратяването на киберзаплахи и реакцията спрямо тях, особено в случаи на трансгранични инциденти.

6. Агенцията насърчава използването на сертифициране **с оглед избягване на разпокъсаността на схемите за сертифициране в ЕС. По-специално, Агенцията допринася** [...] за създаването и поддържането на мрежа за сертифициране на киберсигурността на равнище ЕС съгласно дял III от настоящия регламент, с цел постигане на повече прозрачност на обезпечаването на киберсигурността на ИКТ продукти и услуги и за укрепване на доверието в цифровия вътрешен пазар.

7. Агенцията насърчава високо равнище на осведоменост на гражданите и на предприятията по въпросите на киберсигурността.

ГЛАВА IA
ЗАДАЧИ

Член 5

[...] Разработване и прилагане на политиката и законодателството на Съюза

Агенцията дава своя принос за разработването и прилагането на политиката и законодателството на Съюза, като:

1. подпомага и консултира, особено посредством представяне на независими становища и подготвителна работа по разработването и прегледа на политиката и законодателството на Съюза в областта на киберсигурността, както и специфични за сектора политически и законодателни инициативи, засягащи въпросите на киберсигурността;

2. подпомага държавите членки в последователното прилагане на политиката и законодателството на Съюза по отношение на киберсигурността, особено във връзка с Директива (ЕС) 2016/1148, включително посредством становища, насоки, консултации и споделяне на най-добри практики по въпроси като управление на риска, докладване на инциденти и обмен на информация, както и чрез улесняване на обмена на най-добри практики между компетентните органи в това отношение;

3. дава своя принос за работата на групата за сътрудничество съгласно член 11 от Директива (ЕС) 2016/1148 чрез предоставяне на експертен опит и помощ;

4. подпомага:

(1) разработването и прилагането на политиката на Съюза в областта на електронната самоличност и удостоверителните услуги, по-специално чрез предоставяне на консултации и технически насоки, както и улесняване на обмена на най-добри практики между компетентните органи;

(2) насърчаването на повишено равнище на сигурност на електронните съобщения, включително чрез предоставяне на експертен опит и консултации и улесняване на обмена на най-добри практики между компетентните органи;

5. подпомага редовното преразглеждане на дейностите по политиката на ЕС и представянето на годишния доклад за напредъка на прилагането на съответната нормативна уредба относно:

а) докладването на инциденти от държавите членки до единното звено за контакти на групата за сътрудничество съгласно член 10, параграф 3 от Директива (ЕС) 2016/1148;

б) докладването пред Агенцията от страна на надзорните органи на нарушения на сигурността и целостта на системите, засягащи доставчиците на удостоверителни услуги, както е предвидено в член 19, параграф 3 от Регламент (ЕС) № 910/2014;

в) докладването на [...] **инциденти**, свързани със сигурността, осъществено от предприятията, осигуряващи обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги и предоставяно на Агенцията от компетентните органи съгласно член 40 от [Директива за създаване на Европейския кодекс за електронните съобщения].

Член 6

[...] ***Изграждане на капацитет***

1. Агенцията съдейства:

а) на държавите членки в усилията им да подобрят предотвратяването, откриването, анализа и способността за реагиране на [...] **заплахи** [...] и инциденти на киберсигурността, като им предоставя необходимите знания и експертен опит;

б) на институциите, [...] агенциите **и органите** на Съюза в усилията им да подобрят предотвратяването, установяването, анализа и способността за реагиране на [...] **заплахи** [...] и инциденти на киберсигурността, **по-специално** чрез целесъобразна подкрепа за CERT на институциите, агенциите и органите на Съюза (CERT-EU);

в) на държавите членки, по тяхна молба, за създаване на екипи за реагиране при инциденти с компютърната сигурност (CSIRT) съгласно член 9, параграф 5 от Директива (ЕС) 2016/1148;

г) на държавите членки, по тяхна молба, за разработване на национални стратегии за мрежовите и информационните системи съгласно член 7, параграф 2 от Директива (ЕС) 2016/1148; Агенцията също така насърчава разпространението и [...] **следи** изпълнението на тези стратегии в целия Съюз, за да популяризира най-добрите практики;

д) на институциите на Съюза при изготвянето и прегледа на стратегиите на Съюза за киберсигурността, като насърчава тяхното разпространение и проследява напредъка в изпълнението им;

е) на националните CSIRT и CSIRT на Съюза, като увеличава техните способности, включително чрез насърчаване на диалога и обмена на информация, за да гарантира, че всеки CSIRT отговаря на общ набор от минимални способности и работи в съответствие с най-добрите практики съобразно актуалните технологични постижения;

ж) на държавите членки чрез организиране на **редовни** [...] учения в областта на киберсигурността на равнището на Съюза, посочени в член 7, параграф 6, и чрез препоръки за политиката въз основа на процеса на оценка на ученията и направените от тях изводи;

з) на съответните публични органи чрез предлагане на обучения по киберсигурност, по целесъобразност съвместно със заинтересованите страни;

и) на групата за сътрудничество **при** [...] обмена на [...] най-добри практики, по-специално относно определянето на оператори на основни услуги от държавите членки, включително по отношение на трансграничните взаимовръзки, рисковете и инцидентите, съгласно член 11, параграф 3, буква л) от Директива (ЕС) 2016/1148.

2. Агенцията **подпомага обмена на информация в секторите и между тях** [...], по-специално в секторите, изброени в приложение II към Директива (ЕС) 2016/1148, като им предоставя най-добри практики и насоки относно наличните инструменти и процедури, както и относно начините за преодоляване на нормативните проблеми във връзка с обмена на информация.

Член 7

[...] ***Оперативно сътрудничество на равнището на Съюза***

1. Агенцията подпомага оперативното сътрудничество между **държавите членки, институциите, агенциите и** [...] органите на Съюза и между заинтересованите страни.

2. Агенцията съдейства на оперативно ниво и създава синергии с институциите, [...] агенциите **и органите** на Съюза, включително CERT-EU, службите, работещи в областта на киберпрестъпността и надзорните органи за защита на неприкосновеността на личния живот и на личните данни, с оглед решаване на въпроси от общ интерес, включително посредством:

а) обмен на ноу-хау и най-добри практики;

б) предоставяне на консултации и насоки по актуални въпроси, свързани с киберсигурността;

в) определяне в консултация с Комисията на практически договорености за изпълнението на конкретни задачи.

3. Агенцията осигурява секретариата на мрежата на CSIRT съгласно член 12, параграф 2 от Директива (ЕС) 2016/1148 **и в това си качество** [...] активно улеснява споделянето на информация и сътрудничеството между своите членове.

4. Агенцията **подпомага** [...] оперативното сътрудничество в рамките на мрежата на CSIRT, като предоставя подкрепа на държавите членки **по тяхно искане** чрез:

а) консултации за подобряване на способностите им за предотвратяване, откриване и реагиране на инциденти;

б) [...] **улесняване** на **справянето** в технически аспект [...] с инциденти със значително или съществено въздействие, **включително по-специално чрез подпомагане на доброволното споделяне на технически решения между държавите членки**;

в) анализи на уязвими точки [...] и инциденти**;**

ва) осигуряване на подпомагане за последващи технически разследвания на инциденти със значително или съществено въздействие съгласно Директива (ЕС) 2016/1148.

При изпълнението на тези задачи Агенцията и CERT-EU си сътрудничат структурирано, за да се възползват от синергии **и да избегнат дублирането на дейности**[...].

5. [...]

[...]

6. Агенцията организира **редовни** [...] учения в областта на киберсигурността на равнището на Съюза и подпомага държавите членки и институциите, агенциите и органите на Съюза, като организира учения по тяхно искане. **Тези учения на равнището на Съюза могат да включват технически, оперативни или стратегически елементи**[...]. **Веднъж на всеки две години се организира широкомащабно учение, включващо всички елементи.** По целесъобразност Агенцията също така участва и помага в организирането на секторни учения в областта на киберсигурността заедно със съответните [...] **организации, които могат** да участват и **в** [...] учения на равнището на Съюза.

7. Агенцията, **в тясно сътрудничество с държавите членки**, изготвя редовен доклад за техническото състояние на киберсигурността на ЕС, който разглежда инциденти и заплахи и се основава на информация от открити източници, собствените ѝ анализи и доклади, споделяни от, между другото: CSIRT на държавите членки [...] или единните звена за контакт съгласно Директивата за МИС (**и двете на доброволна основа** [...]); Европейския център за борба с киберпрестъпността (EC3) към Европол, CERT-EU.

8. Агенцията допринася за разработването на колективна реакция на равнище ЕС и на равнище държави членки на широкомащабни трансгранични инциденти или кризи, свързани с киберсигурността, основно чрез:

   а) обобщаване на доклади от национални източници, **подавани доброволно** с цел да допринесе за общата ситуационна осведоменост;

   б) осигуряване на ефективен поток на информация и предоставяне на механизми за ескалация между мрежата на CSIRT и техническите и политическите фактори на равнището на Съюза;

в) [...] **по искане на държавите членки, улесняване** на справянето в технически аспект с инциденти или кризи, включително **по-специално** [...] **чрез подпомагане** на **доброволното** споделяне на технически решения между държавите членки;

г) подпомагане на **институциите, агенциите и органите на ЕС и, по искане, на държавите членки при** представянето пред обществеността, свързано с инциденти или кризи;

д) **подпомагане на държавите членки, по тяхно искане, при** изпитване [...] на плановете за сътрудничество в отговор на такива инциденти или кризи.

Член 8

[...] ***Пазар, сертифициране на киберсигурността и стандартизация***

Агенцията:

а) подпомага и насърчава разработването и изпълнението на политиката на Съюза за сертифициране на киберсигурността на ИКТ **процеси,** продукти и услуги, както е предвидено в дял III от настоящия регламент, като:

(1) изготвя проекти за европейски схеми за сертифициране на киберсигурността на ИКТ **процеси,** продукти и услуги в **сътрудничество с отрасъла и в** съответствие с член 44 от настоящия регламент;

(2) съдейства на Комисията с осигуряване на секретариата на Европейската група за сертифициране на киберсигурността съгласно член 53 от настоящия регламент;

(3) съставя и публикува насоки и разработва добри практики относно изискванията за киберсигурност на ИКТ продукти и услуги в сътрудничество с националните [...] органи по сертифициране на **киберсигурността** и с отрасъла;

(3а) препоръчва подходящи технически спецификации за използването на разработването на европейски схеми за сертифициране на киберсигурността, както е посочено в член 47, параграф 1, буква б), в случаите, когато не са налице стандарти;

(3б) допринася за изграждане на достатъчен капацитет, свързан с процесите на оценяване и сертифициране, чрез съставяне и публикуване на насоки, както и чрез оказване на помощ на държавите членки по тяхно искане;

б) улеснява въвеждането и използването на европейски и международни стандарти за управление на риска и за сигурността на ИКТ **процеси**, продукти и услуги [...]**;**

ба) в сътрудничество с държавите членки съставя препоръки и насоки по отношение на техническите области, свързани с изискванията за сигурност за операторите на основни услуги и доставчиците на цифрови услуги, както и по отношение на вече съществуващите стандарти, включително националните стандарти на държавите членки, съгласно член 19, параграф 2 от Директива (ЕС) 2016/1148;

в) извършва и разпространява редовни анализи на основните тенденции на пазара на киберсигурността по отношение както на търсенето, така и на предлагането, с цел да се развие пазарът за киберсигурност в Съюза.

Член 9

*[...]**Знания* и *информация***[...]

Агенцията:

а) анализира нововъзникващите технологии и предоставя тематични оценки за очакваните социални, правни, икономически и регулаторни въздействия на технологичните нововъведения върху киберсигурността;

б) извършва дългосрочни стратегически анализи на заплахите и инцидентите в областта на киберсигурността, за да установи възникващи тенденции и да спомогне за предотвратяване на [...] **инциденти**, свързани с киберсигурността;

в) в сътрудничество с експерти от органи на държавите членки предоставя консултации, насоки и най-добри практики за сигурността на мрежовите и информационните системи, по-специално за сигурността на [...] инфраструктурите, поддържащи изброените в приложение II към Директива (ЕС) 2016/1148 сектори, **и инфраструктурите, използвани от доставчиците на цифрови услуги, изброени в приложение III към същата директива**;

г) събира, организира и предоставя на разположение на обществеността чрез специален портал информация относно киберсигурността, осигурена от институциите, агенциите и органите на Съюза **и, на доброволна основа, от държавите членки и заинтересованите страни от частния и публичния сектор**;

д) [...]

е) събира и анализира обществено достъпна информация за значителни инциденти и съставя доклади с цел предоставяне на насоки на предприятията и гражданите в целия Съюз.

ж) [...].

Член 9а

Повишаване на осведомеността и образование

Агенцията:

а) повишава обществената осведоменост относно рисковете за киберсигурността и предлага насоки и добри практики за отделните потребители, насочени към гражданите и организациите;

б) в сътрудничество с държавите членки, институциите, органите и агенциите на Съюза и отрасъла организира редовни информационни кампании за повишаване на киберсигурността и на присъствието си в Съюза;

в) подпомага държавите членки в усилията им за повишаване на осведомеността относно киберсигурността и насърчава образованието в областта на киберсигурността;

г) подкрепя по-тясната координация и обмена на най-добри практики между държавите членки относно образованието и осведомеността в областта на киберсигурността чрез улесняване на създаването и поддържането на мрежа от национални образователни центрове за контакт.

Член 10

[...] ***Научни изследвания и иновации***

Във връзка с научните изследвания и иновациите, Агенцията:

а) консултира Съюза и държавите членки относно нуждата от научни изследвания в областта на киберсигурността, с което съдейства за ефективна реакция на настоящите и нововъзникващите рискове и заплахи, както и относно нови и нововъзникващи информационни и комуникационни технологии и ефективното използване на технологиите за предотвратяване на риска;

б) участва, съобразно делегирани ѝ от Комисията правомощия, като изпълнител на програми за финансиране на научните изследвания и иновациите или като бенефициер.

Член 11

[...] ***Международно сътрудничество***

Агенцията дава своя принос в усилията на Съюза за сътрудничество с трети държави и международни организации с оглед насърчаване на международното сътрудничество в областта на киберсигурността, като:

а) участва по целесъобразност като наблюдател при организирането на международни учения, анализира и докладва на управителния съвет резултатите от такива учения;

б) улеснява, [...] **в рамките на съответните рамки за международно сътрудничество**, обмена на най-добри практики [...].

в) по искане предоставя на Комисията експертен опит**;**

ва) ва) в сътрудничество с Европейската група за сертифициране на киберсигурността, създадена съгласно член 53, предоставя консултации и подкрепа на Комисията по въпроси, свързани с договори за взаимно признаване на сертификатите в областта на киберсигурността с трети държави.

ГЛАВА II
ОРГАНИЗАЦИЯ НА АГЕНЦИЯТА

Член 12

Структура

Административната и управленска структура на Агенцията се състои от:

а) управителен съвет, който изпълнява функциите, определени в член 14;

б) изпълнителен съвет, който изпълнява функциите, определени в член 18;

в) изпълнителен директор, който изпълнява задълженията, определени в член 19;[...]

г) постоянна група на заинтересованите страни, която изпълнява функциите, определени в член 20;

га) мрежа на националните служители за връзка, която изпълнява функциите, определени в член 20а.

РАЗДЕЛ 1
УПРАВИТЕЛЕН СЪВЕТ

Член 13

Състав на управителния съвет

1. Съставът на управителния съвет включва по един представител на всяка държава членка и двама представители, назначени от Комисията. Всеки от представителите има право на глас.

2. Всеки член на управителния съвет има заместник, който го представлява при отсъствие.

3. Членовете на управителния съвет и техните заместници се назначават въз основа на познанията им в областта на киберсигурността, като се вземат предвид съответните им умения в областта на управлението, администрацията и бюджетирането. Комисията и държавите членки полагат усилия за ограничаване на текучеството на своите представители в управителния съвет, за да се осигури непрекъснатост на работата му. Комисията и държавите членки се стремят към постигането на балансирано представителство между мъже и жени в управителния съвет.

4. Мандатът на членовете на управителния съвет и на техните заместници е четири години. Този мандат подлежи на подновяване.

Член 14

Функции на управителния съвет

1. Управителният съвет:

а) определя общата насока на дейността на Агенцията и гарантира, че тя работи в съответствие с правилата и принципите, заложени в настоящия регламент. Той също така гарантира съгласуваността на работата на Агенцията с дейностите, осъществявани от държавите членки, както и на нивото на Европейския съюз;

б) приема проекта на единен програмен документ, посочен в член 21, преди представянето му на Комисията за становище;

в) приема, съобразявайки се със становището на Комисията, единния програмен документ на Агенцията с мнозинство от две трети от членовете си и в съответствие с член 17;

ва) упражнява надзор върху изпълнението на многогодишните и годишните програми, включени в единния програмен документ;

г) приема с мнозинство от две трети от членовете годишния бюджет на Агенцията и упражнява други функции във връзка с бюджета на Агенцията в съответствие с глава III;

д) оценява и приема консолидирания годишен доклад за дейностите на Агенцията и изпраща доклада и неговата оценка най-късно до 1 юли на следващата година на Европейския парламент, Съвета, Комисията и Сметната палата. Годишният доклад включва отчетите и описва как Агенцията е изпълнила своите показатели за изпълнение. Годишният доклад е обществено достъпен;

е) приема финансовите правила, приложими за Агенцията, в съответствие с член 29;

ж) приема стратегия за борба с измамите, пропорционална на риска от измами, като взема предвид анализа на разходите и ползите от действията, които следва да бъдат предприети;

з) приема правила за предотвратяване и управление на конфликти на интереси по отношение на своите членове;

и) осигурява подходящи последващи действия във връзка с констатациите и препоръките, произтичащи от разследвания на Европейската служба за борба с измамите (OLAF) и на различни вътрешни или външни одитни доклади и оценки;

й) приема свой правилник за дейността;

к) в съответствие с параграф 2 упражнява по отношение на персонала на Агенцията правомощията, предоставени на органа по назначаването съгласно Правилника за длъжностните лица, както и правомощията, предоставени на органа, оправомощен да сключва трудови договори съгласно Условията за работа на другите служители на Съюза („правомощия на органа по назначаването“);

л) приема правила за прилагане на Правилника за длъжностните лица и Условията за работа на другите служители на Съюза в съответствие с процедурата, предвидена в член 110 от Правилника за длъжностните лица;

м) назначава изпълнителния директор и при необходимост удължава срока на мандата му или го отстранява от длъжност в съответствие с член 33 от настоящия регламент;

н) назначава счетоводител, който може да бъде счетоводителят на Комисията и който се ползва с пълна независимост при изпълнението на своите задължения;

о) взема всички решения относно създаването на вътрешната структура на Агенцията и при необходимост относно нейното изменение, като взема под внимание нуждите за дейността на Агенцията, както и доброто бюджетно управление;

п) разрешава сключването на работни договорености в съответствие с членове 7 и 39.

2. Управителният съвет, в съответствие с член 110 от Правилника за длъжностните лица, приема на основание член 2, параграф 1 от същия правилник и член 6 от Условията за работа на другите служители решение за делегиране на съответните правомощия на орган по назначаването на изпълнителния директор и за определяне на условията, при които делегираните правомощия могат да бъдат оттеглени. Изпълнителният директор има правото от своя страна да делегира тези правомощия на други лица.

3. Когато изключителни обстоятелства налагат това, управителният съвет може с решение временно да оттегли правомощията на орган по назначаването, делегирани на изпълнителния директор, както и правомощията, които последният е делегирал на други лица, и да ги упражнява пряко или да ги делегира на някой от членовете си или на друг служител, различен от изпълнителния директор.

Член 15

Председател на управителния съвет

Управителният съвет избира с мнозинство от две трети от членовете си свой председател и заместник-председател измежду членовете си за срок от четири години, като този срок може да бъде подновяван еднократно. Ако обаче по време на мандата им те престанат да бъдат членове на управителния съвет, мандатът изтича автоматично на същата дата. Заместник-председателят замества служебно председателя, ако последният не е в състояние да изпълнява своите задължения.

Член 16

Заседания на управителния съвет

1. Заседанията на управителния съвет се свикват от неговия председател.

2. Управителният съвет провежда най-малко две редовни заседания годишно. Той провежда и извънредни заседания по искане на председателя, на Комисията или на най-малко една трета от членовете си.

3. Изпълнителният директор взема участие в събранията на управителния съвет без право на глас.

4. По покана на председателя членове на Постоянната група на заинтересованите страни могат да участват в заседанията на управителния съвет без право на глас.

5. По време на заседанията членовете на управителния съвет и техните заместници могат да бъдат подпомагани от съветници или експерти при спазване на правилника за дейността на управителния съвет.

6. Агенцията осигурява секретариата на управителния съвет.

Член 17

Правила за гласуване в управителния съвет

1. Управителният съвет взема решенията си с мнозинство на членовете си.

2. Мнозинство от две трети от всички членове на управителния съвет се изисква за единния програмен документ, годишния бюджет, назначаването, удължаването на мандата или освобождаването от длъжност на изпълнителния директор.

3. Всеки член има един глас. При отсъствие на даден член заместникът му упражнява неговото право на глас.

4. Председателят участва в гласуването.

5. Изпълнителният директор не участва в гласуването.

6. Правилникът за дейността на управителния съвет определя по-подробно условията и реда за гласуване, по-специално условията, при които даден член може да действа от името на друг член.

РАЗДЕЛ 2
ИЗПЪЛНИТЕЛЕН СЪВЕТ

Член 18

Изпълнителен съвет

1. Управителният съвет се подпомага от изпълнителен съвет.

2. Изпълнителният съвет:

   а) подготвя решенията, които трябва да бъдат приети от управителния съвет;

   б) заедно с управителния съвет осигурява подходящи мерки за съобразяване с резултатите и препоръките от разследванията на OLAF и различните вътрешни и външни одитни доклади и оценки;

   в) без да се засягат отговорностите на изпълнителния директор, определени в член 19, подпомага и съветва изпълнителния директор при изпълнението на решенията на управителния съвет по административни и бюджетни въпроси съгласно член 19.

3. Изпълнителният съвет се състои от петима членове, назначени измежду членовете на управителния съвет, като един от тях е председателят на управителния съвет, който може също така да бъде председател на изпълнителния съвет, и един от представителите на Комисията. Изпълнителният директор взима участие в заседанията на изпълнителния съвет, но няма право на глас.

4. Мандатът на членовете на изпълнителния съвет е четири години. Този мандат подлежи на подновяване.

5. Изпълнителният съвет заседава най-малко веднъж на всеки три месеца. Председателят на изпълнителния съвет свиква допълнителни заседания по искане на членовете на съвета.

6. Управителният съвет установява правилника за дейността на изпълнителния съвет.

7. [...]

РАЗДЕЛ 3
ИЗПЪЛНИТЕЛЕН ДИРЕКТОР

Член 19

Отговорности на изпълнителния директор

1. Агенцията се ръководи от изпълнителен директор, който е независим при изпълнението на своите задължения. Изпълнителният директор отговаря пред управителния съвет.

2. Изпълнителният директор докладва на Европейския парламент относно изпълнението на своите задължения, когато бъде поканен да направи това. Съветът може да покани изпълнителния директор да докладва за изпълнението на своите задължения.

3. Изпълнителният директор отговаря за:

а) текущото управление на Агенцията;

б) изпълнението на решенията, приети от управителния съвет;

в) изготвянето на проекта на единния програмен документ и предаването му на управителния съвет за одобрение преди представянето му на Комисията;

г) изпълнението на единния програмен документ и докладването пред управителния съвет за неговото изпълнение;

д) изготвянето на консолидирания годишен доклад за дейностите на Агенцията, **включително изпълнението на годишната работна програма,** и представянето му на управителния съвет за оценка и приемане;

е) изготвянето на план за действие за съобразяване със заключенията от оценки за изминал период, и докладване за напредъка на всеки две години пред Комисията;

ж) изготвянето на план за последващи действия във връзка със заключенията от вътрешните или външните одитни доклади и оценки, както и от разследвания на Европейската служба за борба с измамите (OLAF), представянето на доклади за напредъка два пъти годишно на Комисията и редовно на управителния съвет;

з) изготвя проект за финансовите правила, приложими по отношение на Агенцията;

и) изготвянето на проекта на декларация за разчета на приходите и разходите на Агенцията и изпълнението на нейния бюджет;

й) защитата на финансовите интереси на Съюза чрез прилагането на превантивни мерки срещу измами, корупция и всякакви други незаконни дейности, посредством ефективни проверки и, при наличие на нередности, чрез събирането на недължимо платените суми, а също така, когато това е целесъобразно, чрез ефективни, съразмерни и възпиращи административни и финансови санкции;

к) изготвянето на стратегия на Агенцията за борба с измамите и представянето ѝ на управителния съвет за одобрение;

л) установяването и поддържането на контакт с бизнес общността и потребителските организации с цел осигуряване на редовен диалог със съответните заинтересовани страни;

ла) редовния обмен с институциите, агенциите и органите на Съюза във връзка с техните дейности в областта на киберсигурността, така че да се гарантира съгласуваност в разработването и прилагането на политиката на ЕС;

м) други задачи, възложени на изпълнителния директор с настоящия регламент.

4. При необходимост, в рамките на мандата на Агенцията и в съответствие с нейните цели и задачи, изпълнителният директор може да сформира *ad hoc* работни групи, съставени от експерти, включително от компетентните органи на държавите членки. Управителният съвет се информира предварително за това. Процедурите, по-специално относно състава на работните групи, назначаването на експертите от изпълнителния директор и дейността на *ad hoc* работните групи, се определят във вътрешния правилник за дейността на Агенцията.

5. **Когато е необходимо, за целите на ефективното и ефикасно изпълнение на задачите на Агенцията и въз основа на подходящ анализ на разходите и ползите,** изпълнителният директор **може** да вземе решение [...]**за установяването на един или повече местни офиси в една или повече държави членки.** Преди да вземе решение за установяването на местен офис, изпълнителният директор **иска становището на засегнатата(ите) държава(и) членка(и), включително държавата членка, в която се намира седалището на Агенцията, и** получава предварителното съгласие на Комисията **и на** управителния съвет[...]. **В случаи на несъгласие по време на процеса на консултация между изпълнителния директор и засегнатите държави членки, въпросът се представя на Съвета за обсъждане.** В решението се уточнява обхватът на дейностите, които ще се извършват в местния офис, така че да се избегнат ненужни разходи и дублиране на административни функции на Агенцията.[...] **Броят на служителите във всички местни офиси е най-малкият възможен и общо не надвишава 40 % от [...] персонала в държавата членка, в която се намира седалището на Агенцията. Броят на служителите във всеки местен офис не надхвърля 10 % от [...] броя на [...] служителите в държавата членка, в която се намира седалището на Агенцията.**

РАЗДЕЛ 4
ПОСТОЯННА ГРУПА НА ЗАИНТЕРЕСОВАНИТЕ СТРАНИ

Член 20

Постоянна група на заинтересованите страни

1. По предложение на изпълнителния директор управителният съвет учредява Постоянна група на заинтересовани страни, съставена от доказани експерти, представляващи съответните заинтересовани страни, например отрасъла на ИКТ, доставчиците на обществени електронни съобщителни мрежи или услуги, **операторите на основни услуги,** потребителски групи, академични експерти в областта на киберсигурността и представители на компетентните органи, нотифицирани съгласно [Директивата за установяване на Европейски кодекс за електронни съобщения], както и правоприлагащите органи и надзорните органи за защита на данните.

2. Процедурите за Постоянната група на заинтересованите страни, и по-специално тези относно броя, състава, назначаването на членовете от управителния съвет, предложението на изпълнителния директор и дейността на групата, се определят във вътрешния правилник за дейността на Агенцията и се публикуват.

3. Постоянната група на заинтересованите страни се председателства от изпълнителния директор или лице, определено от изпълнителния директор за всеки конкретен случай.

4. Мандатът на членовете на Постоянната група на заинтересованите страни е с продължителност две години и половина. Членовете на управителния съвет не могат да бъдат членове на Постоянната група на заинтересованите страни. Експертите на Комисията и от държавите членки имат право да присъстват на заседанията на Постоянната група на заинтересованите страни и да участват в нейната работа. Представители на други органи, които не са членове на Постоянната група на заинтересованите страни, но които изпълнителният директор счита за подходящи, могат да бъдат поканени да присъстват на заседанията на Постоянната група на заинтересованите страни и да участват в работата ѝ.

5. Постоянната група на заинтересованите страни консултира Агенцията при изпълнението на нейните дейности. По-специално тя консултира изпълнителния директор относно изготвянето на предложение за работна програма на Агенцията и гарантирането на диалог със съответните заинтересовани страни по всички въпроси, свързани с работната програма.

5а. Постоянната група на заинтересовани страни редовно информира управителния съвет за дейностите си.

РАЗДЕЛ 4А
МРЕЖА НА НАЦИОНАЛНИТЕ СЛУЖИТЕЛИ ЗА ВРЪЗКА

Член 20а

Мрежа на националните служители за връзка

1. Управителният съвет, като действа по предложение на изпълнителния директор, създава мрежа на националните служители за връзка, съставена от представители на държавите членки.

2. Мрежата на националните служители за връзка се състои от представители на всички държави членки. Всяка държава членка определя по един представител. Заседанията на мрежата могат да се провеждат в различни експертни формати.

3. Мрежата на националните служители за връзка по-специално улеснява обмена на информация между ENISA и държавите членки. Мрежата по-специално подкрепя ENISA в разпространението на нейните дейности, констатации и препоръки в целия ЕС — за съответните заинтересовани страни.

4. Националните служители за връзка действат като единни звена за контакт на национално равнище, така че да се улесни сътрудничеството между ENISA и националните експерти в контекста на изпълнението на работната програма на ENISA.

5. Макар че националните служители за връзка следва тясно да си сътрудничат с представителите на управителния съвет на съответните си държави, мрежата не трябва да дублира работата нито на управителния съвет, нито на други форуми на ЕС.

6. Функциите и процедурите, изпълнявани от мрежата на националната служители за връзка, се определят във вътрешния правилник за дейността на Агенцията и се оповестяват публично.

РАЗДЕЛ 5
ДЕЙНОСТ

Член 21

Единен програмен документ

1. Агенцията извършва дейността си в съответствие със единен програмен документ, който съдържа многогодишната и едногодишната програма, включващи всички планирани дейности.

2. Всяка година изпълнителният директор изготвя проект на единен програмен документ, който съдържа годишно и многогодишно програмиране на съответните човешки и финансови ресурси съгласно член 32 от Делегиран регламент (ЕС) № 1271/2013[14] на Комисията, като взема предвид насоките на Комисията.

3. До 30 ноември всяка година управителният съвет приема единния програмен документ, посочен в параграф 1, и го изпраща на Европейския парламент, Съвета и Комисията не по-късно от 31 януари следващата година, както и всички следващи актуализирани варианти на този документ.

4. Единният програмен документ става окончателен след окончателното приемане на общия бюджет на Съюза и, ако е необходимо, съответно се коригира.

5. Годишната работна програма включва подробни цели и очаквани резултати, включително показатели за изпълнение. В нея също така са описани действията, които ще се финансират, и са посочени финансовите и човешките ресурси, разпределени за всяко действие, в съответствие с принципите за бюджетиране и управление по дейности. Годишната работна програма е съгласувана с многогодишната работна програма, посочена в параграф 7. В годишната работна програма се посочват ясно добавените, променените или отменените задачи в сравнение с предходната финансова година.

---

[14] Делегиран регламент (ЕС) № 1271/2013 на Комисията от 30 септември 2013 г. относно рамковия Финансов регламент за органите, посочени в член 208 от Регламент (ЕС, Евратом) № 966/2012 на Европейския парламент и на Съвета (ОВ L 328, 7.12.2013 г., стр. 42)

6. Управителният съвет внася изменения в приетата годишна работна програма, когато на Агенцията бъде възложена нова задача. Всяко съществено изменение на годишната работна програма се приема по същата процедура като първоначалната годишна работна програма. Управителният съвет може да делегира на изпълнителния директор правомощие за внасяне на несъществени изменения в годишната работна програма.

7. В многогодишната работна програма е определен общият стратегически план, включително целите, очакваните резултати и показателите за изпълнението. В нея се съдържа също програмирането на ресурсите, включително на многогодишния бюджет и персонала.

8. Програмирането на ресурсите се актуализира ежегодно. Стратегическото програмиране се актуализира по целесъобразност, и по-специално в отговор на резултата от оценката, посочена в член 56.

Член 22

Деклариране на интерес

1. Членовете на управителния съвет, изпълнителният директор и длъжностните лица, временно командировани от държавите членки, представят декларация за ангажираност и декларация за липса или наличие на преки или косвени интереси, които биха могли да се считат за накърняващи тяхната независимост. Тези декларации са точни и изчерпателни, правят се писмено всяка година и се актуализират при необходимост.

2. Членовете на управителния съвет, изпълнителният директор и външните експерти, участващи в *ad hoc* работни групи, декларират точно и изчерпателно най-късно в началото на всяко заседание наличието на интереси, които биха могли да се считат за засягащи тяхната независимост по отношение на точките в дневния ред, и се въздържат от участие в обсъждането на тези точки и гласуването по тях.

3. Агенцията установява във вътрешния правилник за дейността си практическите ред и условия за прилагане на правилата за деклариране на интереси, посочени в параграфи 1 и 2.

Член 23

Прозрачност

1. Агенцията осъществява дейността си при високо ниво на прозрачност и в съответствие с член 25.

2. Агенцията гарантира, че на обществеността и на заинтересованите страни се предоставя целесъобразна, обективна, достоверна и леснодостъпна информация, по-специално по отношение на резултатите от нейната дейност. Освен това тя оповестява публично декларациите за интереси, направени в съответствие с член 22.

3. По предложение на изпълнителния директор управителният съвет може да разреши на заинтересовани страни да наблюдават хода на някои от дейностите на Агенцията.

4. Агенцията установява във вътрешния правилник за дейността си практическите ред и условия за прилагане на правилата на прозрачност, посочени в параграфи 1 и 2.

Член 24

Поверителност

1. Без да се засяга член 25, Агенцията няма право да разкрива на трети страни информация, която обработва или получава, за която е отправено обосновано искане за поверително цялостно или частично обработване.

2. Членовете на управителния съвет, изпълнителният директор, членовете на Постоянната група на заинтересовани страни, участващите в работните *ad hoc* групи външни експерти и членовете на персонала на Агенцията, включително временно командированите от държавите членки длъжностни лица, са задължени да спазват изискванията за поверителност съгласно член 339 от Договора за функционирането на Европейския съюз (ДФЕС), дори и след приключване на службата им.

3. Агенцията установява във вътрешния правилник за дейността си практическите ред и условия за прилагане на правилата на поверителност, посочени в параграфи 1 и 2.

4. Ако това се изисква за изпълнението на задачите на Агенцията, управителният съвет решава да позволи на Агенцията да работи с класифицирана информация. В такъв случай управителният съвет, със съгласието на службите на Комисията, приема вътрешен правилник за дейността, като прилага принципите на сигурността, установени в решения (ЕС, Евратом) 2015/443[15] и 2015/444[16] на Комисията. Посоченият правилник включва разпоредби за обмена, обработката и съхранението на класифицирана информация.

---

[15] Решение (ЕС, Евратом) 2015/443 на Комисията от 13 март 2015 г. относно сигурността в Комисията (ОВ L 72, 17.3.2015 г., стр. 41)

[16] Решение (ЕС, Евратом) 2015/444 на Комисията от 13 март 2015 г. относно правилата за сигурност за защита на класифицираната информация на ЕС (ОВ L 72, 17.3.2015 г., стр. 53)

Член 25

Достъп до документи

1. Регламент (ЕО) № 1049/2001 се прилага за документи, притежавани от Агенцията.

2. Управителният съвет приема реда за прилагането на Регламент (ЕО) № 1049/2001 в срок до шест месеца от създаването на Агенцията.

3. Срещу решенията, взети от Агенцията съгласно член 8 от Регламент (ЕО) № 1049/2001, може да се подава жалба до омбудсмана по реда и при условията на член 228 от ДФЕС или те може да се обжалват пред Съда на Европейския съюз по реда и при условията на член 263 от ДФЕС.

ГЛАВА III
СЪСТАВЯНЕ И УСТРОЙСТВО НА БЮДЖЕТА

Член 26

Съставяне на бюджета

1. Всяка година изпълнителният директор изготвя проект на разчета за предвидените приходи и разходи на Агенцията за следващата финансова година и го изпраща на управителния съвет заедно с проект на щатно разписание. Приходите и разходите са балансирани.

2. Въз основа на проекта на разчета за предвидените приходи и разходи, посочен в параграф 1, управителният съвет ежегодно изготвя разчет за предвидените приходи и разходи на Агенцията за следващата финансова година.

3. До 31 януари всяка година управителният съвет изпраща разчета за предвидените средства, посочен в параграф 2, който е част от проекта на единен програмен документ, на Комисията и на третите държави, с които Европейският съюз е сключил споразумения в съответствие с член 39.

4. Въз основа на този разчет Комисията включва в проекта за бюджет на Съюза прогнозните средства, които прецени за необходими за щатното разписание, и размера на вноската, която се заделя от общия бюджет, и ги представя на Европейския парламент и на Съвета в съответствие с членове 313 и 314 от ДФЕС.

5. Европейският парламент и Съветът разрешават отпускане на бюджетни кредити за вноската в Агенцията.

6. Европейският парламент и Съветът приемат щатното разписание на Агенцията.

7. Заедно с единния програмен документ управителният съвет приема бюджета на Агенцията. Той става окончателен след окончателното приемане на общия бюджет на Съюза. Когато е уместно, управителният съвет коригира бюджета и единния програмен документ на Агенцията в съответствие с общия бюджет на Съюза.

Член 27

Устройство на бюджета

1. Без да се засягат други ресурси, приходите на Агенцията включват:

   а) вноска от бюджета на Съюза;

   б) приходи, заделени за финансиране на определени разходи съгласно финансовите правила, посочени в член 29;

   в) финансиране от Съюза под формата на споразумения за делегиране или *ad hoc* безвъзмездни средства в съответствие с нейните финансови правила, посочени в член 29, и с разпоредбите на съответните инструменти за подкрепа на политиките на Съюза;

   г) вноски от трети държави, участващи в работата на Агенцията, както е предвидено в член 39;

д) всякакви доброволни парични или непарични вноски от държавите членки. Държавите членки, осигуряващи доброволни вноски, не могат да предявяват претенции за особени права или услуги в резултат от тези вноски.

2. Разходите на Агенцията се състоят от разходи за персонал, административна и техническа поддръжка, разходи за инфраструктура и оперативни разходи, както и разходи в резултат от договори, сключени с трети страни.

Член 28

Изпълнение на бюджета

1. Изпълнителният директор отговаря за изпълнението на бюджета на Агенцията.

2. Вътрешният одитен орган на Комисията се ползва със същите правомощия спрямо Агенцията като тези спрямо отделите на Комисията.

3. До 1 март на следващата финансова година (1 март на година N + 1) счетоводителят на Агенцията изпраща междинния счетоводен отчет на счетоводителя на Комисията и на Сметната палата.

4. След като получи забележките на Сметната палата по междинния счетоводен отчет, счетоводителят на Агенцията изготвя на своя отговорност нейния окончателен счетоводен отчет.

5. Изпълнителният директор изпраща окончателния счетоводен отчет на управителния съвет за становище.

6. До 31 март на година N + 1, изпълнителният директор изпраща доклада за бюджетното и финансовото управление до Европейския парламент, Съвета, Комисията и Сметната палата.

7. До 1 юли на година N + 1 счетоводителят изпраща окончателния счетоводен отчет заедно със становището на управителния съвет до Европейския парламент, Съвета, счетоводителя на Комисията и до Сметната палата.

8. В деня на предаване на окончателния си счетоводен отчет счетоводителят също така изпраща на Сметната палата представително писмо относно окончателния отчет с копие до счетоводителя на Комисията.

9. Изпълнителният директор публикува окончателния счетоводен отчет до 15 ноември на следващата година.

10. Изпълнителният директор изпраща на Сметната палата отговор на нейните констатации в срок до 30 септември на година N + 1, с копие до управителния съвет и до Комисията.

11. Изпълнителният директор представя на Европейския парламент по искане на последния цялата информация, необходима за безпрепятственото изпълнение на процедурата по освобождаване от отговорност за въпросната финансова година, както е предвидено в член 165, параграф 3 от Финансовия регламент.

12. До 15 май на година N + 2 по препоръка на Съвета Европейският парламент освобождава изпълнителния директор от отговорност по отношение на изпълнението на бюджета за година N.

Член 29

Финансови правила

Финансовите правила, приложими за Агенцията, се приемат от управителния съвет след консултация с Комисията. Те не се отклоняват от Регламент (ЕС) № 1271/2013, освен ако специфичните изисквания за функционирането на Агенцията го налагат и ако Комисията е дала предварителното си съгласие.

Член 30

Борба с измамите

1. За улесняване на борбата с измамите, корупцията и други неправомерни дейности в рамките на Регламент (ЕС, Евратом) № 883/2013[17] на Европейския парламент и на Съвета, в срок от шест месеца от деня на започване на дейността си Агенцията се присъединява към Междуинституционалното споразумение от 25 май 1999 г. относно вътрешните разследвания от Европейската служба за борба с измамите (OLAF) и приема съответните разпоредби, приложими по отношение на всички служители на Агенцията, като използва образеца в приложението към посоченото споразумение.

2. Сметната палата на Европейския съюз има правомощия за извършване на одити по документи и на място на всички бенефициери на безвъзмездни средства, изпълнители и подизпълнители, които са получили средства от Съюза чрез Агенцията.

[17] Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета от 11 септември 2013 година относно разследванията, провеждани от Европейската служба за борба с измамите (OLAF), и за отмяна на Регламент (ЕО) № 1073/1999 на Европейския парламент и на Съвета и Регламент (Евратом) № 1074/1999 на Съвета (ОВ L 248, 18.9.2013 г., стр. 1)

3. OLAF може да извършва разследвания, включително проверки и инспекции на място, в съответствие с разпоредбите и процедурите, предвидени в Регламент (ЕС, Евратом) № 883/2013 на Европейския парламент и на Съвета и Регламент (Евратом, ЕО) № 2185/96[18] на Съвета от 11 ноември 1996 г. относно контрола и проверките на място, извършвани от Комисията за защита на финансовите интереси на Европейския съюз срещу измами и други нередности, с цел да се установи дали е налице измама, корупция или друга незаконна дейност, накърняваща финансовите интереси на Съюза, във връзка с безвъзмездни средства или поръчка, финансирани от Агенцията.

4. Без да се засягат параграфи 1, 2 и 3, споразуменията за сътрудничество с трети държави и международни организации, договорите, споразуменията и решенията на Агенцията за отпускане на безвъзмездни средства съдържат разпоредби, с които Сметната палата и OLAF изрично се упълномощават да провеждат такива одити и разследвания съгласно съответните техни компетенции.

ГЛАВА IV
ПЕРСОНАЛ НА АГЕНЦИЯТА

Член 31

Общи разпоредби

Правилникът за длъжностните лица и Условията за работа на другите служители, както и правилата за прилагането им, приети чрез споразумение между институциите на Съюза, се прилагат за персонала на Агенцията.

---

18 Регламент (Евратом, ЕО) № 2185/96 на Съвета от 11 ноември 1996 г. относно контрола и проверките на място, извършвани от Комисията за защита на финансовите интереси на Европейските общности срещу измами и други нередности (ОВ L 292, 15.11.1996 г., стр. 2)

Член 32

Привилегии и имунитети

Протокол № 7 за привилегиите и имунитетите на Европейския съюз, приложен към Договора за Европейския съюз и към ДФЕС, се прилага за Агенцията и нейния персонал.

Член 33

Изпълнителен директор

1. Изпълнителният директор се назначава като срочно нает служител на Агенцията съгласно член 2, буква а) от Условията за работа на другите служители.

2. Изпълнителният директор се назначава от управителния съвет от списък с кандидати, предложен от Комисията, след открита и прозрачна процедура по подбор.

3. За целите на сключването на договора на изпълнителния директор Агенцията се представлява от председателя на управителния съвет.

4. Преди назначаването избраният от управителния съвет кандидат се поканва да направи изявление пред съответната комисия на Европейския парламент и да отговори на въпроси на членовете.

5. Мандатът на изпълнителния директор е **четири**[...] години. Към края на този период Комисията извършва оценка, която взема предвид оценката на работата на изпълнителния директор и бъдещите цели и предизвикателства пред Агенцията.

6. Управителният съвет взема решения относно назначаването, удължаването на мандата и освобождаването от длъжност на изпълнителния директор с мнозинство от две трети от своите членове с право глас.

7. По предложение на Комисията, което взема предвид оценката, посочена в параграф 5, управителният съвет може еднократно да удължи мандата на изпълнителния директор с не повече от **четири**[...] години.

8. Управителният съвет уведомява Европейския парламент за намерението си да удължи мандата на изпълнителния директор. Най-късно три месеца преди такова удължаване изпълнителният директор, ако бъде поканен, прави изявление пред съответната комисия на Европейския парламент и отговаря на въпроси на членовете.

9. Изпълнителен директор, чийто мандат е бил удължен, не може да участва в нова процедура за подбор за същата длъжност.

10. Изпълнителният директор може да бъде отстранен от длъжност единствено с решение на управителния съвет[...].

Член 34

Командировани национални експерти и друг персонал

1. Агенцията може да използва командировани национални експерти или друг персонал, който не е нает от Агенцията. Правилникът за длъжностните лица и Условията за работа на другите служители не се прилагат за такъв персонал.

2. Управителният съвет приема решение за определяне на правилата относно командироването на национални експерти в Агенцията.

ГЛАВА V
ОБЩИ РАЗПОРЕДБИ

Член 35

Юридически статут на Агенцията

1. Агенцията е орган на Съюза и притежава правосубектност.

2. Във всяка държава членка Агенцията се ползва с най-широката правоспособност, предоставяна на юридически лица съгласно националното законодателство. По-специално тя може да придобива или да се разпорежда с движимо и недвижимо имущество и да бъде страна по съдебни производства[...].

3. Агенцията се представлява от нейния изпълнителен директор.

Член 36

Отговорност на Агенцията

1. Договорната отговорност на Агенцията се урежда от правото, приложимо към съответния договор.

2. Съдът на Европейския съюз е компетентен да се произнася с решение на основание на арбитражна клауза, съдържаща се в сключен от Агенцията договор.

3. В случай на извъндоговорна отговорност, съгласно общите принципи, общи за правните системи на държавите членки, Агенцията поправя всяка вреда, причинена от нея или от нейните служители при изпълнението на техните задължения.

4. Съдът на Европейския съюз е компетентен по отношение на всякакви спорове, отнасящи се до поправянето на такива вреди.

5. По отношение на личната отговорност на служителите спрямо Агенцията се прилагат съответните условия, приложими по отношение на служителите на Агенцията.

Член 37

Езиков режим

1. Към Агенцията се прилага Регламент № 1 на Съвета[19].Държавите членки и другите органи, определени от тях, могат да се обръщат към Агенцията и да получават отговор на избран от тях официален език на институциите на Съюза.

2. Преводаческите услуги, необходими за функционирането на Агенцията, се предоставят от Центъра за преводи за органите на Европейския съюз.

Член 38

Защита на личните данни

1. Обработването на лични данни от Агенцията се осъществява при спазване на Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета[20].

2. Управителният съвет приема мерките по прилагане, посочени в член 24, параграф 8 от Регламент (ЕО) № 45/2001. Управителният съвет може да приеме допълнителни мерки, необходими за прилагането на Регламент (ЕО) № 45/2001 от Агенцията.

---

[19] Регламент № 1 за определяне на езиковия режим на Европейската икономическа общност (ОВ 17, 6.10.1958 г., стр. 401)

[20] Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета от 18 декември 2000 г. относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни (ОВ L 8, 12.1.2001 г., стр. 1)

Член 39

Сътрудничество с трети държави и международни организации

1. Доколкото е необходимо за постигането на целите, посочени в настоящия регламент, Агенцията може да си сътрудничи с компетентните органи на трети държави или с международни организации, или и двете. За тази цел след предварително одобрение от Комисията Агенцията може да установява работни договорености с органите на трети държави и с международни организации. Тези договорености не създават правни задължения за Съюза и неговите държави членки.

2. Агенцията е отворена за участие на трети държави, които са сключили споразумения със Съюза за тази цел. Съгласно съответните разпоредби на тези споразумения се постигат договорености, уточняващи по-специално естеството, степента и начина на участие на тези държави в работата на Агенцията, включително разпоредби, свързани с участието в инициативите, предприемани от Агенцията, финансовите вноски и персонала. По въпросите, свързани с персонала, при всички случаи посочените договорености са в съответствие с Правилника за длъжностните лица.

3. Управителният съвет приема стратегия за отношенията с трети държави или международни организации, отнасящи се до въпроси от компетентността на Агенцията. Комисията гарантира, че Агенцията действа в обхвата на своя мандат и съществуващата институционална рамка посредством сключване на подходяща работна договореност с изпълнителния директор.

Член 40

Правила за сигурност за защита на класифицирана информация и на чувствителна некласифицирана информация

Като се консултира с Комисията, Агенцията приема свои правила за сигурност, прилагайки принципите, залегнали в правилата за сигурност на Комисията за защита на класифицирана информация на Европейския съюз и на чувствителна некласифицирана информация, както е посочено в Решения (ЕС, Евратом) 2015/443 и 2015/444 на Комисията. Това обхваща, наред с другото, разпоредби за обмена, обработката и съхранението на такава информация.

Член 41

Споразумение за седалището и условия за дейността

1. Необходимите разпоредби за установяването на Агенцията в приемащата държава членка и за съоръженията, които трябва да бъдат предоставени от тази държава, както и конкретните правила, приложими в приемащата държава членка по отношение на изпълнителния директор, членовете на управителния съвет, персонала на Агенцията и членовете на семействата им, се определят в споразумение за седалището между Агенцията и държавата членка, в която се намира седалището, като това споразумение се сключва след одобрение от управителния съвет и не по-късно от [2 години след влизането в сила на настоящия регламент].

2. Приемащата Агенцията държава членка предоставя [...]условия за гарантиране на правилното функциониране на Агенцията, включително на достъпност на мястото, наличие на съответната учебна инфраструктура за децата на служителите, подходящ достъп до пазара на труда, социално осигуряване и медицински услуги както за децата, така и за съпрузите.

Член 42

Административен контрол

Дейността на Агенцията подлежи на надзор от омбудсмана в съответствие с член 228 от ДФЕС.

ДЯЛ III
РАМКА ЗА СЕРТИФИЦИРАНЕ НА КИБЕРСИГУРНОСТТА

Член 43

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 равнището на киберсигурността в Съюза. С нея се установява управление, което дава възможност за хармонизиран подход на равнище ЕС по отношение на европейските схеми за сертифициране на киберсигурността, с оглед създаването на единен цифров пазар за ИКТ процеси, продукти и услуги.**

2. **С Европейската рамка за сертифициране на киберсигурността се определя механизъм за установяване** [...]на европейски схеми за сертифициране на киберсигурността [...]**и за удостоверяване**, че ИКТ **процесите,** продуктите и услугите, които са били [...]**оценени** в съответствие с такава схема, 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, процеси **и** услуги [...] **през целия им жизнен цикъл**.

Член 44

Изготвяне и приемане на европейска схема за сертифициране на киберсигурността

1. По искане на Комисията **или на Европейската група за сертифициране на киберсигурността („Групата“), създадена по член 53,** ENISA изготвя проект за европейска схема за сертифициране на киберсигурността, която отговаря на изискванията на членове 45, 46 и 47 от настоящия регламент.[...]

1а. Предложение за изготвяне на проект за европейска схема за сертифициране на киберсигурността може да бъде представено на Групата от държави членки или от заинтересовани страни. Групата оценява тези предложения спрямо критериите, определени от Групата чрез насоки в съответствие с член 53, параграф 3, буква ва), и може да поиска ENISA да изготви проект за европейска схема за сертифициране на киберсигурността.

2. При изготвянето на проектите за схеми, посочени в параграф 1 от настоящия член, ENISA провежда консултации с всички съответни заинтересовани страни **посредством прозрачни процеси на консултация** и си сътрудничи тясно с Групата. Групата предоставя на ENISA съдействие и експертни консултации [...]във връзка с изготвянето на проекта за схема **и приема становище относно проекта за схема, преди да го представи на Комисията**[...]. **ENISA гарантира, че проектите за схеми са в съответствие с приложимия хармонизиран стандарт, използван за акредитиране на органа за оценяване на съответствието.**

3. ENISA **се съобразява максимално със становището на Групата преди да предаде** на Комисията [...]изготвения съгласно параграф 2 от настоящия член проект за [...]схема[...].

4. На основата на проекта за схема, предложен от ENISA, Комисията може да приема актове за изпълнение съгласно член 55, параграф 2, с които осигурява европейски схеми за сертифициране на киберсигурността за ИКТ **процеси,** продукти и услуги, отговарящи на изискванията по членове 45, 46 и 47 от настоящия регламент.

5. [...]

Член 44а

Поддръжка на европейска схема за сертифициране на киберсигурността

1. Агенцията поддържа специален уебсайт за предоставяне на информация относно и публичност на европейски схеми за сертифициране в областта на киберсигурността, сертификати и декларации на ЕС за съответствие, издадени съгласно член 47а.

2. Най-малко на всеки 5 години Агенцията, в тясно сътрудничество с Групата, прави преглед на приетите европейски схеми за сертифициране на киберсигурността, като взема под внимание обратната информация, получена от заинтересованите страни. Ако счете за необходимо, Комисията или Групата може да поиска Агенцията да започне процес за разработване на проект за преразгледана схема в съответствие с член 44, параграфи 2 и 3.

Член 45

Цели за сигурност на европейските схеми за сертифициране на киберсигурността

Европейските схеми за сертифициране на киберсигурността се проектират така, че да [...]**постигнат**, според нуждите, **най-малко** следните цели за сигурност:

а) защита на данните, които се съхраняват, предават или обработват по друг начин срещу случайно или неразрешено съхраняване, обработка, достъп или разкриване **по време на целия процес или целия жизнен цикъл на продукта или услугата**;

б)

защита на данните, които се съхраняват, предават или обработват по друг начин срещу случайно или неразрешено унищожаване, [...]загуба или промяна **по време на целия процес или целия жизнен цикъл на продукта или услугата**;

в) [...]достъп до данните, услугите или функциите имат единствено оправомощени лица, програми или машини, за които се отнася правото им на достъп;

г) **регистрира се до кои данни, функции или услуги е [...]имало достъп или са били обработвани по друг начин,** кога и от кого;

д) [...]възможно е да се провери до кои данни, услуги или функции е имало достъп, [...]били са използвани **или обработвани по друг начин**, кога и от кого;

е) възстановява се своевременно наличието и достъпът до данни, услуги и функции в случай на физически или технически инцидент;

ж) [...] ИКТ **процесите**, продуктите и услугите се предоставят с актуален софтуер **и хардуер**, които нямат [...]**обществено** известни към момента уязвими точки, и са осигурени механизми за безопасни [...]актуализации**;**

жа) ИКТ процесите, продуктите и услугите се разработват, произвеждат и доставят в съответствие с изискванията за сигурност, посочени в конкретната схема.

Член 46

Нива на обезпеченост на европейските схеми за сертифициране на киберсигурността

1. Европейските схеми за сертифициране на киберсигурността могат да посочват едно или повече от следните нива на обезпечаване на сигурност: основно, значително и/или високо, за ИКТ **процеси,** продукти и услуги[...]. **Нивото на обезпеченост на сигурността следва да е съизмеримо със степента на риск, свързана с предвидената употреба на ИКТ процеса, продукта или услугата.**

2. Нивата на обезпеченост „основно“, „значително“ и „високо“ **се отнасят до сертификат или декларация на ЕС за съответствие, издадени в контекста на европейска схема за сертифициране на киберсигурността, която предвижда за всяко ниво на обезпеченост съответните изисквания за сигурност, включително функции по сигурността и съответната степен на усилия за оценката на даден ИКТ процес, продукт или услуга. Сертификатът или декларацията на ЕС за съответствие се характеризират с препратка към съответните технически спецификации, стандарти и процедури, включително технически проверки, чиято цел е да се намали рискът от киберинциденти или да се предотвратят киберинциденти, както следва:**

а) **европейският сертификат за киберсигурност или декларацията на ЕС за съответствие, отнасящи се за „**основно**“** ниво на обезпеченост**, обезпечава, че ИКТ процесите, продуктите и услугите отговарят на съответните изисквания за сигурността, включително функции по сигурността, и са били оценени на ниво, което има за цел да се сведат до минимум известните основни рискове от киберинциденти и кибератаки. Дейностите по оценката включват поне преглед на техническата документация, а когато това не е приложимо включват заместващи дейности с равностоен ефект**[...];

б) **европейският сертификат за киберсигурност, отнасящ се за** „значително“ ниво на обезпеченост **обезпечава, че ИКТ процесите, продуктите и услугите отговарят на съответните изисквания за сигурността, включително функции по сигурността, и са били оценени на ниво, което има за цел да се сведат до минимум известните киберрискове, киберинциденти и кибератаки, извършвани от субекти с ограничени умения и ресурси. Дейностите по оценката включват поне: преглед на неприложимостта на обществено известни уязвими точки и изпитване за това, че ИКТ процесите, продуктите или услугите правилно прилагат необходимата функционалност за сигурност; или, когато не е приложимо, те включват заместващи дейности с равностоен ефект**[...];

в) **европейският сертификат за киберсигурност, отнасящ се за** „високо“ ниво на обезпеченост **обезпечава, че ИКТ процесите, продуктите и услугите отговарят на съответните изисквания за сигурността, включително функции по сигурността, и 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 оценката включват поне: преглед на неприложимостта на обществено известни уязвими точки, изпитване за това, че ИКТ процесите, продуктите или услугите правилно прилагат необходимата функционалност за сигурност, на най-високото ниво на съвременните технологии, и оценяване на устойчивостта им на атаки от опитни нападатели чрез изпитване за пробив; или, когато не е приложимо, те включват заместващи дейности с равностоен ефект**[...].

2а. Европейската схема за сертифициране на киберсигурността може да посочи няколко нива на оценка в зависимост от взискателността и задълбочеността на методиката за оценка. Всяко от нивата на оценка съответства на едно от нивата на обезпеченост на сигурността и се определя от подходяща комбинация компоненти на обезпечеността.

Член 47

Елементи на европейските схеми за сертифициране на киберсигурността

1. Европейските схеми за сертифициране на киберсигурността включват **най-малко** следните елементи:

а) предмет и обхват на **схемата** за сертифициране, включително вида или категориите ИКТ **процеси**, продукти и услуги, обхванати от него**, както и подробно описание на начина, по който схемата за сертифициране съответства на потребностите на очакваните целеви групи**;

б) [...]позоваване на [...]международни**, европейски или национални** стандарти, **които са били приложени при оценката. Когато не са налични стандарти, се прави позоваване на** [...]технически спецификации, **които отговарят на изискванията на приложение II от Регламент 1025/2012, или ако не са налични такива — на технически спецификации или други изисквания за киберсигурност, определени в схемата**;

в) когато е уместно, едно или повече нива на обезпечаване на сигурност;

ва) когато е приложимо, специални или допълнителни изисквания, приложими спрямо органите за оценяване на съответствието, така че да се гарантира тяхната техническа компетентност за оценяване на изискванията за киберсигурност;

г) конкретните критерии и методи за оценка (включително типовете оценки), използвани с цел да се докаже постигането на конкретните цели, посочени в член 45;

д) **когато е приложимо,** необходимата за сертифицирането информация, която **трябва да бъде изпратена или по друг начин предоставена от кандидата на разположение** на органите за оценяване на съответствието;

е) когато схемата предвижда маркировки или етикети — условията, при които те могат да бъдат използвани;

ж) [...]правилата за наблюдение на съответствието на сертификатите **или на декларацията на ЕС за съответствие** с изискванията, включително механизми за удостоверяване на трайното съответствие с определените изисквания за киберсигурност;

з) **когато е приложимо,** условията за предоставяне **и подновяване на сертификат, както и за** поддържане, продължаване, удължаване на срока **или** ограничаване обхвата на сертифицирането;

и) правила относно последиците от несъответствието на сертифицирани **или самооценени** ИКТ продукти и услуги с изискванията [...]**на схемата**;

й) правила за начина, по който неоткрити до момента уязвими точки на киберсигурността на ИКТ **процеси,** продукти и услуги трябва да се докладват и отстраняват;

к) **когато е приложимо,** правила за съхраняването на документация от органите за оценяване на съответствието;

л) списък на национални **или международни** схеми за сертифициране на киберсигурността, които обхващат същия тип или категории ИКТ **процеси,** продукти и услуги, изисквания за сигурност и критерии и методи за оценка;

м) съдържанието на издадения сертификат **или декларация на ЕС за съответствие;**

ма) срокът на съхранение на декларацията на ЕС за съответствие и техническата документация с цялата съответна информация, предоставена от производителя или доставчика на ИКТ продукти и услуги;

мб[...]) максимален срок на валидност на сертификатите;

мв[...]) начините за осведомяване относно издадени, изменени или отнети сертификати;

мг[...]) условия за взаимно признаване на схеми за сертифициране с трети държави;

мд[...]) когато е приложимо, правилата относно механизъм за партньорска проверка за органите, издаващи сертификати на ЕС за киберсигурност за високо ниво на обезпеченост съгласно член 48, параграф 4а.

2. Определените изисквания на схемата не противоречат на никои приложими правни изисквания, по-специално на изискванията, произтичащи от хармонизираното законодателство на ЕС.

3. Когато това е предвидено в конкретен акт на Съюза, сертифицирането **или декларацията на ЕС за съответствие** по европейска схема за сертифициране на киберсигурността може да се използва за удостоверяване на презумпцията за съответствие с изискванията на посочения акт.

4. При липса на хармонизирани правни актове на Съюза в законодателството на държавата членка може да се предвиди също така, че дадена европейска схема за сертифициране на киберсигурността може да се използва за установяване на презумпцията за съответствие с правните изисквания.

Член 47а

Самооценяване на съответствието

1. В рамките на европейска схема за сертифициране на киберсигурността може да се даде възможност за извършване на оценка на съответствието при отговорност единствено на производителя или доставчика на ИКТ продукти и услуги. Тази оценка на съответствието се прилага само за ИКТ продукти и услуги с ниско ниво на риск, съответстващо на основното ниво на обезпеченост на сигурността.

2. Производителят или доставчикът на ИКТ продукти и услуги може да издаде декларация на ЕС за съответствие, в която да се заявява, че е доказано спазването на определените в схемата изисквания. Чрез изготвянето на такава декларация производителят или доставчикът на ИКТ продукти и услуги поема отговорността за съответствието на ИКТ продукта или услугата с определените в схемата изисквания.

3. Производителят или доставчикът на ИКТ продукти и услуги съхранява декларацията на ЕС за съответствие и техническата документация с цялата съответна информация, отнасяща се до съответствието на ИКТ продуктите или услугите с дадена схема, на разположение на националния орган за сертифициране на киберсигурността, посочен в член 50, параграф 1, за срок, определен в съответната европейска схема за сертифициране на киберсигурността. Копие от декларацията на ЕС за съответствие се предоставя на националния орган за сертифициране на киберсигурността и на ENISA.

4. Издаването на декларация на ЕС за съответствие е доброволно, освен ако не е предвидено друго в правото на Съюза или в правото на държавите членки.

5. Декларацията на ЕС за съответствие, издадена съгласно настоящия член, се признава във всички държави членки.

Член 48

Сертифициране на киберсигурността

1. ИКТ **процесите,** продуктите и услугите, сертифицирани по европейска схема за сертифициране на киберсигурността, приета съгласно член 44, по презумпция се приемат за съответстващи на изискванията на такава схема.

2. Сертифицирането е доброволно, освен ако не е посочено друго в законодателството на Съюза **или в правото на държавите членки**.

3. **Когато се отнася за основно и значително ниво на обезпеченост,** европейски сертификат за киберсигурност по настоящия член се издава от органите за оценяване на съответствието, посочени в член 51, на основата на критерии, включени в европейската схема за сертифициране на киберсигурността, приета съгласно член 44.

4. Чрез дерогация от параграф 3, в надлежно обосновани случаи дадена европейска схема за **сертифициране** на киберсигурността може да предвиди, че европейски сертификат за киберсигурност в резултат от тази схема може да бъде издаден само от публичен орган. Такъв [...]орган е един от следните:

а) национален [...]орган за сертифициране **на киберсигурността**, посочен в член 50, параграф 1;

б) **публичен** орган, акредитиран като орган за оценяване на съответствието съгласно член 51, параграф 1[...];

в) [...].

4а. Когато европейска схема за сертифициране на киберсигурността по член 44 изисква високо ниво на обезпеченост, сертификатът може да бъде издаден само от национален орган за сертифициране на киберсигурността по член 50, параграф 1, или от орган за оценяване на съответствието по член 51, при следните условия:

а) след предварително одобрение от националния орган за сертифициране на киберсигурността за всеки отделен сертификат, издаден от орган за оценка на съответствието; или

б) след предварително общо делегиране на изпълнението на тази задача на орган за оценка на съответствието от националния орган за сертифициране на киберсигурността.

5. Физическото или юридическото лице, което подлага своите ИКТ **процеси,** продукти или услуги на процедурите за сертифициране предоставя на [...]**разположение на** органа за оценяване на съответствието по член 51 **или на националния орган за сертифициране на киберсигурността по член 50, когато този орган е издаващият сертификата орган,** [...]цялата необходима информация за провеждане на процедурата по сертифициране.

5а. Притежателят на сертификата уведомява органа, който е издал сертификата, за всички открити впоследствие уязвими точки или нередности във връзка със сигурността на сертифицирания ИКТ процес, продукт или услуга, които може да окажат въздействие върху изискванията, свързани със сертифицирането. Органът изпраща тази информация без излишно забавяне на националния орган за сертифициране на киберсигурността.

6. Сертификатите се издават за [...]**срока, определен от съответната схема за сертифициране,** и могат да бъдат подновени, [...]ако съответните изисквания продължават да се изпълняват.

7. Европейски сертификат за киберсигурност, издаден съгласно настоящия член, се признава във всички държави членки.

Член 49

Национални сертификати и схеми за сертифициране на киберсигурността

1. Без да се засягат разпоредбите на параграф 3, националните схеми за сертифициране на киберсигурността и свързаните с тях процедури за ИКТ **процеси,** продукти и услуги, обхванати от европейска схема за сертифициране на киберсигурността, прекратяват правното си действие от датата, посочена в акта за изпълнение, приет съгласно член 44, параграф 4. Националните схеми за сертифициране на киберсигурността и свързаните с тях процедури за ИКТ **процеси,** продукти и услуги, 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 **процеси,** продукти и услуги, обхванати от съществуваща европейска схема за сертифициране на киберсигурността.

3. Съществуващите сертификати, издадени по силата на националните схеми за сертифициране на киберсигурността **и обхванати от европейска схема за сертифициране на киберсигурността**, остават в сила до изтичането си.

Член 50

Национални [...] ***органи за сертифициране*** **на киберсигурността**

1. Всяка държава членка [...]**определя един или повече** национални [...]органи за сертифициране **на киберсигурността на своята територия или, по взаимно споразумение с друга държава членка, определя един или повече органи, установен(и) във въпросната друга държава членка, който(които) да отговаря(т) за задачите по надзора в определящата държава членка**.

2. Всяка държава членка уведомява Комисията за наименованието на **определените** [...]**органи и за възложените им задачи**.

3. **Без да се засягат разпоредбите на член 48, параграф 4, буква а) и член 48, параграф 4а,** [...]всеки национален [...]орган за сертифициране **на киберсигурността** е независим от субектите, върху които упражнява надзор, по отношение на своята организация, решения за финансиране, правна структура и процес на вземане на решения.

3а. Държавите членки гарантират, че дейностите на националния орган за сертифициране на киберсигурността, свързани с издаването на сертификати по член 48, параграф 4, буква а) и член 48, параграф 4а се осъществяват при строго разделение на ролите и отговорностите по надзорните дейности съгласно настоящия член и че двата вида дейности са независими едни от други.

4. Държавите членки гарантират, че националните [...]органи за сертифициране **на киберсигурността** разполагат с достатъчно ресурси за упражняване на правомощията си и за изпълнение на възложените им задачи по ефективен и ефикасен начин.

5. За ефективното изпълнение на регламента е целесъобразно тези органи да участват активно, реално и съобразно правилата за поверителност в Европейската група за сертифициране на киберсигурността, създадена по силата на член 53.

6. Националните [...] органи за сертифициране **на киберсигурността**:

а) [...]

аа) наблюдават и следят за изпълнението на задълженията на установени на съответните им територии производители или доставчици на ИКТ продукти и услуги, посочени в член 47а, параграфи 2 и 3 и в съответната европейска схема за сертифициране на киберсигурността;

б) [...]**без да се засягат разпоредбите на член 51, параграф 1б, съдействат на националните органи по акредитация за наблюдението и надзора на** дейностите на органите за оценка на съответствието за целите на настоящия регламент[...];

ба) извършват наблюдение и надзор върху дейностите на органите, посочени в член 48, параграф 4;

бб) разрешават на органите за оценка на съответствието, посочени в член 51, параграф 1б, и ограничават, временно прекратяват или отнемат съществуващо разрешение при неспазване на изискванията на настоящия регламент;

в) разглеждат жалбите, внесени от физически или юридически лица във връзка със сертификати, издадени от [...] **националния орган за сертифициране на киберсигурността или съгласно член 48, параграф 4а от органите за оценка на съответствието**, разследват жалбите по същество, доколкото е необходимо, и информират жалбоподателя за напредъка и резултатите от разследването в разумен срок;

г) сътрудничат си с други национални [...]органи за сертифициране **на киберсигурността** или други публични органи, включително чрез споделяне на информация за възможни несъответствия на ИКТ **процеси,** продукти и услуги с изискванията на настоящия регламент или с конкретни европейски схеми за сертифициране на киберсигурността.

д) наблюдават промените в областта на сертифицирането на киберсигурността.

7. Всеки национален [...]орган за сертифициране **на киберсигурността** разполага най-малко със следните правомощия:

а) да изисква от органите за оценяване на съответствието**,** [...] от притежателите на европейски сертификат за киберсигурност **и от издаващите декларация на ЕС за съответствие** да представят всяка информация, която му е необходима за изпълнението на неговите задачи;

б) да провежда под формата на одити разследвания на органите за оценяване на съответствието, [...]притежателите на европейски сертификат за киберсигурност **и издаващите декларация на ЕС за съответствие** за целите на проверка на съответствието с разпоредбите по дял III;

в) да взема подходящи мерки съгласно националното законодателство, за да гарантира, че органите за оценяване на съответствието, [...]притежателите на сертификат **и издаващите декларация на ЕС за съответствие** спазват настоящия регламент или дадена европейска схема за сертифициране на киберсигурността;

г) да получава достъп до всички помещения на органите за оценяване на съответствието и на притежателите на европейски сертификати за киберсигурност за целите на провеждане на разследвания съгласно процесуалното право на Съюза или на държавата членка;

д) да отнема в съответствие с националното законодателство сертификатите, **издадени от националния орган за сертифициране на киберсигурността или в съответствие с член 48, параграф 4а от органите за оценка на съответствието,** които не са в съответствие с настоящия регламент или с европейска схема за сертифициране на киберсигурността;

е) да налага санкции, както е предвидено в член 54, съгласно националното законодателство, и да изисква незабавното преустановяване на нарушенията на задълженията по настоящия регламент.

8. 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 **процеси,** продукти и услуги.

Член 51

Органи за оценяване на съответствието

1. Органите за оценяване на съответствието се акредитират от националния орган по акредитация, определен по силата на Регламент (ЕО) № 765/2008, само когато те отговарят на изискванията, определени в приложението към настоящия регламент.

1а. Когато европейски сертификат за киберсигурност се издава от национален орган за сертифициране на киберсигурността по член 48, параграф 4, буква а) и член 48, параграф 4а, сертифициращата структура на националния орган за сертифициране на киберсигурността се акредитира като орган за оценяване на съответствието съгласно параграф 1 от настоящия член.

1б. Когато е приложимо, органите за оценка на съответствието се оправомощават от националния орган за сертифициране на киберсигурността да изпълняват неговите задачи, когато те отговарят на специфични или допълнителни изисквания, предвидени в европейската схема за сертифициране по член 47, параграф 1, буква ва).

2. Акредитацията се издава за максимален срок от пет години и може да бъде подновена при същите условия, ако органът за оценяване на съответствието отговаря на изискванията, определени в настоящия член. Органите по акредитация **вземат в разумен срок всички подходящи мерки за ограничаване, временно прекратяване или** отнемане на акредитацията на органа за оценяване на съответствието по параграф 1 от настоящия член, ако условията за акредитация не са били спазени или вече не се спазват или ако действия, предприети от органа за оценяване на съответствието, нарушават настоящия регламент.

Член 52

Уведомления

1. За всяка европейска схема за сертифициране на киберсигурността, приета съгласно член 44, националните [...]органи за сертифициране **на киберсигурността** уведомяват Комисията за [...] органите за оценяване на съответствието, акредитирани **и когато е приложимо — оправомощени по член 51, параграф 1б,** да издават сертификати при определени нива на обезпечаване на сигурност, както е посочено в член 46, и без неоправдано закъснение за всяка свързана с тях промяна.

2. Една година след датата на влизане в сила на дадена европейска схема за сертифициране на киберсигурността Комисията публикува списък на съобщените ѝ органи за оценяване на съответствието в Официален вестник на Европейския съюз.

3. Ако Комисията получи уведомление след изтичане на срока, посочен в параграф 2, тя публикува в *Официален вестник на Европейския съюз* измененията на списъка, посочен в параграф 2, в рамките на два месеца от датата на получаване на уведомлението.

4. Всеки национален [...]орган за сертифициране **на киберсигурността** може да представи на Комисията искане за заличаване на съобщен от него орган за оценяване на съответствието от списъка, посочен в параграф 2 от настоящия член. Комисията публикува в *Официален вестник на Европейския съюз* съответните изменения на списъка в срок от един месец от датата на получаване на искането от националния [...]орган за сертифициране **на киберсигурността**.

5. Комисията може да определи посредством актове за изпълнение обстоятелствата, форматите и процедурите за уведомяването, посочено в параграф 1 от настоящия член. Актовете за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 55, параграф 2.

Член 53

Европейска група за сертифициране на киберсигурността

1. Създава се Европейска група за сертифициране на киберсигурността („Групата“).

2. Групата е съставена от **представители на** националните [...]органи за сертифициране **на киберсигурността или представители на други съответни национални органи**. [...]**Всеки член на групата може да представлява не повече от една друга държава членка.**

3. Групата има следните задачи:

а) да консултира и подпомага Комисията в работата ѝ с цел гарантиране на съгласувано изпълнение и прилагане на настоящия дял, по-специално по въпроси на политиката на сертифицирането на киберсигурността, както и в изготвянето на европейски схеми за сертифициране на киберсигурността;

б) да подпомага, консултира и сътрудничи на ENISA във връзка с подготовката на проекти за схеми съгласно член 44 от настоящия регламент;

ба) да приеме становище относно проекта за схема по член 44 от настоящия регламент;

в) да [...]**поиска** Агенцията да подготви даден проект за европейска схема за сертифициране на киберсигурността съгласно член 44 от настоящия регламент;

ва) да разработва и приема насоки относно критериите за оценка на предложенията за изготвяне на проект за схема, представени на [...]Групата в съответствие с член 44, параграф 1а;

г) да приема становища, адресирани до Комисията, свързани с поддръжката и преразглеждането на съществуващите европейски схеми за сертифициране на киберсигурността;

д) да проучва важните новости в областта на сертифицирането на киберсигурността и да обменя добри практики във връзка със схемите за сертифициране на киберсигурността;

е) да улеснява сътрудничеството между националните [...]органи за сертифициране **на киберсигурността** по настоящия дял чрез **изграждане на капацитет,** обмен на информация, по-специално чрез установяване на методи за ефективен обмен на информация, свързана с всички въпроси на сертифицирането на киберсигурността**;**

еа) да оказва подкрепа за прилагането на механизма за партньорска проверка в съответствие с правилата, установени в европейска схема за сертифициране на киберсигурността съгласно член 47, параграф 1, буква мг) от настоящия регламент.

4. Комисията председателства групата **в качеството на модератор** и осигурява нейния секретариат с помощта на ENISA, както е предвидено в член 8, буква а).

Член 53а

***Право да се подаде жалба до националния [...] орган за сертифициране* на киберсигурността**

1. Физическите или юридическите лица имат право да подадат жалба до националния орган за сертифициране на киберсигурността във връзка със сертификат, издаден от същия орган или съгласно член 48, параграф 4а — от органите за оценка на съответствието.

2. Националният орган за сертифициране на киберсигурността, до когото е подадена жалбата, информира жалбоподателя за напредъка в разглеждането на жалбата и резултата от нея, включително за възможността за съдебна защита съгласно член 53б.

Член 53б

Право на ефективна съдебна защита

1. Физическите или юридическите лица имат право на ефективна съдебна защита срещу правнообвързващо решение на национален орган за сертифициране на киберсигурността, което ги засяга.

2. Физическите или юридическите лица имат право на ефективна съдебна защита, ако националният орган за сертифициране на киберсигурността не разгледа жалбата.

3. Производствата срещу националния орган за сертифициране на киберсигурността се образуват пред съдилищата на държавата членка, в която е установен органът.

Член 54

Санкции

Държавите членки определят правилата относно санкциите, приложими при нарушаване на настоящия дял и на Европейските схеми за сертифициране на киберсигурността, и вземат всички необходими мерки, за да гарантират прилагането на тези санкции. Предвидените санкции трябва да са ефективни, пропорционални и възпиращи. Държавите членки съобщават на Комисията тези правила и мерки [до …/незабавно] и я уведомяват за всяко последващо изменение, което ги засяга.

ДЯЛ IV
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 55

Процедура на комитет

1. Комисията се подпомага от комитет. Този комитет е комитет по смисъла на Регламент (ЕС) № 182/2011.

2. При позоваване на настоящия параграф се прилага член 5, параграф **4, буква б)** от Регламент (ЕС) № 182/2011.

Член 56

Оценка и преглед

1. Не по-късно от пет години след датата, посочена в член 58, и на всеки пет години след това Комисията извършва оценка на въздействието и ефективността на работата на Агенцията и нейните работни практики, както и на евентуалната необходимост от изменение на мандата на Агенцията и финансовите последици от такова изменение. В оценката се взема предвид всякаква обратна информация, предоставена в Агенцията в отговор на нейните дейности. Ако Комисията сметне, че съществуването на Агенцията вече не е оправдано от гледна точка на възложените ѝ цели, мандат и задачи, тя може да предложи настоящият регламент да бъде изменен в частта му, свързана с Агенцията.

2. Оценката също така разглежда въздействието и ефективността на разпоредбите на дял III по отношение на целите за осигуряване на адекватно ниво на киберсигурност на ИКТ продукти и услуги в Съюза и се подобряване на функционирането на вътрешния пазар.

3. Комисията изпраща доклада за оценка заедно със своите заключения на Европейския парламент, Съвета и управителния съвет. Заключенията от оценката се оповестяват публично.

Член 57

Отмяна и правоприемство

1. Регламент (ЕС) № 526/2013 се отменя считано от [….].

2. Позоваванията на Регламент (ЕО) № 526/2013 и на ENISA се считат за позовавания на настоящия регламент и на Агенцията.

3. Агенцията е правоприемник на агенцията, учредена с Регламент (ЕО) № 526/2013, по отношение на цялата собственост, споразумения, правни задължения, трудови договори, финансови ангажименти и задължения. Всички съществуващи решения на управителния съвет и изпълнителния съвет остават в сила, доколкото не противоречат на разпоредбите на настоящия регламент.

4. Агенцията се учредява за неограничен срок считано от [….].

5. Изпълнителният директор, назначен съгласно член 24, параграф 4 от Регламент (ЕС) № 526/2013, е изпълнителен директор на Агенцията за останалата част от мандата си.

6. Членовете и техните заместници в управителния съвет, назначени съгласно член 6 от Регламент (ЕС) № 526/2013, са членове и техни заместници в управителния съвет на Агенцията за останалата част от мандата си.

Член 58

Влизане в сила

1. Настоящият регламент влиза в сила на двадесетия ден след деня на публикуването му в Официален вестник на Европейския съюз.

1а. Настоящият регламент се прилага от [...], с изключение на членове 50, 51, 52, 53а, 53б и 54, които се прилагат от [24 месеца след датата на публикуването му в *Официален вестник на Европейския съюз*].

2. Настоящият регламент е задължителен в своята цялост и се прилага пряко във всички държави членки.

Съставено в Брюксел на […] година.

За Европейския парламент	*За Съвета*
Председател	*Председател*

ПРИЛОЖЕНИЕ

ИЗИСКВАНИЯ, НА КОИТО ТРЯБВА ДА ОТГОВАРЯТ ОРГАНИТЕ ЗА ОЦЕНЯВАНЕ НА СЪОТВЕТСТВИЕТО

Органите за оценяване на съответствието, които желаят да бъдат акредитирани, трябва да отговарят на следните изисквания:

1. Органът за оценяване на съответствието се създава съгласно националното право и притежава юридическа правосубектност.

2. Органът за оценяване на съответствието е трета страна, независима от организацията или от ИКТ продуктите или услугите, 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 или услуги, 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 оценяваните ИКТ продукт или услуга, нито пък да са упълномощен представител на някоя от тези страни. Това не изключва използването на оценявани продукти, които са необходими за дейностите на органа за оценяване на съответствието, или използването на такива 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, предлагането на пазара, монтирането, използването или поддръжката на тези продукти, нито представляват страните, ангажирани в тези дейности. Те не участват в никаква дейност, която може да е в противоречие с тяхната независима преценка или тяхното почтено поведение по отношение на дейностите по оценяване на съответствието, за които са нотифицирани. Това се прилага по-конкретно за консултантски услуги.

6. Органите за оценяване на съответствието гарантират, че дейностите на техните поделения или подизпълнители не влияят върху поверителността, обективността или безпристрастността на техните дейности по оценяване на съответствието.

7. Органите за оценяване на съответствието и техният персонал осъществяват дейностите по оценяване на съответствието с най-висока степен на професионална почтеност и с необходимата техническа компетентност в определената област и са напълно неподвластни на всякакъв натиск или облаги, включително такива от финансов характер, които биха могли да повлияят на тяхната преценка или на резултатите от техните дейности по оценяване на съответствието, особено от страна на лица или групи лица, заинтересовани от резултатите от тези дейности.

8. Органът за оценяване на съответствието е в състояние да изпълнява всички задачи по оценяване на съответствието, които са му възложени по силата на настоящия регламент, независимо дали тези задачи се изпълняват от самия орган за оценяване на съответствието или от негово име и на негова отговорност.

9. По всяко време и за всяка процедура за оценка на съответствието, както и за всеки вид, категория или подкатегория ИКТ продукти или услуги органът за оценяване на съответствието разполага с необходимите:

а) персонал с технически знания и достатъчен и подходящ опит за изпълнение на задачите за оценяване на съответствието;

б) описания на процедурите, в съответствие с които се извършва оценяването на съответствието, чрез които се гарантира прозрачността на тези процедури и възможността за тяхното възпроизвеждане. Той разполага с подходящи политики и процедури, които позволяват разграничаване между задачите, които изпълнява като нотифициран орган, и останалите му дейности;

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 ИКТ продукта или ИКТ услугата и масовия или сериен характер на производството.

10. Органът за оценяване на съответствието разполага със средствата, необходими за изпълнението на технически и административни задачи, свързани с дейностите по оценяване на съответствието, по подходящ начин, както и с достъп до цялото необходимо оборудване и съоръжения.

11. Персоналът, отговорен за провеждането на дейностите по оценяване на съответствието, разполага със:

а) солидно техническо и професионално обучение, обхващащо цялата дейност по оценяване на съответствието;

б) задоволително познаване на изискванията за оценяването, което извършва, както и подходящи правомощия за извършването на такова оценяване;

в) подходящи знания и разбиране на приложимите изисквания и стандарти за изпитване;

г) способност да изготвя сертификати, записи и доклади, доказващи, че оценките са били извършени.

12. Безпристрастността на органите за оценяване на съответствието, тяхното висше ръководство и персонала, който извършва оценяването, е гарантирана.

13. Възнаграждението на висшето ръководство и на персонала, който извършва оценяването в даден орган за оценяване на съответствието, не зависи от броя на извършените оценявания или резултатите от тях.

14. Органите за оценяване на съответствието сключват застраховка за покриване на отговорността им, освен ако отговорността се поема от държавата съгласно националното право или държавата членка е пряко отговорна за оценяване на съответствието.

15. Персоналът на органа за оценяване на съответствието спазва служебна тайна по отношение на информацията, получена при изпълнение на неговите задачи съгласно настоящия регламент, или по силата на всяка разпоредба от вътрешното право, която го изисква, освен по отношение на компетентните органи на държавите членки, в които осъществява дейностите си.

16. Органите за оценяване на съответствието отговарят на изискванията на **съответния** стандарт**, който е хармонизиран по силата на Регламент (ЕО) № 765/2008 за акредитацията на органи за оценяване на съответствието, които извършват сертифициране на процеси, продукти или услуги**[...].

17. Органите за оценяване на съответствието гарантират, че изпитвателните лаборатории, използвани за целите на оценяването на съответствието, отговарят на изискванията на **съответния** стандарт**, който е хармонизиран по силата на Регламент (ЕО) № 765/2008 за акредитацията на лаборатории, които извършват изпитвания**[...].