Съвет на
Европейския съюз

Брюксел, 31 октомври 2022 г.
(OR. en)

14128/22

Междуинституционално досие:
2022/0085(COD)

CYBER 343
TELECOM 428
INST 396
CSC 472
CSCI 157
INF 176
FIN 1158
BUDGET 22
DATAPROTECT 294
CODEC 1617

БЕЛЕЖКА ПО ТОЧКИ I/A

От:	Генералния секретариат на Съвета
До:	Комитета на постоянните представители (II част)/Съвета
№ предх. док.:	10097/5/22 REV 5
№ док. Ком.:	7474/22 + ADD 1
Относно:	Предложение за регламент на Европейския парламент и на Съвета за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза – Общ подход

ВЪВЕДЕНИЕ

1. На 22 март 2022 г. Комисията прие предложение за регламент за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза. Предложението е една от мерките, предвидени в Стратегията на ЕС за киберсигурност за цифровото десетилетие[1], чиято цел е повишаване на колективната устойчивост на Съюза срещу киберзаплахи.

   В заключенията си от 22 март 2021 г. относно тази стратегия[2] Съветът подчерта, че киберсигурността е изключително важна за функционирането на публичната администрация и институции и на национално равнище, и на равнище ЕС, както и за нашето общество и икономика като цяло.

1 14133/20.
2 6722/21.

2. Предложението на Комисията, основано на член 298 от Договора за функционирането на Европейския съюз, има за цел да подобри равнището на киберсигурност в институциите, органите, службите и агенциите на Съюза чрез създаване на обща рамка, при надлежно зачитане на автономността на всеки субект на Съюза. По-специално целите на предложението са:

   – укрепване на мандата и финансирането на CERT-EU (автономен междуинституционален екип за незабавно реагиране при компютърни инциденти за субектите на Съюза);

   – създаване на междуинституционална структура (Междуинституционален съвет по киберсигурност – МСК), обединяваща представители на всички субекти на Съюза, за да се осигури правилното прилагане на регламента;

   – въвеждане на задължение за субектите на Съюза да споделят (некласифицирана) информация относно инциденти със CERT-EU и да съобщават за значителни заплахи, уязвимости и инциденти; и

   – насърчаване на координацията и сътрудничеството при реагиране на значителни инциденти.

3. Европейският парламент определи Хена Виркунен (ЕНП) за докладчик на Комисията по промишленост, изследвания и енергетика (ITRE), която е водещата комисия по въпроса. Проектодокладът беше публикуван на 7 октомври 2022 г.

4. Европейският надзорен орган по защита на данните прие становището си на 17 май 2022 г.[3]

[3] 9252/22.

5. В Съвета разглеждането на предложението в Хоризонталната работна група по въпроси на киберпространството (Работната група) започна на 29 март 2022 г. по време на френското председателство. Френското председателство изготви първия компромисен текст, обсъден в рамките на Работната група през юни 2022 г., и представи на Съвета доклад за напредъка[4] на 21 юни 2022 г.

6. По време на чешкото председателство Работната група посвети осем заседания[5] на обсъжданията на предложението и на няколко последователни компромисни текста.

7. На 23 май 2022 г. председателството поиска становище от Комитета по сигурността на Съвета относно аспектите на предложението, свързани с информационната сигурност, и по-специално с класифицираната информация. Комитетът по сигурността на Съвета даде становището си на 19 март 2022 г.[6] Както предлага Комитета по сигурността на Съвета, класифицираната информация на ЕС е изрично изключена от обхвата на регламента. Разпоредбите, свързани с освобождаването от задължения за споделяне и докладване във връзка с информация, получена от субекти извън Съюза, бяха съответно изменени.

8. На 28 октомври 2022 г. Работната група постигна съгласие по компромисния текст на председателството, изложен в приложението.

---

4 9719/22.

5 На 6 и 20 юли, на 13, 21 и 28 септември и на 5, 19 и 28 октомври 2022 г.

6 12603/22 + COR 1.

ОСНОВНИ ВЪПРОСИ

9. Държавите членки приветстваха предложението като навременно и допълващо бъдещата Директива относно мерки за високо общо ниво на киберсигурност в Съюза (Директивата за МИС 2) и подкрепиха общите ѝ цели. Държавите членки обаче призоваха за по-нататъшно привеждане в съответствие с Директивата за МИС 2, по-голяма реципрочност в обмена на информация между субектите на Съюза и държавите членки и изтъкнаха твърде доброволния характер на някои от предложените мерки. Държавите членки заявиха също, че предпочитат да се заличи позоваването на съвместното киберзвено, чиито мандат и състав все още не са определени.

10. Въз основа на обсъжданията в Работната група като основни политически въпроси бяха набелязани следните точки:

а) Привеждане в съответствие с бъдещата Директива за МИС 2

Както беше поискано от държавите членки, се извърши допълнително привеждане в съответствие с бъдещата Директива за МИС 2, т.е.:

– редица определения (член 3) бяха приведени в съответствие с тези в Директивата за МИС 2;

– беше добавен нов член 7а относно доброволните партньорски проверки в съответствие с Директивата за МИС 2, адаптирани към нуждите на субектите на Съюза;

– задълженията за докладване по член 20 бяха приведени в съответствие с тези в Директивата за МИС 2.

б) Състав на Междуинституционалния съвет по киберсигурност (МСК) (член 9)

След обсъждане на подходящото участие на представители на държавите членки в работата на МСК беше постигнат компромис чрез изявление на Съвета за протокола.

в) Институционална автономия

Беше намерен балансиран подход между волята на държавите членки за укрепване на механизмите за постигане на съответствие и необходимостта от зачитане на принципа на институционална автономност, по-специално по отношение на одитите и дисциплинарните мерки (член 11).

Накрая, позоваването на определен процент от бюджета за информационни технологии, заделен за киберсигурност, беше заличено от съображение 8.

ЗАКЛЮЧЕНИЕ

11. Комитетът на постоянните представители се приканва:

а) да одобри поместения в приложението компромисен текст, който след това ще формира мандата за преговори с Европейския парламент;

б) да прикани Съвета да одобри поместения в приложението компромисен текст на заседанието си на 18 ноември 2022 г. и да впише в протокола изявлението на Съвета, поместено в допълнението към настоящия документ.

ПРИЛОЖЕНИЕ

2022/0085 (COD)

Предложение за

РЕГЛАМЕНТ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

за определяне на мерки за високо общо ниво на киберсигурност в институциите, органите, службите и агенциите на Съюза

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

като взеха предвид Договора за функционирането на Европейския съюз, и по-специално член 298 от него,

като взеха предвид Договора за създаване на Европейската общност за атомна енергия, и по-специално член 106а него от него,

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

в съответствие с обикновената законодателна процедура,

като имат предвид, че:

(1) В цифровата ера информационните и комуникационните технологии са крайъгълен камък на откритата, ефикасна и независима администрация на Съюза. Развиващите се технологии и повишената сложност и взаимосвързаност на цифровите системи увеличават рисковете за киберсигурността, в резултат на което администрацията на Съюза става по-уязвима за киберзаплахи и киберинциденти, което в крайна сметка поражда заплахи за непрекъснатостта на нейната дейност и за способността ѝ да гарантира сигурността на своите данни. Въпреки че в днешно време засиленото използване на услуги „в облак“, повсеместното използване на информационни технологии, високата степен на цифровизация, дистанционната работа и развиващите се технологии и свързаност представляват основни характеристики на всички дейности на образуванията, изграждащи администрацията на Съюза, все още не е налице достатъчно ниво на цифрова устойчивост.

(2) Картината на киберзаплахите, пред които са изправени [...] **субектите** на Съюза, непрекъснато се променя. Тактиката, техниките и процедурите, използвани от авторите на заплахи, непрекъснато се развиват, докато най-честите мотиви за подобни атаки почти не се променят: от кражба на ценна неразкрита информация до сдобиване с парични средства, манипулиране на общественото мнение или подкопаване на цифровата инфраструктура. Продължава да расте темпът, с който те осъществяват своите кибератаки, а същевременно кампаниите им стават все по-сложни и автоматизирани, като са насочени срещу открити за атаки области, които продължават да се разширяват, и уязвимостите бързо се използват.

(3) ИТ средите на **субектите** [...] на Съюза се характеризират с взаимозависимост и с интегрирани потоци от данни, а ползвателите им са изградили тясно сътрудничество. Тази взаимосвързаност означава, че всяко прекъсване, дори когато първоначално е ограничено само до един [...] **субект** на Съюза, може да породи каскадни ефекти в по-широк план, което потенциално да доведе до широкообхватни и дълготрайни отрицателни въздействия върху останалите субекти. Освен това ИТ средите на някои [...] **субекти на Съюза** са свързани с ИТ средите на държавите членки, в резултат на което инцидент в един субект на Съюза би могъл да породи риск за киберсигурността на ИТ средите на държавите членки и обратно. **Освен това субектите на Съюза обработват големи количества често чувствителна информация от държавите членки, поради което инцидентите биха могли да се отразят отрицателно и на държавите членки. По тази причина киберсигурността на субектите на Съюза е от голямо значение и за държавите членки. Информацията за конкретен инцидент може също да улесни откриването на подобни киберзаплахи или инциденти, засягащи държавите членки.**

(4) [...] **Субектите** на Съюза са привлекателни мишени, които са изправени пред висококвалифицирани и добре обезпечени с ресурси автори на заплахи, както и пред други заплахи. Същевременно съществуват значителни разлики в нивото и зрелостта на кибернетичната устойчивост на тези субекти и в способността им за откриване и реагиране на злонамерени действия в киберпространството. Поради това за функционирането на европейската администрация е необходимо [...] **субектите** на Съюза да постигнат високо общо ниво на киберсигурност чрез **прилагане на** [...] мерки за киберсигурност [...], обмен на информация и сътрудничество.

(5) Директивата [предложение за МИС 2] относно мерки за високо общо ниво на киберсигурност в Съюза има за цел да се подобрят допълнително устойчивостта в областта на киберсигурността и капацитетът за реагиране при инциденти на публичните и частните субекти, на националните компетентни органи и субекти, както и на Съюза като цяло. Поради това е необходимо [...] **субектите** на Съюза да последват този пример чрез осигуряването на правила, които са в съответствие с Директивата [предложение за МИС 2] и се характеризират със същото равнище на амбиция.

(6) За да се постигне високо общо ниво на киберсигурност, е необходимо всеки [...] **субект** на Съюза да създаде вътрешна рамка за управление, ръководство и контрол на рисковете за киберсигурността, която да осигури ефективно и разумно управление на всички рискове за киберсигурността [...]. **Рамката следва да определя политики за киберсигурност, включително процедури за оценка на ефективността на прилаганите мерки за киберсигурност. Рамката следва да се основава на подход, обхващащ всички опасности, който има за цел да защити мрежите и информационните системи и физическата среда на тези системи от събития като кражба, пожар, наводнение, телекомуникационни повреди или прекъсване на захранването или от неразрешен физически достъп и щети и намеса в информацията и съоръженията за обработване на информация на субекта на Съюза, които биха могли да застрашат наличността, автентичността, целостта или поверителността на данните, съхранявани, предавани, обработвани или достъпни чрез мрежи и информационни системи. Рамката следва да отразява констатациите от анализа на риска, като се вземат предвид всички съответни технически, оперативни и организационни рискове за киберсигурността на съответния субект на Съюза.**

(6а) За да управлява рисковете, установени съгласно рамката, всеки субект на Съюза следва да осигури предприемането на подходящи и пропорционални технически, оперативни и организационни мерки. Те следва да обхващат областите, включително мерките за киберсигурност, определени в настоящия регламент, с цел укрепване на киберсигурността на всеки субект на Съюза.

(6б) Активите и рисковете, установени в рамката, както и заключенията, направени вследствие на редовните оценки на зрелостта, следва да бъдат отразени в плана за киберсигурност, изготвен от всеки субект на Съюза. Планът за киберсигурност следва да включва приетите мерки за киберсигурност с цел повишаване на цялостната киберсигурност на съответния субект на Съюза.

(6в) Тъй като осигуряването на киберсигурност е непрекъснат процес, пригодността и ефективността на всички мерки следва редовно да се преразглеждат спрямо променящите се рискове, активи и зрялост на субектите на Съюза. Рамката следва да се преглежда редовно и най-малко веднъж на всеки три години, а планът за киберсигурност следва да се преразглежда най-малко веднъж на всеки две години или след всяка оценка на зрелостта или всеки преглед на рамката.

(6г) Субектите на Съюза следва редовно да обменят релевантна информация, включително по отношение на съответните инциденти и киберзаплахи, като същевременно осигуряват поверителността и подходящата защита на информацията, предоставена от докладващия субект на Съюза.

(6д) Следва да се въведе механизъм за осигуряване на ефективен обмен на информация, координация и сътрудничество между субектите на Съюза в случай на сериозни инциденти, включително ясно установяване на ролите и отговорностите на участващите субекти на Съюза. Обменяната информация следва да се взема предвид от определеното звено за контакт за EU-CyCLONe, когато се споделя релевантна информация с EU-CyCLONe като принос към споделената ситуационна осведоменост.

(7) Разликите между [...] **субектите** на Съюза изискват гъвкавост при изпълнението, тъй като няма да е възможно използването на универсално решение. Мерките за високо общо ниво на киберсигурност не следва да включват задължения, които директно възпрепятстват изпълнението на задачите на [...] **субектите** на Съюза или нарушават тяхната институционална автономност. Поради това [...] **субектите на Съюза** следва да създадат свои собствени рамки за управление, ръководство и контрол на рисковете за киберсигурността **и планове за киберсигурност** и да приемат [...] мерки [...] за киберсигурност. **При прилагането на тези мерки следва надлежно да се отчитат съществуващите полезни взаимодействия между субектите на Съюза с цел правилно управление на ресурсите и оптимизиране на разходите. Следва да се обърне надлежно внимание и на това мерките да не засягат по отрицателен начин ефикасния обмен на информация и операциите на субектите на Съюза с други субекти на Съюза и с националните компетентни органи.**

(8) С цел да се избегне налагането на непропорционална финансова и административна тежест върху [...] **субектите** на Съюза изискванията за управление на риска, свързан с киберсигурността, следва да бъдат пропорционални на риска, който съществува по отношение на съответната мрежа и информационна система, като се отчитат последните достижения в областта на тези мерки. Всеки [...] **субект** на Съюза следва да се стреми да отдели подходяща част от своя ИТ бюджет за подобряване на своето равнище на киберсигурност [...]. **В оценката на зрелостта следва също така да се прецени дали разходите на субекта на Съюза за киберсигурност са пропорционални на рисковете, пред които е изправен.**

(9) Високото общо ниво на киберсигурност изисква поставянето на киберсигурността под надзора на най-високото равнище на управление на всеки [...] **субект** на Съюза [...]**.** [...] **Най-високото равнище на управление следва да наблюдава прилагането на настоящия регламент, включително създаването на рамка за управление, ръководство и контрол на рисковете за киберсигурността и плановете за киберсигурност, включващи мерки за киберсигурност**. Предприемането на действия във връзка с културата на киберсигурност, т.е. ежедневното практикуване на киберсигурност, е неразделна част от [...] **рамката** за киберсигурност във всички [...] **субекти** на Съюза.

(10) [...] [...] Мерки**те за киберсигурност** следва да представляват част от [...] **плана** за киберсигурност и да бъдат допълнително уточнени в документи с насоки или препоръки, отправени от CERT-EU. При определянето на мерки и насоки следва надлежно да се вземат предвид **актуалната степен на технологично развитие, и когато е приложимо – съответните европейски и международни стандарти, както и** съответното законодателство и политики на ЕС, включително оценките на риска и препоръките, отправени от групата за сътрудничество за МИС, като например координираната оценка на риска на равнището на ЕС и инструментариума на ЕС за киберсигурност на 5G технологиите. Освен това би могло да се изисква сертифициране на съответните ИКТ продукти, услуги и процеси съгласно конкретни схеми на ЕС за сертифициране на киберсигурността, приети в съответствие с член 49 от Регламент (ЕС) 2019/881. **Когато е целесъобразно, CERT-EU следва да си сътрудничи с ENISA.**

(11) През май 2011 г. генералните секретари на институциите и органите на Съюза решиха да създадат експериментален екип за незабавно реагиране при компютърни инциденти за институциите, органите и агенциите на Съюза (CERT-EU), чийто контрол се осъществява от междуинституционален управителен съвет. През юли 2012 г. генералните секретари потвърдиха практическите договорености и постигнаха съгласие CERT-EU да просъществува като постоянна структура и да продължи да спомага за подобряването на общото ниво на сигурност на информационните технологии на институциите, органите и агенциите на Съюза като пример за видимо междуинституционално сътрудничество в областта на киберсигурността. CERT-EU беше създаден през септември 2012 г. като работна група на Европейската комисия с междуинституционален мандат. През декември 2017 г. институциите и органите на Съюза сключиха междуинституционална договореност относно организацията и функционирането на CERT-EU[7]. [...] **Настоящият регламент** следва [...] **да предвижда цялостен набор от правила за организацията, функционирането и дейността на CERT-EU. Разпоредбите на настоящия регламент имат предимство пред разпоредбите на сключената през декември 2017 г. междуинституционална договореност относно организацията и функционирането на CERT-EU**.

[...]

[7] ОВ C 12, 13.1.2018 г., стр. 1—11.

(13) Много кибератаки представляват част от по-широкообхватни кампании, насочени към групи от [...] **субекти** на Съюза или заинтересовани общности, които включват [...] **субекти** на Съюза. За да се даде възможност за проактивно откриване и реагиране на инциденти или предприемане на смекчаващи мерки, [...] **субектите** на Съюза следва да уведомяват CERT-EU за [...] киберзаплахи, [...] уязвимости**, ситуации, близки до инциденти,** и [...] инциденти и да споделят подходящи технически подробности, които позволяват откриване или смекчаване, както и реагиране на подобни киберзаплахи, уязвимости**, ситуации, близки до инциденти,** и инциденти в други [...] **субекти** на Съюза. Като се следва същият подход като предвидения в Директива [предложение за МИС 2], когато субектите **на Съюза** узнаят за значителен инцидент, те следва да бъдат задължени да подадат [...] **ранно предупреждение** до CERT-EU в срок от 24 часа. Този обмен на информация следва да даде възможност на CERT-EU да разпространи информацията до останалите [...] **субекти** на Съюза, както и до подходящи партньори, за да се спомогне за защитата на ИТ средите на Съюза и тези на неговите партньори срещу подобни инциденти [...].

(13а) С настоящия регламент се определя многоетапен подход по отношение на докладването на значителни инциденти с цел да се постигне подходящ баланс между бързото докладване, което подпомага ограничаването на потенциалното разпространение на значителни инциденти и позволява на субектите на Съюза да потърсят помощ, от една страна, и задълбоченото докладване, което подпомага извличането на ценни изводи от отделни инциденти и подобряването с течение на времето на кибернетичната устойчивост на отделните субекти на Съюза, от друга страна. В това отношение настоящият регламент следва да включва докладването на инциденти, които въз основа на извършена от субекта на Съюза първоначална оценка биха могли да причинят сериозни оперативни смущения във функционирането на субекта на Съюза или финансови загуби за съответния субект на Съюза или да засегнат други физически или юридически лица, като причинят значителни имуществени или неимуществени вреди. При тази първоначална оценка следва, наред с другото, да се вземат предвид засегнатите мрежи и информационни системи, и по-специално тяхното значение за функционирането на субекта на Съюза, тежестта и техническите характеристики на киберзаплахата и всички заложени уязвимости, които се използват, както и опитът на субекта на Съюза при сходни инциденти. Показатели като степента, в която е засегнато функционирането на субекта на Съюза, продължителността на инцидента или броя на засегнатите физически или юридически лица, биха могли да играят важна роля при определянето на това дали оперативното смущение е сериозно.

(13б) Тъй като инфраструктурата и мрежите на съответния субект на Съюза и държавата членка, в която се намира този субект на Съюза, са взаимосвързани, от решаващо значение е тази държава членка да бъде информирана своевременно за всеки значителен инцидент в рамките на този субект на Съюза. За тази цел засегнатият субект на Съюза следва да уведоми националния партньор на CERT-EU, определен от държавата членка в съответствие с Директива [предложение за МИС 2], в същия срок, в който следва да докладва на CERT-EU за значителен инцидент. CERT-EU следва също така да уведоми този национален партньор, когато узнае за значителен инцидент в рамките на държавата членка, освен ако вече не е докладвано от засегнатия субект на Съюза.

(14) В допълнение към възлагането на повече задачи и разширена роля на CERT-EU следва да се създаде Междуинституционален съвет по киберсигурност (МСК), който**, за да улеснява постигането на високо общо ниво на киберсигурност сред субектите на Съюза, следва да има изключителна роля за** [...] [...] мониторинг**а** на прилагането на настоящия регламент от страна на [...] **субектите** на Съюза [...] **и за** надзор**а** на изпълнението на общите приоритети и цели от страна CERT-EU и [...] предоставян**е то** на стратегически насоки на CERT-EU. **Затова** МСК следва да гарантира представителство на институциите и да включва представители на агенциите и органите чрез Мрежата от агенции на Съюза. **Организацията и функционирането на МСК следва да бъдат допълнително уредени във вътрешния му процедурен правилник, който може да включва допълнително уточняване на редовните заседания на МСК, включително на годишните срещи на политическо равнище, на които представители на най-високото равнище на управление на всеки член на МСК биха позволили на МСК да провежда стратегически дискусии и да предоставя стратегически насоки на МСК. Освен това МСК може да създаде изпълнителен комитет, който да го подпомага в работата, и да му делегира някои от своите задачи и правомощия, особено задачите, които изискват** [...] **специфичен експертен опит на неговите членове, например одобряване на каталога на услугите и на евентуалните му последващи актуализации, на условията за споразуменията за нивото на обслужване, на оценките на документи и доклади, представени от субектите на Съюза на МСК съгласно настоящия регламент, или задачите, свързани с изготвянето на решения относно мерките за съответствие, издадени от МСК, и с мониторинга на тяхното изпълнение. МСК следва да определи процедурния правилник на изпълнителния комитет, включително неговите задачи и правомощия.**

(15) CERT-EU следва да подпомага изпълнението на мерки за високо общо ниво на киберсигурност чрез представяне на предложения за документи с насоки и за препоръки на МСК или чрез отправяне на призиви за действие. Тези документи с насоки и препоръки следва да се одобряват от МСК. При необходимост CERT-EU следва да отправя призиви за действие с описани спешни мерки за сигурност, които [...] **субектите** на Съюза настоятелно се призовават да предприемат в рамките на определен срок**. МСК може да инструктира CERT-EU да отправи, оттегли или измени предложение за документ с насоки или за препоръка или призив за действие.**

(16) МСК следва да наблюдава спазването на настоящия регламент и предприемането на последващи действия във връзка с документите с насоки, препоръките и призивите за действие [...]. МСК следва да се подпомага по технически въпроси от технически консултативни групи, съставени по преценка на МСК, които следва да работят в тясно сътрудничество със CERT-EU, [...] **със субектите** на Съюза и с други заинтересовани страни, ако е необходимо. [...] **Когато МСК установи, че субекти на Съюза не прилагат или не изпълняват настоящия регламент, включително документите с насоки, препоръките или призивите за действие, отправени съгласно настоящия регламент, той може, без да се засягат вътрешните процедури на съответния субект на Съюза, да предприеме мерки за съответствие. Системата от мерки за съответствие следва да се използва с нарастваща строгост, което означава, че когато МСК приема мерки за съответствие, той следва да започне с предупреждение като най-леката мярка, и ако е необходимо, да приложи цялата поредица до най-строгата мярка – издаването на съвещателно становище, препоръчващо временно спиране на потоците от данни към съответния субект на Съюза, което би се прилагало в изключителни случаи на дългосрочно, умишлено и/или сериозно неизпълнение от страна на засегнатия субект на задължението му съгласно настоящия регламент.**

(16а) Предупреждението представлява най-леката мярка за съответствие, целяща отстраняване на установените недостатъци на субекта на Съюза и съдържаща препоръки за изменение на документите му в областта на киберсигурността в определен срок. Предупреждението следва да бъде на разположение на всички субекти на Съюза, освен ако не е ограничено по подходящ начин в съответствие с настоящия регламент.

(16б) Освен това МСК може да препоръча извършването на одит на субект на Съюза. За тази цел субектът на Съюза може да използва структурата си за вътрешен одит. МСК може също така да поиска извършването на одит от служба за одит на трета страна, включително от доставчик на услуги от частния сектор по взаимно съгласие.

(16в) Въз основа на резултатите от одит, извършен по препоръка или по искане на МСК, МСК може също да изиска от субекта на Съюза да приведе управлението, ръководството и контрола на рисковете за киберсигурността в съответствие с разпоредбите на настоящия регламент.

(16г) Тъй като държавите членки споделят със съответните субекти на Съюза информация, която може да бъде от чувствително естество, киберсигурността на адресата на тази информация е от решаващо значение за държавите членки. Поради това в изключителни случаи на дългосрочно, умишлено, повтарящо се и/или сериозно неизпълнение на задължението на субекта на Съюза, като крайна мярка, МСК може да издаде съвещателно становище до всички държави членки и субекти на Съюза, препоръчващо временно спиране на потоците от данни към субекта на Съюза, което следва да остане в сила, докато състоянието на киберсигурността на този субект не бъде коригирано. Това съвещателно становище следва да се съобщи на всички държави членки и субекти на Съюза чрез подходящи сигурни канали за комуникация.

(16д) **За да се гарантира правилното прилагане на настоящия регламент, ако счете, че продължаващо нарушение на настоящия регламент от страна на субект на Съюза е било причинено пряко от действие или бездействие на член на неговия персонал, включително на най-високото равнище на управление, МСК следва да изиска от съответния субект на Съюза да предприеме подходящи действия срещу този служител в съответствие с Правилника за длъжностните лица, както и с други равностойни правила, приложими в рамките на някои субекти на Съюза. Тези действия могат да включват например дисциплинарни производства, и когато е целесъобразно, в конкретния случай на агенциите на Съюза, искане до компетентния орган да предприеме необходимите стъпки, свързани с евентуалното отстраняване от длъжност на лицето, което може да е отговорно за продължаващото нарушение на настоящия регламент.**

(17) На CERT-EU следва да е възложена мисията да допринася за сигурността на ИТ средата на всички [...] **субекти** на Съюза. **Когато решава дали да предостави технически съвети или информация по съответни въпроси на политиката по искане на субект на Съюза, CERT-EU следва да гарантира, че това не възпрепятства изпълнението на неговите останали задачи, определени в настоящия регламент.**

(17а) CERT-EU следва да действа като еквивалент на определения координатор за [...] **субектите** на Съюза с цел координирано оповестяване на уязвимости в Европейския регистър на уязвимостите, както е посочено в член 6 от Директива [предложение за МИС 2]**, и следва да разработи политика за управление на уязвимостите, включваща насърчаването и улесняването на доброволното координирано оповестяване на уязвимости.**

[...]

(19) CERT-EU следва също така да изпълнява предвидената му роля в Директива [предложение за МИС 2] по отношение на сътрудничеството и обмена на информация с мрежата на екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС). Освен това, в съответствие с Препоръка (ЕС) 2017/1584 на Комисията[8], CERT-EU следва да си сътрудничи и да координира реакцията със съответните заинтересовани страни. За да допринесе за постигането на високо ниво на киберсигурност навсякъде в Съюза, CERT-EU следва да споделя с националните партньори информация за конкретни инциденти. CERT-EU следва също да си сътрудничи с други публични и частни партньори, включително в рамките на НАТО, след предварително одобрение от МСК.

[8] Препоръка (ЕС) 2017/1584 на Комисията от 13 септември 2017 г. относно координирана реакция на мащабни киберинциденти и кризи (ОВ L 239, 19.9.2017 г., стр. 36).

(20) При подпомагане на оперативната киберсигурност CERT-EU следва да използва наличния експертен опит на Агенцията на Европейския съюз за киберсигурност **(ENISA)** чрез структурирано сътрудничество, както е предвидено в Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[9]. Когато е целесъобразно, следва да бъдат сключени специални договорености между двете организации, за да се определи практическото изражение на това сътрудничество и да се избегне дублирането на дейности. CERT-EU следва да си сътрудничи с [...] **ENISA** във връзка с анализа на заплахите и редовно да споделя с Агенцията своя доклад относно картината на заплахите.

[...]

(22) **Дейностите и боравенето с информация на CERT-EU съгласно настоящия регламент могат да включват обработването на лични данни.** Всяко обработване на лични данни съгласно настоящия регламент следва да се извършва в съответствие със законодателството за защита на данните, включително Регламент (ЕС) 2018/1725 на Европейския парламент и на Съвета[10]. **Когато съгласно настоящия регламент лични данни се предават на получатели, установени в Съюза, различни от субекти на Съюза, това следва да се извършва в съответствие с член 9 от Регламент (ЕС) 2018/1725.**

---

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

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

(23) При боравенето с информация от страна на CERT-EU и [...] **субектите** на Съюза следва да се спазват **приложимите** правила [...] относно информационната сигурност[...]. [...]

(23a) За целите на обмена на информация се използват видими маркировки, за да се укаже, че получателите на информацията трябва да прилагат граници на споделяне въз основа по-специално на споразумения за неразкриване на информация или на неформални споразумения за неразкриване на информация, като например протокола за обмен на информация с цветен код за поверителност или други ясни указания от източника. Протоколът за обмен на информация с цветен код за поверителност следва да се разбира като средство за предоставяне на информация за всички ограничения по отношение на по-нататъшното разпространение на информацията. Използва се в почти всички екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) и в някои центрове за анализ и обмен на информация.

(24) **Настоящият регламент и новите задачи, възложени на CERT-EU, няма да окажат въздействие върху общите разходи по многогодишната финансова рамка.** Тъй като услугите и задачите на CERT-EU са в интерес на всички [...] **субекти** на Съюза, всеки [...] **субект** на Съюза с ИТ разходи следва да участва със справедлив дял в тези услуги и задачи. Тези вноски не засягат бюджетната автономност на [...] **субектите** на Съюза. **Всички субекти на Съюза и техните администрации следва да гарантират оптимизиране на ресурсите си на настоящото равнище и да се стремят към все повече ефективност, включително чрез задълбочаване на междуинституционалното сътрудничество в областта на киберсигурността. Поради това следва да се отдаде предпочитание на съвместен подход за обединяване на административните разходи пред индивидуалното харчене от страна на субектите на Съюза.**

(25) МСК, със съдействието на CERT-EU, следва да извършва преглед и оценка на прилагането на настоящия регламент и да докладва констатациите си на Комисията. Въз основа на тази информация Комисията следва да докладва на Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите. **Освен това Европейската сметна палата се приканва да оценява редовно функционирането на CERT-EU,**

ПРИЕХА НАСТОЯЩИЯ РЕГЛАМЕНТ:

Глава I
ОБЩИ РАЗПОРЕДБИ

Член 1

Предмет

1. С настоящия регламент се определят **мерки, които имат за цел постигането на високо общо ниво на киберсигурност в рамките на субектите на Съюза** [...]**.**

2. За тази цел с настоящия регламент се определят:

в) задължения за **всеки субект**[...] на Съюза да създаде [...] рамка за управление, ръководство и контрол на рисковете за киберсигурността;

г) задължения за [...] **субектите** на Съюза за управление**,** [...] докладване **и обмен на информация за** [...] рисковете за киберсигурността;

д) правила за организацията**,** [...] функционирането **и дейността** на **автономния междуинституционален екип за незабавно реагиране при компютърни инциденти за субектите** [...] на Съюза (CERT-EU) и за организацията**,** [...] функционирането **и дейността** на Междуинституционалния съвет по киберсигурност **(МСК);**

е) правила, свързани с мониторинга на прилагането на настоящия регламент.

Член 2

Обхват

1. Настоящият регламент се прилага за [...] всички [...] **субекти** на Съюза [...] и за [...] CERT-EU и **МСК** [...].

2. Настоящият регламент се прилага, без да се засяга институционалната автономност съгласно Договорите.

3. С изключение на член 12, параграф 7, настоящият регламент не се прилага за мрежи и информационни системи, боравещи с класифицирана информация на ЕС (КИЕС).

Член 3

Определения

За целите на настоящия регламент се прилагат следните определения:

1) „[...] **субекти** на Съюза“ означава институциите, органите**, службите** и агенциите на Съюза, създадени съгласно или въз основа на Договора за Европейския съюз, Договора за функционирането на Европейския съюз или Договора за създаване на Европейската общност за атомна енергия;

2) „мрежа и информационна система“ означава мрежа и информационна система**, както са определени в** [...] член 4, точка 1 от Директива [предложение за МИС 2];

3) „сигурност на мрежите и информационните системи“ означава сигурност на мрежите и информационните системи**, както е определено в** [...] член 4, точка 2 от Директива [предложение за МИС 2];

4) „киберсигурност“ означава киберсигурност**, както е определена в член 2, точка 1 от Регламент (ЕС) 2019/881** [...];

5) „най-високо равнище на управление“ означава ръководител, ръководство или координационен и надзорен орган на най-високото административно равнище **с правомощия за вземане на решения**, като се вземат предвид структурите за управление на високо равнище във всеки [...] **субект** на Съюза;

5а) „ситуация, близка до инцидент“ означава ситуация, близка до инцидент, както е определена в член 4, точка 4а от Директива [предложение за МИС 2];

6) „инцидент“ означава инцидент**, както е определен в** [...] член 4, точка 5 от Директива [предложение за МИС 2];

[...]

8) „**сериозен инцидент** [...]“ означава всеки инцидент**, който причинява ниво на смущение, което надхвърля способността на даден субект на Съюза и на CERT-EU да реагират, или който има значително въздействие върху поне два субекта на Съюза;** [...]

9) „действия при инцидент“ означава действията при инцидент**, както е определен в** [...] член 4, точка 6 от Директива [предложение за МИС 2];

10) „киберзаплаха“ означава киберзаплаха**, както е определена в** [...] член 2, точка 8 от Регламент (ЕС) 2019/881;

[...]

12) „уязвимост“ означава уязвимост по смисъла на член 4, точка 8 от Директива [предложение за МИС 2];

[...]

14) „[...] риск“ означава **риск по смисъла на член 4, точка 7б от Директива [предложение за МИС 2]** [...];

[...]

[...]

Член 3а

Обработване на лични данни

1) Обработването на лични данни съгласно настоящия регламент от CERT-EU, МСК или субекти на Съюза се извършва в съответствие с Регламент (ЕС) 2018/1725.

2) CERT-EU, МСК и субектите на Съюза обработват и обменят лични данни, доколкото това е необходимо и единствено с цел изпълнение на съответните им задължения съгласно настоящия регламент.

Глава II
МЕРКИ ЗА ВИСОКО ОБЩО НИВО НА КИБЕРСИГУРНОСТ

Член 4

Рамка за управление, ръководство и контрол на рисковете

1. Всеки [...] **субект** на Съюза [...] създава своя собствена [...] рамка за управление, ръководство и контрол на рисковете за киберсигурността („рамката“) в подкрепа на мисията на субекта**.** [...]**Тази рамка се наблюдава** на най-високото равнище на управление в субекта, за да се гарантира ефективно и разумно управление на всички рискове за киберсигурността. Рамката се въвежда най-късно до [….] [15 месеца след влизането в сила на настоящия регламент].

2. Рамката обхваща цялата **некласифицирана** ИТ среда на съответния **субект на Съюза**[...], включително всяка ИТ среда в неговите помещения, **оперативна технологична мрежа,** активи и услуги в условията на компютърни услуги „в облак“, възложени на подизпълнители или хоствани от трети страни, мобилни устройства, корпоративни мрежи, бизнес мрежи, които не са свързани с интернет, и всякакви устройства, свързани с ИТ средата. [...] Рамката **се основава на подход, обхващащ всички опасности, и на оценка на зрелостта в съответствие с член 6, обхващаща всички съответни технически, оперативни и организационни рискове, които биха могли да окажат въздействие върху киберсигурността на съответния субект на Съюз**[...].

2а. В рамката се определят политиките за киберсигурност, включително целите и приоритетите за сигурността на мрежите и информационните системи, както и политиките и процедурите за оценка на ефективността на прилаганите мерки за управление на рисковете за киберсигурността, и се определят ролите и отговорностите на членовете на персонала.

2б. Рамката се преразглежда редовно и най-малко веднъж на всеки три години спрямо променящите се рискове, активите и зрелостта на субекта от Съюза.

3. Висшето ръководство на всеки [...] **субект** на Съюза [...] **наблюдава** [...] спазването от страна на [...] **неговата** организация на задълженията, свързани с управлението, ръководството и контрола на рисковете за киберсигурността, без това да засяга официалните отговорности на други равнища на управление относно спазването на изискванията и управлението на риска в техните съответни области на отговорност.

3а. Когато е целесъобразно и без да се засяга отговорността му за прилагането на настоящия регламент, най-високото равнище на управление на всеки субект на Съюза може да делегира на други старши служители в рамките на съответния субект конкретно задължение съгласно настоящия регламент. Независимо от евентуалното делегиране на свое конкретно задължение, най-високото равнище на управление може да бъде подведено под отговорност за неизпълнението от субектите на задълженията по настоящия регламент.

3б. Най-високото равнище на управление на всеки субект на Съюза гарантира, че субектите на Съюза одобряват плана за киберсигурност, който включва мерки за управление на рисковете за киберсигурността в съответствие с анализа си на риска, така че рамката да се прилага в съответствие с настоящия регламент.

[...]

5. Всеки [...] **субект** на Съюза назначава местен служител по киберсигурността или служител на равностойна позиция, който действа като единно звено за контакт по отношение на всички аспекти на киберсигурността.

Местният служител по киберсигурността улеснява прилагането на настоящия регламент и се отчита пряко и редовно пред най-високото равнище на управление за напредъка по прилагането.

Без да се засяга фактът, че местният служител по киберсигурността е единно звено за контакт във всеки субект на Съюза, субект на Съюза може да делегира определени задачи на местния служител по киберсигурността във връзка с прилагането на настоящия регламент на CERT-EU въз основа на споразумение за нивото на обслужване, сключено между този субект на Съюза и CERT-EU. МСК решава дали предоставянето на тази услуга да бъде част от базовите услуги на CERT-EU, като взема предвид човешките и финансовите ресурси на съответния субект на Съюза. Всеки субект на Съюза уведомява своевременно CERT-EU за назначените местни служители по киберсигурността и за всяка последваща промяна, свързана с тях. CERT-EU поддържа редовно актуализиран списък на назначените местни служители по киберсигурността.

6. Старшите служители по смисъла на член 29, параграф 2 от Правилника за длъжностните лица[11] или други служители на еквивалентно равнище във всеки субект на Съюза редовно преминават специфични обучения, за да придобият достатъчно знания и умения с цел разбиране и оценка на рисковете за киберсигурността и на управленските практики, свързани с киберсигурността, както и на тяхното въздействие върху дейността на организацията.

11 Регламент (ЕИО, Евратом, ЕОВС) № 259/68 на Съвета от 29 февруари 1968 г. относно Правилника за длъжностните лица и Условията за работа на другите служители на Европейските общности (ОВ L 56, 4.3.1968 г., стр. 1).

7. Всеки субект на Съюза разполага с ефективни механизми, за да гарантира, че подходящ процент от ИТ бюджета се изразходва за киберсигурност. При определянето на този процент надлежно се взема предвид рамката.

Член 5

[...]***Мерки за управление на рисковете за киберсигурността***

1. **Под надзора на** най-високото равнище на управление [...] [...] **всеки субект на Съюза осигурява предприемането на подходящи и пропорционални технически, оперативни и организационни мерки за управление на установените съгласно рамката, посочена в член 4, параграф 1, рискове и за предотвратяване и/или свеждане до минимум на въздействието на инцидентите. Като се вземат предвид актуалната степен на технологично развитие, и когато е приложимо, съответните европейски и международни стандарти, както и разходите за прилагане, тези мерки гарантират ниво на сигурност на мрежите и информационните системи, което съответства на рисковете за тях. При оценката на пропорционалността на тези мерки надлежно се вземат предвид степента на изложеност на субекта на рискове, неговият размер, вероятността от настъпване на инциденти и тяхната сериозност, включително тяхното обществено и икономическо въздействие.**

[...]

3. В съответствие с документите с насоки и препоръките на МСК, при прилагането на мерките за управление на рисковете за киберсигурността в рамките на своите планове за киберсигурност субектите на Съюза обхващат най-малко следните специфични области:

а) политика за киберсигурност, що се отнася до определянето на инструментите и мерките, необходими за постигане на целите и приоритетите по член 4 и член 5, параграф 4;

б) анализ на риска и политики на сигурност в областта на информационните системи;

в) организация на киберсигурността, включително определяне на ролите и отговорностите;

г) управление на активите, включително инвентарен опис на ИТ активите и картографиране на ИТ мрежата;

д) сигурност на човешките ресурси и контрол на достъпа;

е) сигурност на операциите;

ж) сигурност на комуникациите;

з) придобиване, разработване и поддържане на системите, включително действия при уязвимости и тяхното оповестяване;

и) сигурност на веригата на доставки, включително аспектите, свързани със сигурността, на отношенията между всеки субект на Съюза и неговите преки доставчици на стоки и услуги. Субектите на Съюза вземат предвид уязвимостите, специфични за всеки пряк доставчик на стоки и услуги, и цялостното качество на продуктите и практиките в областта на киберсигурността на своите доставчици на стоки и услуги, включително техните процедури за сигурно разработване;

й) действия при инциденти и сътрудничество със CERT-EU, като например осъществяване на мониторинг на сигурността и водене на регистри;

к) управление на непрекъснатостта на дейността, като например управление на съхраняването на резервни копия на данните и възстановяване след бедствия, и управление на кризи; и

л) насърчаване и развитие на образованието, уменията, повишаването на осведомеността, упражненията и програмите за обучение в областта на киберсигурността.

4. В съответствие с документите с насоки и препоръките на МСК, при прилагането на мерките за управление на рисковете за киберсигурността в рамките на своите планове за киберсигурност субектите на Съюза обхващат най-малко следните специфични мерки за управление на рисковете за киберсигурността:

а) цели и приоритети по отношение на използването на компютърни услуги „в облак“ (по смисъла на член 4, точка 19 от Директива [предложение за МИС 2]), и технически договорености, позволяващи работа от разстояние;

б) конкретни стъпки за бъдещо използване на принципите за нулево доверие, включително на модел за сигурност, и координирана стратегия за киберсигурност и управлението на системи, основаваща се на разбирането, че заплахи съществуват както вътре, така и извън традиционните граници на мрежите;

в) приемане на многофакторната автентификация като норма в мрежите и информационните системи;

г) установяване на сигурността на веригите за доставка на софтуер чрез критерии за сигурно разработване и оценка на софтуера;

д) подобряване на правилата за възлагане на обществени поръчки, за да се улесни постигането на високо общо ниво на киберсигурност чрез:

i) премахване на договорните пречки, които ограничават доставчиците на ИТ услуги да споделят информация със CERT-EU относно инциденти, уязвимости и киберзаплахи;

ii) договорно задължение за докладване на инциденти, уязвимости и киберзаплахи, както и за въвеждане на подходящи механизми за реакция и мониторинг на инцидентите;

е) използване на криптография и криптиране, и по-специално криптиране от край до край;

ж) защитени комуникационни системи в рамките на организацията.

Член 6

Оценки на зрелостта

1. В**секи субект** [...] на Съюза извършва**, по целесъобразност и с помощта на специализирана трета страна,** оценка на зрелостта [...] най-малко веднъж на всеки три години, като включва всички елементи на своята ИТ среда, както е описано в член 4, при отчитане на съответните документи с насоки и препоръки, приети в съответствие с член 13.

2. По препоръка на CERT-EU и след консултация с Агенцията на Европейския съюз за киберсигурност (ENISA) МСК приема в срок от 4 месеца след влизането в сила на настоящия регламент методически насоки за извършване на оценки на зрелостта.

3. След приключване на оценката [...] на зрелостта субектите на Съюза я представят на МСК. Първата оценка на зрелостта се извършва най-късно [12 месеца след влизането в сила на настоящия регламент].

Член 7

Планове за киберсигурност

1. Като следва заключенията от оценката на зрелостта и като отчита активите и установените рискове съгласно член 4, най-високото равнище на управление на [...] **всеки субект** на Съюза одобрява план за киберсигурност без ненужно забавяне след създаването на [...] рамката, [...] **приемането на мерките за управление на рисковете** за киберсигурността [...] **и извършване на оценката на зрелостта — не по-късно от 21 месеца след влизането в сила на настоящия регламент**. Планът **за киберсигурност** цели повишаване на цялостната киберсигурност на съответния субект **на Съюза**, като по този начин допринася за [...] утвърждаването на високо общо ниво на киберсигурност сред всички **субекти** [...] на Съюза. [...] Планът **за киберсигурност** включва най-малко **мерките за управление на рисковете за киберсигурността по член 5** [...]. Планът **за киберсигурност** се преразглежда най-малко на всеки [...] **две** години **или** след [...] **всяка оценка** на зрелостта, извършена съгласно член 6, **или на всяко преразглеждане на рамката съгласно член 4.**

2. [...]

3. В плана за киберсигурност **се вземат под внимание** [...] всички приложими документи с насоки и препоръки**, отправени в съответствие с член 13** [...].

4. **След приключване на плана за киберсигурност субектът на Съюза го представя на МСК.**

Член 7а

Партньорска проверка

1. Като действа по препоръка на CERT-EU и след консултация с ENISA, най-късно до ... [24 месеца след влизането в сила на настоящия регламент] МСК създава — като използва методиката за партньорски проверки и методиката за самооценка в съответствие с член 16 от Директива [предложение за МИС 2], адаптирана при необходимост към нуждите на субектите на Съюза — методиката и организационните аспекти на партньорската проверка с цел извличане на поуки от споделения опит, укрепване на взаимното доверие, постигане на високо общо ниво на киберсигурност, както и повишаване на способностите и политиките на субектите на Съюза в областта на киберсигурността, необходими за прилагането на настоящия регламент. Участието в партньорските проверки е доброволно. Представители на държавите членки могат да участват в партньорската проверка като наблюдатели. Партньорските проверки се извършват от експерти в областта на киберсигурността, определени от най-малко два субекта на Съюза, различни от проверяваните субекти на Съюза, и обхващат най-малко едно от следното:

(i) степента на прилагане на мерките за управление на рисковете за киберсигурността и задълженията за докладване по членове 5 и 20;

(ii) равнището на способностите, включително наличните финансови, технически и човешки ресурси;

(iii) степента на прилагане на рамката за обмен на информация по член 19;

(iv) специфични въпроси от междусекторно естество.

2. Субектите на Съюза могат да набележат конкретни въпроси, посочени в параграф 1, подточка iv), които да бъдат преразгледани. Обхватът на прегледа, включително установените проблеми, се съобщават на участващите субекти на Съюза преди започването на партньорската проверка.

3. Преди началото на партньорската проверка субектите на Съюза могат да извършат самооценка на преразглежданите аспекти и да предоставят тази самооценка на определените експерти.

4. Партньорските проверки включват реални или виртуални посещения на място, както и дистанционен обмен. С оглед на принципа за добро сътрудничество субектите на Съюза, подлежащи на партньорска проверка, предоставят на определените експерти необходимата за оценката информация, без да се засяга националното законодателство или правото на Съюза относно защитата на чувствителна или класифицирана информация. Всяка информация, получена в процеса на партньорска проверка, се използва единствено за тази цел. Участващите в партньорската проверка експерти не оповестяват никаква чувствителна или класифицирана информация, получена в хода на тази проверка, на които и да е трети страни.

5. Аспектите, които като част от субект на Съюза са преминали партньорска проверка, не подлежат на допълнителна партньорска проверка в този субект на Съюза за период от две години след приключването на партньорската проверка, освен ако не бъде поискано друго от субектите на Съюза или не бъде договорено друго след предложение от МСК.

6. Субектите на Съюза гарантират, че всеки риск от конфликт на интереси по отношение на определените експерти се разкрива на другите субекти на Съюза и на МСК преди началото на партньорската проверка. Субектите на Съюза, които преминават партньорска проверка, могат да възразят срещу определянето на конкретни експерти по надлежно обосновани причини, съобщени на определящите ги субекти на Съюза.

7. **Участващите в партньорските проверки експерти изготвят доклади за констатациите и заключения от проверката. Субектите на Съюза имат право да представят коментари по съответните си проектодоклади, които се прилагат към докладите. Докладите включват препоръки за подобряване на аспектите, обхванати от партньорската проверка. Докладите се представят на МСК и на мрежата на ЕРИКС, когато е уместно. Субектите на Съюза, които са обект на проверка, могат да решат да направят публично достояние своя доклад или редактирана версия на доклада.**

Член 8

Прилагане

1. [...]

2. Документите с насоки и препоръките, отправени в съответствие с член 13, подпомагат изпълнението на разпоредбите, предвидени в настоящата глава.

3. **По искане на МСК субектите на Съюза докладват за специфични аспекти от настоящата глава.**

Глава III
МЕЖДУИНСТИТУЦИОНАЛЕН СЪВЕТ ПО КИБЕРСИГУРНОСТ

Член 9

Междуинституционален съвет по киберсигурност

1. Създава се Междуинституционален съвет по киберсигурност (МСК).

2. МСК отговаря за:

   а) мониторинга на прилагането на настоящия регламент от **субектите** [...] **на Съюза**;

   б) надзора по отношение на изпълнението на общите приоритети и цели от страна на CERT-EU и предоставянето на стратегически насоки на CERT-EU.

3. МСК се състои от:

   а) по един представител, определен от:

      i) Европейския парламент;

      ii) Европейския съвет

      iii) Съвета на Европейския съюз;

      iv) Европейската комисия;

      v) Съда на Европейския съюз;

      vi) Европейската централна банка;

vii) Европейската сметна палата;

viii) Европейската служба за външна дейност;

ix) Европейския икономически и социален комитет;

x) Европейския комитет на регионите;

xi) Европейската инвестиционна банка;

xii) Европейския център за промишлени, технологични и изследователски експертни познания в областта на киберсигурността; и

xiii) Агенцията на Европейския съюз за киберсигурност;

б) трима представители [...], определени от Мрежата от агенции на Съюза (EUAN) по предложение на нейния Консултативен комитет за ИКТ да представляват интересите на агенциите и органите, управляващи своя собствена ИТ среда. [...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

3а. Членовете може да се подпомагат от заместник. Председателят може да покани и други представители на изброените по-горе [...] **субекти** или на други **субекти** [...] на Съюза да присъстват на заседанията на МСК без право на глас.

4. МСК приема своя вътрешен процедурен правилник.

5. В съответствие с вътрешния си процедурен правилник МСК определя председател измежду своите членове за срок от [...] **две** години. Неговият заместник става пълноправен член на МСК за същия срок.

6. МСК провежда заседания **поне три пъти годишно** по инициатива на своя председател **и/или** по искане на CERT-EU **и/**или по искане на някой от неговите членове.

7. Всеки член на МСК разполага с един глас. Решенията на МСК се вземат с обикновено мнозинство, освен ако в настоящия регламент е предвидено друго. Председателят не гласува, освен в случай на равен брой гласове, при което може да участва в гласуването с решаващ глас.

8. МСК може да предприема действия чрез опростена писмена процедура, инициирана в съответствие с вътрешния процедурен правилник на МСК. Съгласно тази процедура съответното решение се счита за одобрено в определения от председателя срок, освен ако някой от членовете не подаде възражение.

9. Ръководителят на CERT-EU**, председателят на групата за сътрудничество за МИС, председателят на EU-CyCLONe и председателят на мрежата на ЕРИКС** или **техните** [...] заместници [...] **могат да** участват **като наблюдатели** в заседанията на МСК, освен ако МСК не реши друго.

10. Секретариатът на МСК се осигурява от [...] **ENISA и отговаря пред председателя на МСК**.

11. Представителите, определени от EUAN по предложение на Консултативния комитет за ИКТ, предават решенията на МСК на **членовете на EUAN** […]. Всяка агенция и орган на Съюза има право да отправя до представителите или до председателя на МСК всякакви въпроси, които счита, че трябва да бъдат отнесени до МСК.

12. [...]

13. МСК може да [...] **създаде** изпълнителен комитет, който да го подпомага в работата, и да му делегира някои от своите задачи и правомощия. МСК определя процедурния правилник на изпълнителния комитет, включително неговите задачи и правомощия, както и мандата на неговите членове.

14. На всеки 12 месеца МСК представя на Съвета доклад, в който подробно се описва напредъкът, постигнат при прилагането на настоящия регламент, и се уточнява по-специално степента на сътрудничество на CERT-EU с неговите национални партньори във всяка от държавите членки. Този доклад представлява принос към двугодишния доклад за състоянието на киберсигурността в Съюза за същия период от време в съответствие с член 15 от Директива [предложението за МИС 2].

Член 10

Задачи на МСК

При упражняване на своите отговорности МСК по-специално:

(a) [...] **ефективно наблюдава и упражнява надзор върху прилагането** на настоящия регламент [...] **и подпомага субектите** [...] на Съюза **с цел укрепване на тяхната киберсигурност**; **за тази цел МСК може да изисква *ad hoc* доклади от CERT-EU и от субектите на Съюза;**

аа) **след стратегическа дискусия приема многогодишна стратегия за повишаване на нивото на киберсигурност в субектите на Съюза и я оценява редовно — най-малко на всеки пет години, като при необходимост я изменя;**

б) одобрява годишната работна програма на CERT-EU въз основа на предложение, **представено от** [...] ръководителя на CERT-EU, и наблюдава нейното изпълнение;

в) одобрява каталог на услугите на CERT-EU въз основа на предложение на ръководителя на CERT-EU **и евентуалните му последващи актуализации**;

г) одобрява годишното финансово планиране на приходите и разходите за дейностите на CERT-EU, включително неговия персонал, въз основа на предложение, представено от ръководителя на CERT-EU;

д) одобрява условията за споразуменията за нивото на обслужване въз основа на предложение на ръководителя на CERT-EU;

е) разглежда и одобрява годишния доклад, изготвен от ръководителя на CERT-EU, който обхваща дейностите на CERT-EU и управлението на средствата от страна на CERT-EU;

ж) одобрява и наблюдава ключовите показатели за ефективност по отношение на CERT-EU, които са определени въз основа на предложение на ръководителя на CERT-EU;

з) одобрява договорености за сътрудничество, **споразумения** [...] за нивото на обслужване или договори между CERT-EU и други субекти съгласно член 17;

и) създава [...] технически консултативни групи [...], които да подпомагат работата на МСК, одобрява техния мандат и определя съответните им председатели.

й) **приема документи с насоки и препоръки въз основа на предложение от CERT-EU съгласно член 13 и дава указания на CERT-EU за издаване, оттегляне или изменение на предложение за документи с насоки или препоръки или за призив за действие;**

к) получава и оценява документи и доклади, представени от субектите на Съюза съгласно настоящия регламент;

л) подкрепя създаването на неформална група, обединяваща местните служители по киберсигурността на всички субекти, и по този начин улеснява обмена на добри практики и информация във връзка с прилагането на настоящия регламент;

м) разработва план за управление на киберкризи в подкрепа на координираното управление на сериозни инциденти на оперативно равнище, засягащи субекти на Съюза, и допринася за редовния обмен на съответна информация, по-специално относно въздействието и тежестта на сериозните инциденти и възможните начини за смекчаване на последиците.

Член 11

Спазване

1. **В съответствие с член 9, параграф 2 и член 10**, МСК **ефективно** наблюдава прилагането на настоящия регламент и на приетите документи с насоки, препоръки и призиви за действие от страна на **субектите** [...] на Съюза. **За тази цел МСК може да поиска информация или документация, необходими за оценка на правилното прилагане на разпоредбите на регламента от субектите на Съюза. За целите на приемането на мерки за съответствие съгласно настоящия член съответният субект на Съюза няма право на глас.**

2. Когато МСК установи, че [...] **субекти** на Съюза не прилагат ефективно или не изпълняват настоящия регламент или документите с насоки, препоръките и призивите за действие, отправени съгласно настоящия регламент, той може, без да се засягат вътрешните процедури на съответния [...] **субект** на Съюза **и след като на засегнатия субект или засегнатото лице е дадена възможност да представи становището си**:

а) да отправи предупреждение **за отстраняване на установените недостатъци в рамките на определен срок, включително препоръки за изменение на документите в областта на киберсигурността, приети от субектите на Съюза въз основа на настоящия регламент**; при необходимост, с оглед на неизбежен риск за киберсигурността, да ограничи аудиторията на предупреждението по подходящ начин;

аа) да издаде мотивирано уведомление на субект на Съюза, в случай че недостатъците, установени в издаденото по-рано предупреждение, не са отстранени в достатъчна степен в определен срок, и официално да уведоми за това становище Съвета, Европейския парламент и Комисията;

б) **да издаде по-специално:** [...]

i. препоръка за извършване на одит на субект на Съюза;

ii. искане за извършване на одит от одиторска служба на трета страна.

в) да изиска от субекта на Съюза да приведе управлението, ръководството и контрола на рисковете за киберсигурността в съответствие с разпоредбите на настоящия регламент, по целесъобразност, по определен начин и в рамките на определен срок.

г) да издава съвети за всички държави членки и субекти на Съюза, като препоръча временно спиране на потоците от данни към субекта на Съюза.

3. Когато МСК е приел мерки съгласно параграф 2, букви а) — г), съответният субект на Съюза представя подробен отчет за мерките и действията, предприети за отстраняване на твърдените недостатъци, установени от МСК. Субектът на Съюза представя този отчет в разумен срок, който се договаря с МСК.

4. Когато МСК счете, че е налице непрекъснато нарушение на разпоредбите на настоящия регламент от страна на субект на Съюза, произтичащо пряко от действия или бездействия на длъжностно лице или друг служител на Съюза, включително на най-високо управленско равнище, МСК изисква от съответния субект да предприеме подходящи действия, включително от дисциплинарен характер, в съответствие по-специално с правилата, установени в Правилника за длъжностните лица и Условията за работа на другите служители на Европейския съюз. За тази цел МСК предава необходимата информация на съответния субект.

Глава IV
CERT-EU

Член 12

Мисия и задачи на CERT-EU

1. [...] [...] **Мисията на CERT-EU** е да допринася за сигурността на некласифицираната ИТ среда на всички **субекти** [...] на Съюза посредством предоставяне на съвети в областта на киберсигурността, осигуряване на подкрепа за предотвратяването, откриването, смекчаването и реагирането на инциденти и осъществяване на дейност като техен координационен център за обмен на информация и реагиране при инциденти в областта на киберсигурността.

1a. CERT-EU събира, управлява, анализира и обменя информация с участниците относно заплахи, уязвими места и инциденти във връзка с некласифицирана инфраструктура на ИКТ. Той координира реакциите на инциденти на междуинституционално равнище и на равнището на субект на Съюза, включително като предоставя или координира предоставянето на специализирана оперативна помощ.

2. CERT-EU изпълнява следните задачи за [...] **субектите** на Съюза:

а) подпомага ги при прилагането на настоящия регламент и допринася за координацията във връзка с прилагането на настоящия регламент чрез разпоредбите [...], изброени в член 13, параграф 1, или чрез *ad-hoc* доклади, поискани от МСК;

б) [...] **предлага стандартните услуги на ЕРИКС за всички субекти на Съюза чрез** пакет от услуги за киберсигурност, описани в неговия каталог на услугите („базови услуги“);

в) поддържа мрежа от партньори и колеги с цел подпомагане на услугите, посочени в членове 16 и 17;

г) насочва вниманието на МСК към всеки въпрос, свързан с прилагането на настоящия регламент и с прилагането на документите с насоки, препоръките и призивите за действие;

д) **въз основа на посочената в параграф 1а информация,** [...] допринася за ситуационната осведоменост на ЕС по отношение на кибернетичното пространство **в тясно сътрудничество с ENISA**. **Тази информация се споделя с МСК, както и с мрежата на ЕРИКС и EU-INTCEN;**

е) действа като еквивалент на определения координатор за субектите на Съюза, както е посочено в член 6 от Директива [предложението за МИС 2].

[...]

[...]

[...]

[...]

[...]

4. **В рамките на компетентностите,** CERT-EU участва в структурирано сътрудничество с [...] **ENISA** за изграждането на капацитет, оперативното сътрудничество и дългосрочните стратегически анализи на киберзаплахите в съответствие с Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета.

5. CERT-EU може да предоставя следните услуги, които не са описани в неговия каталог на услугите („услуги, за които се събира такса“):

   а) услуги за подпомагане на киберсигурността на ИТ средата на [...] **субекти** на Съюза, различни от посочените в параграф 2, въз основа на споразумения за нивото на обслужване и в зависимост от наличните ресурси;

   б) услуги за подпомагане на свързани с киберсигурността операции или проекти на [...] **субекти** на Съюза, различни от насочените към защитата на тяхната ИТ среда, въз основа на писмени споразумения и с предварителното одобрение на МСК;

   в) услуги за подпомагане на сигурността на ИТ средата на организации, различни от [...] **субектите** на Съюза, които си сътрудничат тясно със [...] **субектите** на Съюза, например чрез възлагане на задачи или отговорности съгласно правото на Съюза, въз основа на писмени споразумения и с предварителното одобрение на МСК.

6. CERT-EU може да организира **или да участва в** учения в областта на киберсигурността или да препоръчва участие в съществуващи учения, по целесъобразност в тясно сътрудничество с [...] **ENISA**, с цел да се изпита нивото на киберсигурност на субектите на Съюза.

7. CERT-EU може да предоставя съдействие на [...] **субектите** на Съюза във връзка с инциденти в класифицирани ИТ среди, ако съответните [...] **субекти на Съюза изрично поискат това съгласно своите съответни процедури**. **В този случай разпоредбите на членове 19—21 от настоящия регламент не се прилагат. Предоставянето на помощ от CERT-EU съгласно настоящия параграф не засяга приложимите правила на държавите членки или на Съюза относно защитата на чувствителна или класифицирана информация.**

8. CERT-EU уведомява субектите на Съюза за своите процедури и процеси за действия при инциденти.

9. CERT-EU може да наблюдава мрежовия трафик на субектите на Съюза със съгласието на съответния субект на Съюза.

10. CERT-EU може, ако това е изрично поискано от политическите служби на субектите на Съюза, да предоставя технически съвети или информация относно имащи отношение политически въпроси.

11. CERT-EU, в сътрудничество с Европейския надзорен орган по защита на данните, подпомага засегнатите субекти на Съюза при справянето с инциденти, водещи до нарушаване сигурността на личните данни.

Член 13

Документи с насоки, препоръки и призиви за действие

1. CERT-EU подпомага прилагането на настоящия регламент, като отправя:

   а) призиви за действие, в които се описват спешни мерки за сигурност, които [...] **субектите** на Съюза настоятелно се призовават да предприемат в рамките на определен срок. Без ненужно забавяне след получаване на поканата за действие съответният субект на Съюза информира CERT-EU за начина, по който са приложени тези мерки;

   б) предложения до МСК за документи с насоки, насочени към всички [...] **субекти** на Съюза или към част от тях;

   в) предложения до МСК за препоръки, насочени към отделни [...] **субекти** на Съюза.

2. Документите с насоки и препоръките могат да включват:

   а) реда и условията за или подобренията на управлението на риска за киберсигурността, както и **мерките за управление на рисковете** за киберсигурността [...];

   б) реда и условията за оценките на зрелостта и плановете за киберсигурност; и

   в) когато е целесъобразно, използването на обща технология и архитектура и свързаните с тях най-добри практики с цел постигане на оперативна съвместимост и общи стандарти, **включително координиран подход към сигурността на веригите за доставка** [...]**.**

[...]

[...]

Член 14

Ръководител на CERT-EU

1. Комисията назначава ръководителя на CERT-EU, след като получи одобрението на две трети от членовете на МСК. Консултации с МСК се провеждат на всички етапи на процедурата преди назначаването на ръководителя на CERT-EU, и по-специално при изготвянето на обявленията за свободна длъжност, разглеждането на кандидатурите и назначаването на комисии за подбор във връзка с тази длъжност.

2. Ръководителят на CERT-EU отговаря за правилното функциониране на CERT-EU, като действа в рамките на правомощията си под ръководството на МСК. Той отговаря за прилагането на стратегическите указания, насоки, цели и приоритети, определени от МСК, и за управлението на CERT-EU, включително на неговите финансови и човешки ресурси. Той докладва редовно на председателя на МСК.

3. Ръководителят на CERT-EU подпомага отговорния упълномощен разпоредител с бюджетни кредити при изготвянето на годишния отчет за дейността, съдържащ финансова информация и информация за управлението, включително резултатите от контрола, изготвян съгласно член 66, параграф 9 от Финансовия регламент, и редовно му докладва за изпълнението на мерките, по отношение на които са му били делегирани правомощия.

4. Ръководителят на CERT-EU изготвя ежегодно финансово планиране на административните приходи и разходи за дейностите, предложението за годишна работна програма, предложението за каталог на услугите на CERT-EU и неговото преразглеждане, предложението за реда и условията за сключване на споразумения за нивото на обслужване и предложението за ключови показатели за ефективност за CERT-EU, които се одобряват от МСК в съответствие с член 10.

При преразглеждането на списъка на услугите в каталога на услугите на CERT-EU ръководителят на CERT-EU взема предвид отпуснатите на CERT-EU ресурси.

5. Ръководителят на CERT-EU [...] представя на МСК [...] **годишни** доклади относно резултатите от дейността на CERT-EU, финансовото планиране, приходите, изпълнението на бюджета, сключените споразумения за нивото на обслужване и сключените писмени споразумения, сътрудничеството с партньори и колеги и предприетите от персонала мисии, включително докладите, посочени в член 10, [...] **буква а).**

Член 15

Финансови въпроси и въпроси, свързани с персонала

[...]

1а. Макар да е създаден като самостоятелен междуинституционален доставчик на услуги за всички субекти на Съюза, CERT-EU е интегриран в административната структура на една от генералните дирекции на Комисията, така че да се ползва от структурите на Комисията за подкрепа при административната дейност, финансовото управление и счетоводството. Комисията информира МСК за мястото на CERT-EU в административната структура, както и за всички промени във връзка с това. Този подход се оценява редовно, най-късно преди края на всяка многогодишна финансова рамка, установена в съответствие с член 312 от ДФЕС, така че да се даде възможност за предприемане на подходящи действия.

2. По отношение на прилагането на административните и финансовите процедури ръководителят на CERT-EU действа под ръководството на Комисията.

3. Задачите и дейностите на CERT-EU, включително услугите, предоставяни на [...] **субектите** на Съюза съгласно член 12, параграфи 2, [...] 4 и 6 и член 13, параграф 1, които подлежат на финансиране от функцията на многогодишната финансова рамка, предназначена за европейската публична администрация, се финансират чрез отделен бюджетен ред от бюджета на Комисията. Определените за CERT-EU длъжности се описват подробно в бележка под линия към щатното разписание на Комисията.

4. **Субектите** [...] на Съюза, различни от посочените в параграф 3, правят годишни финансови вноски за дейността на CERT-EU с цел покриване на услугите, предоставяни от CERT-EU съгласно параграф 3. Съответните вноски се правят въз основа на насоките, дадени от МСК и договорени между всеки субект и CERT-EU в споразуменията за нивото на обслужване. Вноските представляват справедлив и пропорционален дял от общите разходи за предоставените услуги. Те се получават по отделния бюджетен ред, посочен в параграф 3, като целеви приходи, както е предвидено в член 21, параграф 3, буква в) от Регламент (ЕС, Евратом) 2018/1046 на Европейския парламент и на Съвета[12].

5. Разходите за задачите, определени в член 12, параграф 5, се възстановяват от [...] **субектите** на Съюза, които използват услугите на CERT-EU. Приходите се разпределят по бюджетните редове в подкрепа на разходите.

[12] Регламент (ЕС, Евратом) 2018/1046 на Европейския парламент и на Съвета от 18 юли 2018 г. за финансовите правила, приложими за общия бюджет на Съюза, за изменение на регламенти (ЕС) № 1296/2013, (ЕС) № 1301/2013, (ЕС) № 1303/2013, (ЕС) № 1304/2013, (ЕС) № 1309/2013, (ЕС) № 1316/2013, (ЕС) № 223/2014 и (ЕС) № 283/2014 и на Решение № 541/2014/ЕС и за отмяна на Регламент (ЕС, Евратом) № 966/2012 (ОВ L 193, 30.7.2018 г., стр. 1).

Член 16

Сътрудничество между CERT-EU и партньори от държавите членки

1. CERT-EU **без ненужно забавяне** си сътрудничи и обменя информация с националните си партньори в държавите членки, **по-конкретно** [...] [...] [...], **посочените в член 9 от Директива [предложение за МИС 2]** ЕРИКС **и/или, когато е приложимо, с националните компетентни органи** и единните звена за контакт, посочени в член 8 от Директива [предложение за МИС 2], по отношение на киберзаплахи, уязвимости и инциденти, по евентуални мерки за противодействие и по всички въпроси от значение за подобряването на защитата на ИТ средите на [...] **субектите** на Съюза, включително чрез мрежата на ЕРИКС, посочена в член 13 от Директива [предложение за МИС 2].

1а. CERT-EU незабавно уведомява съответните посочени в параграф 1 национални партньори в дадена държава членка, когато узнае за значителни инциденти, настъпили на територията на тази държава членка, освен ако CERT-EU не разполага с информацията, че засегнатият субект на Съюза вече е докладвал за такъв инцидент в съответствие с член 20, параграф 2а.

2. CERT-EU [...] **без ненужно забавяне** обменя информация за конкретни инциденти с националните партньори в държавите членки, за да се улесни откриването на подобни киберзаплахи или инциденти **или за да се способства за анализа на инцидента,** без да е необходимо съгласието на засегнатия [...] **субект** на Съюза. CERT-EU [...] **не** обменя информация за конкретен инцидент, от която става ясна мишената на киберинцидента, [...] **освен когато:**

а) има съгласието на засегнатия субект на Съюза;

б) засегнатият субект на Съюза вече е огласил, че е засегнат;

в) няма съгласие от засегнатия субект на Съюза, но огласяването на това кой е засегнатият субект на Съюза би увеличило вероятността инцидентите другаде да бъдат избегнати или смекчени. За тези решения е необходимо одобрение от ръководителя на CERT-EU. Засегнатият субект на Съюза се уведомява преди огласяването.

Член 17

Сътрудничество между CERT-EU и [...] <u>други</u> партньори

1. CERT-EU може да си сътрудничи с партньори [...] **в Европейския съюз, различни от посочените в член 16**, включително с партньори от специфични промишлени отрасли, във връзка с инструменти и методи, например техники, тактики, процедури и добри практики, както и във връзка с киберзаплахи и уязвимости. За [...] сътрудничеството с такива партньори CERT-EU иска предварително одобрение от МСК **за всеки отделен случай**. **Когато CERT-EU установява сътрудничество с такива партньори, CERT-EU информира съответните посочени в член 16, параграф 1 национални партньори в държавата членка, в която се намира партньорът.**

2. CERT-EU може да си сътрудничи с други партньори, например търговски субекти, международни организации, национални субекти от държави извън Европейския съюз или отделни експерти, с цел събиране на информация относно общи и специфични киберзаплахи, уязвимости и възможни мерки за противодействие. За по-широкообхватно сътрудничество с такива партньори CERT-EU иска предварително одобрение от МСК **за всеки отделен случай**.

3. CERT-EU може, **при условие че е налице споразумение или договор за неразгласяване със съответния партньор** и със съгласието на [...] **субекта на Съюза**, който е засегнат от инцидент, да предоставя информация във връзка с **конкретен** инцидента на партньори**, посочени в параграфи 1 и 2 единствено с цел** [...] да допринесат за неговия анализ. **Тези споразумения или договори за неразгласяване подлежат на правна проверка съгласно съответните вътрешни процедури на Комисията. За споразуменията и договорите за неразгласяване не е необходимо предварителното одобрение на МСК, но неговият председател трябва да бъде информиран за тях.**

4. **По изключение CERT-EU може да сключва споразумения за нивото на обслужване с образувания, които не са субекти на Съюза, с предварително одобрение от МСК.**

Глава V
ЗАДЪЛЖЕНИЯ ЗА СЪТРУДНИЧЕСТВО И ДОКЛАДВАНЕ

Член 18

Обработка на информация

1. CERT-EU и [...] **субектите** на Съюза спазват задължението за професионална тайна в съответствие с член 339 от Договора за функционирането на Европейския съюз или равностойни приложими уредби.

2. Разпоредбите на Регламент (ЕО) № 1049/2001[13] на Европейския парламент и на Съвета се прилагат по отношение на искания за публичен достъп до документи, съхранявани от CERT-EU, включително предвиденото в този регламент задължение за консултиране със [...] **субектите на Съюза и по целесъобразност с държавите членки,** когато дадено искане се отнася до техни документи.

[...]

4. При обработката на информация от страна на CERT-EU и от [...] **субектите** на Съюза се спазват **приложимите** правила [...] относно информационната сигурност [...].

[...]

Член 19

[...] ***Обмен на информация относно киберсигурността***

-1. Субектите на Съюза може на доброволен принцип да предоставят на CERT-EU информация за киберзаплахи, инциденти, ситуации, близки до инциденти, и уязвимости, които ги засягат. CERT-EU осигурява наличието на ефикасни средства за комуникация за улесняване на обмена на информация със субектите на Съюза. CERT-EU може да обработва задължителните уведомления с предимство пред доброволните уведомления.

[13] 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).

1. За [...] **да изпълнява мисията и задачите си, определени в член 12,** CERT-EU [...] може да поиска от [...] **субектите** на Съюза да му предоставят информация от регистрите на съответните си ИТ системи, **включително информация, свързана с киберзаплахи, ситуации, близки до инциденти, уязвимости, показатели за компрометиране, предупреждения във връзка с киберсигурността и препоръки относно конфигурацията на инструментите за киберсигурност за откриване на киберинциденти** [...]. [...] Субектът на Съюза, към който е отправено искането, предава исканата информация и всички последващи актуализации по нея без ненужно забавяне.

2. [...] Субектите на Съюза предоставят на CERT-EU, при искане от негова страна и без ненужно забавяне, цифрова информация, създадена чрез използването на електронните устройства, засегнати от съответните инциденти. CERT-EU може да поясни допълнително какъв вид цифрова информация му е необходима за постигане на ситуационна осведоменост и за реагиране при инциденти.

3. CERT-EU може да обменя **със субектите на Съюза** информация за конкретен инцидент, която разкрива [...] кой е **субектът** на Съюза, засегнат от инцидента, само със съгласието на съответния субект. **При отказ на съгласие съответният субект представя надлежно обосновани причини на CERT-EU.** [...]

4. Задълженията за споделяне не обхващат класифицирана информация на ЕС (КИЕС) и информация, **чието разпространение извън получаващия субект на Съюза е изключено от източника на информацията чрез видима маркировка, освен ако източникът на информацията** [...] **изрично позволява тази информация да се споделя със CERT-EU**. [...]

Член 20

[...] ***Задължения за докладване***

-1. За значителен се счита инцидент, който:

а) е причинил или е в състояние да причини сериозно оперативно смущение във функционирането на субекта на Съюза или финансови загуби за съответния субект на Съюза;

б) е засегнал или е в състояние да засегне други физически или юридически лица, като причини значителни имуществени или неимуществени вреди.

1. Всички [...] **субекти** на Съюза **представят** [...] **на CERT-EU**: [...]

[...].

(a) без излишно забавяне и при всички случаи в срок от 24 часа след узнаването за значителния инцидент — ранно предупреждение, в което, когато е приложимо, се посочва дали се подозира, че значителният инцидент се дължи на незаконосъобразно или злонамерено действие или е имал или би могъл да има трансгранично въздействие;

(b) без излишно забавяне и при всички случаи в срок от 72 часа след узнаването за значителния инцидент — уведомление за инцидент, в което, когато е приложимо, се актуализира информацията, посочена в буква а), и се дава първоначална оценка за значителния инцидент, неговата тежест и въздействие, както и, когато има такива, **показателите** за компрометиране;

(c) по искане на CERT-EU — междинен доклад за съответните актуализации на състоянието;

(d) окончателен доклад не по-късно от един месец след подаването на уведомлението за значителен инцидент по буква б), включващ най-малко следното:

i) подробно описание на значителния инцидент, неговата тежест и въздействие;

ii) вида на заплахата или причината, която вероятно е породила значителния инцидент;

iii) приложените и текущите мерки за ограничаване;

iv) когато е приложимо, трансграничното въздействие на значителния инцидент;

(е) в случаи на продължаващи значителни инциденти към момента на представяне на окончателния доклад, посочен в буква г), доклад за напредъка към този момент и окончателен доклад в рамките на един месец след инцидента.

[...]

ж) [...]

з) [...]

и) [...]

й) [...]

2а. Всички субекти на Съюза споделят в рамките на един и същ график информацията, докладвана в съответствие с параграф 1, със съответните национални партньори, посочени в член 16, параграф 1, където се намира тя.

3. CERT-EU **всяко тримесечие** представя [...] **на МСК, EU INTCEN и мрежата на ЕРИКС** [...] обобщен доклад, включващ анонимизирани и обобщени данни относно [...] киберзаплахите, [...] уязвимостите **в съответствие с член 19, отговорите на субектите на Съюза на призиви за действие в съответствие с член 13, параграф 1, буква а)** и значителните инциденти, за които е уведомен в съответствие с параграф 1. **Този доклад представлява принос към двугодишния доклад за състоянието на киберсигурността в Съюза по член 15 от Директива [предложението за МИС 2].**

4. **В срок от [6 месеца след датата на влизане в сила на настоящия регламент]** МСК [...] издава документи с насоки или препоръки, **уточняващи допълнително** [...] реда и условията, както и **формата** за изготвянето на уведомлението и съдържанието **за докладването** [...]. **Документите с насоки или препоръки трябва да са надлежно съобразени с разпоредбите, прилагани чрез актове за изпълнение съгласно член 20, параграф 11 от Директива [предложение за МИС 2].** CERT-EU разпространява подходящите технически подробности, които дават възможност за проактивно откриване и реагиране на инциденти или за предприемане на смекчаващи мерки от страна на [...] **субектите** на Съюза.

5. Задълженията за [...] **докладване** не обхващат КИЕС и информация, **чието разпространение извън получаващия субект на Съюза е изключено от източника на информацията чрез видима маркировка, освен ако източникът на информацията** [...] **изрично позволява тази информация да се споделя със CERT-EU**. [...]

Член 21

Координация и сътрудничество при реагиране на инциденти [...]

1. При осъществяване на дейност като координационен център за обмен на информация и реагиране при инциденти в областта на киберсигурността CERT-EU улеснява обмена на информация по отношение на киберзаплахи, уязвимости и инциденти между:

   а) **субектите** [...] на Съюза;

   б) партньорите, посочени в членове 16 и 17.

2. CERT-EU**,** [...] **когато е уместно — в тясно сътрудничество с ENISA съгласно член 7, параграф 7, буква г) от Акта за киберсигурността**[14], улеснява координацията между [...] **субектите** на Съюза при реагирането на инциденти, което включва:

   а) принос за съгласувани външни комуникации;

   [...]

   в) оптимално използване на оперативните ресурси;

   г) координация с други механизми за реакция при кризи на равнището на Съюза.

3. **В тясно сътрудничество с ENISA** CERT-EU подпомага [...] **субектите** на Съюза по отношение на ситуационната осведоменост във връзка с киберзаплахи, уязвимости и инциденти.

---

14 Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета от 17 април 2019 г. относно ENISA (Агенцията на Европейския съюз за киберсигурност) и сертифицирането на киберсигурността на информационните и комуникационните технологии, както и за отмяна на Регламент (ЕС) № 526/2013 (Акт за киберсигурността).

4. **До [12 месеца след датата на влизане в сила на настоящия регламент], въз основа на предложение от CERT-EU,** МСК [...] **приема документи с** насоки **или препоръки** относно координацията и сътрудничеството при реагиране на значителни инциденти. Когато се подозира, че даден инцидент е с престъпен характер, CERT-EU предоставя съвети как да се съобщи за инцидента на правоприлагащите органи.

Член 22

Управление на сериозни инциденти [...]

-1. За да подпомогне координираното управление на сериозни инциденти на оперативно равнище, засягащи субекти на Съюза, и да допринесе за редовния обмен на съответна информация между субектите на Съюза и с държавите членки, МСК, в тясно сътрудничество със CERT-EU и ENISA, разработва план за управление на киберкризи въз основа на дейностите, описани в член 21, параграф 2, като включва най-малко следните елементи:

а) условията и реда за координацията и информационния поток между субектите на Съюза за управлението на сериозни инциденти на оперативно равнище;

б) общите стандартни оперативни процедури (СОП);

в) обща таксономия за тежестта на сериозните инциденти и за точките, които могат да породят криза;

г) редовните учения;

д) сигурните канали за комуникация, които да се използват;

е) звено за контакт за EU-CyCLONe, което споделя съответната информация с EU-CyCLONe като принос към споделената ситуационна осведоменост.

1. CERT-EU координира реакциите на [...] **субектите** на Съюза в случай на сериозни **инциденти** [...]. Той поддържа опис на техническия експертен опит, който би бил необходим при реагиране на инциденти в случай на **сериозни инциденти** [...].

2. [...] **Субектите** на Съюза допринасят за описа на техническия експертен опит, като предоставят ежегодно актуализиран списък на наличните в техните организации експерти с подробно описание на техните специфични технически умения.

3. След специално искане от държавата членка, в която се намира засегнатият субект на Съюза, и с [...] одобрението на [...] **засегнатия субект** на Съюза [...] CERT-EU може да се обърне и към експертите от списъка, посочен в параграф 2, за да допринесат за реакцията в случай на сериозен **инцидент** [...] **във** [...] **въпросния** [...] **субект на Съюза**.

ГЛАВА VI
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 23

Първоначално преразпределяне на бюджета

Комисията предлага преразпределяне на персонал и финансови ресурси от съответните [...] **субекти** на Съюза към бюджета на Комисията. Преразпределянето се извършва едновременно с първия бюджет, който се приема след влизането в сила на настоящия регламент.

Член 24

Преглед

1. МСК, със съдействието на CERT-EU, периодично докладва на Комисията за прилагането на настоящия регламент. МСК може също да отправя препоръки към Комисията във връзка с **преразглеждането** [...] на настоящия регламент.

2. Комисията представя доклад за прилагането на настоящия регламент на Европейския парламент и на Съвета най-късно [...] **36** месеца след влизането в сила на настоящия регламент, след което докладва на всеки три години.

3. Комисията извършва оценка на функционирането на настоящия регламент и докладва на Европейския парламент, Съвета, Европейския икономически и социален комитет и Комитета на регионите не по-**късно** [...] от пет години след датата на влизане в сила. **Ако е необходимо, докладът се придружава от законодателно предложение.**

Член 25

Влизане в сила

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

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

Съставено в Брюксел на […] година.

За Европейския парламент
Председател

За Съвета
Председател

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

[...]

ПРИЛОЖЕНИЕ II

[...]

[...]

[...]

[...]

[...]

[...]

[...]