Съвет на
Европейския съюз

Брюксел, 26 ноември 2021 г.
(OR. en)

14337/21

Междуинституционално досие:
2020/0359(COD)

CODEC 1541
CSC 416
CSCI 147
CYBER 312
DATAPROTECT 269
JAI 1295
MI 891
TELECOM 435

БЕЛЕЖКА

От:	Генералния секретариат на Съвета
До:	Съвета
№ предх. док.:	9583/2/21, 11724/21
№ док. Ком.:	14150/20
Относно:	Предложение за директива на Европейския парламент и на Съвета относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148 *– Общ подход*

I. ВЪВЕДЕНИЕ

1. На 16 декември 2020 г. Комисията прие предложението за директива относно мерки за високо общо ниво на киберсигурност в Съюза (преработена директива за МИС или „МИС 2“)[1] с цел да замени настоящата директива за мрежова и информационна сигурност („Директивата за МИС“)[2].

[1] Предложение за директива на Европейския парламент и на Съвета относно мерки за високо общо ниво на киберсигурност в Съюза и за отмяна на Директива (ЕС) 2016/1148.

[2] Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета от 6 юли 2016 г. относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза.

Предложението беше едно от действията, предвидени в Стратегията на ЕС за киберсигурност за цифровото десетилетие[3], за да се гарантира, че гражданите и предприятията се възползват от надеждни цифрови технологии.

2. Предложението се основава на член 114 от Договора за функционирането на Европейския съюз (ДФЕС) и има за цел допълнително да се подобрят устойчивостта и капацитетът за реагиране при инциденти на публичноправните и частноправните субекти, компетентните органи и Съюза като цяло.

3. В Европейския парламент комисията, която отговаря за предложението, е комисията по промишленост, изследвания и енергетика (ITRE). Комисията ITRE прие доклада на докладчика на 28 октомври 2021 г.

4. Европейският икономически и социален комитет прие становището си на 28 април 2021 г.

5. На 3 февруари 2021 г. Комитетът на постоянните представители реши да проведе консултация по предложението с Европейския комитет на регионите[4]. Досега Европейският комитет на регионите не е дал становището си.

6. Европейският надзорен орган по защита на данните прие становището си на 11 март 2021 г.[5]

7. В заключенията[6] си от 22 март 2021 г. относно стратегията на ЕС за киберсигурност за цифровото десетилетие, Съветът взе под внимание новото предложение, което се базира на директивата за МИС, и изрази отново своята подкрепа за укрепването и хармонизирането на националните рамки за киберсигурност и за трайно сътрудничество между държавите членки.

8. В заключенията си от 21—22 октомври 2021 г. Европейският съвет призова за постигане на напредък в работата по предложението за преработена директива за МИС.

---

3 14133/20.
4 5573/21.
5 Становище 5/2021 относно стратегията за киберсигурност и Директивата за МИС 2.0
6 6722/21.

II. РАБОТА В ПОДГОТВИТЕЛНИТЕ ОРГАНИ НА СЪВЕТА

9. Разглеждането на предложението в Съвета се извършва в рамките на Хоризонталната работна група по въпроси на кибернетичното пространство (по-нататък „HWPCI“). Разглеждането на предложението започна по време на португалското председателство на 19 януари с внимателен прочит на предложението, което даде възможност на държавите членки да представят своите въпроси и да изтъкнат основните си опасения, както и да получат подробни обяснения от Комисията относно промените в преработената директива.

10. По време на португалското председателство HWPCI посвети 17 заседания на представянето и прочита на предложението. На заседанието на Съвета по транспорт, телекомуникации и енергетика от 4 юни 2021 г. беше представен доклад за напредъка.

11. Оттогава работата продължи и беше активизирана по време на словенското председателство с цел постигане на общ подход на заседанието на Съвета (Транспорт, телекомуникации и енергетика) на 3 декември 2021 г.Словенското председателство посвети 15 заседания на преработката на предложението за МИС 2, както и много двустранни обсъждания на всички равнища.

12. HWPCI съсредоточи работата си върху преработването на текста на предложението, първоначално относно взаимодействието на Директивата за МИС 2 със секторното законодателство и обхвата, по-специално по отношение на публичната администрация, DNS кореновите сървъри и клаузата за изключване, както и, наред с други теми, относно партньорските проверки, юрисдикцията и взаимопомощта, координираното оповестяване на уязвимости, базите данни с имена на домейни и регистрационните данни и международното сътрудничество.

13. Първото компромисно предложение по текста на предложението за директива беше представено на 21 септември 2021 г.[7] въз основа на писмените бележки и неофициалните документи, получени от държавите членки, както и на предварителните компромисни предложения относно взаимодействието на Директивата за МИС 2 със секторното законодателство и относно обхвата на Директивата за МИС 2.

[7] 12019/21.

14. Последната преработка[8] на компромисното предложение на председателството беше обсъдена на равнище работна група на 22 ноември 2021 г. Въпреки че делегациите като цяло приветстваха компромисния текст, някои от тях все пак изразиха резерви за разглеждане или направиха бележки по части от компромисното предложение. В някои части на текста все още се предлага частично преформулиране от технически характер.

III. ПО СЪЩЕСТВО

15. Въз основа на обсъжданията на равнище работна група като основни политически въпроси бяха набелязани следните точки:

a) Обхват (член 2)

От началото на обсъжданията на предложението за МИС 2 основното опасение, изразено от държавите членки, беше значителното увеличаване на броя на субектите, попадащи в обхвата на директивата, и по-специално въвеждането на правилото за размер на предприятието, според което всички средни и големи субекти, които извършват дейност в секторите или предоставят услугите, обхванати от Директивата за МИС 2, попадат в нейния обхват. Въпреки че в компромисното предложение се запазва това общо правило, то включва допълнителни разпоредби, за да се гарантира необходимата пропорционалност, по-високо равнище на управление на риска и ясни критерии за критичност за определяне на субектите, които попадат в обхвата на директивата. Освен това компромисното предложение включва конкретни разпоредби относно приоритизирането на използването на мерки за надзор, като се следва основан на риска подход.

[8] 12019/5/21 REV 5.

б) Публична администрация (член 2, параграф 2а)

Включването на публичната администрация в обхвата на Директивата за МИС 2 беше широко обсъждана тема, като се има предвид, че секторът на публичната администрация е по-различен от другите сектори, обхванати от Директивата за МИС 2. Председателството се стреми към балансиран подход, който отчита особеностите на националните рамки за публична администрация и гарантира, че държавите членки разполагат с известна гъвкавост при определянето на субектите на публичната администрация, попадащи в обхвата на МИС 2. Поради това в компромисния текст МИС 2 се прилага за субекти на публичната администрация на централните правителства, като същевременно държавите членки могат също така да постановят, че директивата се прилага за субекти на публичната администрация на регионално и местно равнище.

в) Клаузата за изключване (член 2, параграфи 3а и 3аа)

Държавите членки поискаха да се доизясни клаузата за изключване, тъй като директивата не се прилага за субекти, които извършват дейности основно в областта на отбраната, националната сигурност, обществената сигурност или правоприлагането, или за дейности, свързани с националната сигурност или отбрана. Съдебната власт, парламентите и централните банки също са изключени.

г) Взаимодействие със секторното законодателство

Държавите членки подчертаха необходимостта от привеждане в съответствие на Директивата за МИС 2 и секторното законодателство, по-специално Регламента относно оперативната устойчивост на цифровите технологии във финансовия сектор („Регламента DORA“) и Директивата относно устойчивостта на критичните субекти („Директивата за УКС“). Директивата за МИС 2, която следва да бъде основата за минимална хармонизация в областта на киберсигурността, съдържа специален член относно специфичните секторни законодателни актове на Съюза (член 2б). Що се отнася до взаимодействието с Директивата за УКС, компромисното предложение осигурява по-голяма яснота относно подхода, обхващащ всички опасности. Други важни допълнения са свързани с договореностите за сътрудничество между компетентните органи съгласно съответните правни актове.

д) Партньорско обучение (член 16)

С някои изключения държавите членки се противопоставиха на установяването от Комисията на задължителни партньорски проверки. Предложеният компромис гарантира, че новият механизъм за партньорско обучение се основава на взаимно доверие и е доброволен и ръководен от държавите членки процес.

е) Юрисдикция и териториалност (член 24) и взаимопомощ (член 34)

Държавите членки изразиха опасения във връзка с последиците от въвеждането на диференцирана юрисдикция за субектите в сектора на ИКТ, както предлага Комисията. В компромисния текст беше изяснено положението с юрисдикцията въз основа на вида на субектите и беше пояснена формулировката относно взаимопомощта.

ж) Задължения за докладване (член 20)

Вследствие на опасенията, изразени от държавите членки, че това би натоварило прекомерно субекти, попадащи в обхвата на Директивата за МИС 2, и би довело до свръхдокладване, задължителното докладване за значителни киберзаплахи беше изключено от компромисния текст.

IV. ЗАКЛЮЧЕНИЕ

16. На 24 ноември 2021 г. Комитетът на постоянните представители постигна съгласие по компромисния текст в приложението и реши да го представи на Съвета (Транспорт, телекомуникации и енергетика) за приемане на общ подход.

17. Ето защо Съветът се приканва да одобри представения от председателството компромисен текст в приложението и да приеме общ подход на заседанието си на 3 декември 2021 г.

ПРИЛОЖЕНИЕ

Предложение за

ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

относно мерки за високо общо ниво на киберсигурност в Съюза, за изменение на Регламент (ЕС) 910/2014 и Директива (ЕС) 2018/1972 и за отмяна на Директива (ЕС) 2016/1148

(Текст от значение за ЕИО)

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[9],

като взеха предвид становището на Комитета на регионите[10],

в съответствие с обикновената законодателна процедура,

[9] ОВ С , , p. .
[10] ОВ С , , p. .

като имат предвид, че:

(1) Директива (ЕС) 2016/1148 на Европейския парламент и на Съвета[11] има за цел да изгради способности в областта на киберсигурността в Съюза, да ограничи заплахите за мрежите и информационните системи, използвани за предоставяне на основни услуги в ключови сектори, и да гарантира непрекъснатостта на тези услуги при инциденти с киберсигурността, като по този начин допринася за ефективното функциониране на икономиката и обществото на Съюза.

(2) След влизането в сила на Директива (ЕС) 2016/1148 бе постигнат значителен напредък при повишаването на нивото на устойчивост на киберсигурността на Съюза. Прегледът на тази директива показа, че е послужила като катализатор за институционалния и регулаторния подход към киберсигурността в Съюза, като е проправила пътя за значителна промяна в нагласите. Директивата осигури завършването на националните рамки чрез определянето на национални стратегии [...] **за сигурността на мрежите и информационните системи**, създаването на национални способности и изпълнението на регулаторни мерки, обхващащи съществени инфраструктури и участници, установени от всяка държава членка. Тя допринесе и за развитието на сътрудничеството на равнището на Съюза посредством установяването на групата за сътрудничество[12] и мрежа**та** от национални екипи за реагиране при инциденти с компютърната сигурност („мрежата на ЕРИКС“)[13]. Прегледът на Директива (ЕС) 2016/1148 обаче разкри, че независимо от тези постижения, тя има и присъщи слабости, които пречат на намирането на ефективни решения за съвременните и възникващи предизвикателства в областта на киберсигурността.

---

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

12 Член 11 от Директива (ЕС) 2016/1148

13 Член 12 от Директива (ЕС) 2016/1148

(3) Мрежите и информационните системи се превърнаха в централен елемент на всекидневния живот на фона на бързата цифрова трансформация и взаимосвързаността на обществото, включително в трансграничния обмен. Това развитие води до разширяването на набора от заплахи, пораждайки нови такива, и изисква адаптирани, координирани и новаторски реакции във всички държави членки. Броят, мащабите, сложността, честотата и въздействието на свързаните със сигурността инциденти се увеличават и представляват крупна заплаха за функционирането на мрежите и информационните системи. В резултат на това киберинцидентите могат да попречат на извършването на стопански дейности в рамките на вътрешния пазар, да причинят финансови загуби, да подкопаят доверието на потребителите и да причинят големи вреди на икономиката и обществото на Съюза. Затова подготвеността и ефективността в областта на киберсигурността сега са по-важни от всякога за правилното функциониране на вътрешния пазар.

(4) Правното основание за Директива (ЕС) 1148/2016 е член 114 от Договора за функционирането на Европейския съюз (ДФЕС), чиято цел е създаването и функционирането на вътрешния пазар чрез усъвършенстване на мерките за сближаване на националните правила. Изискванията за киберсигурност, наложени на субектите, предоставящи услуги или икономически относими дейности, се различават значително в държавите членки от гледна точка на вида на изискванията, степента им на подробност и метода на надзор. Тези различия водят до допълнителни разходи и пораждат затруднения за предприятията, предлагащи трансгранично стоки или услуги. Наложените от една държава членка изисквания, които са различни от наложените в друга или дори са в противоречие с тях, може съществено да засегнат тези трансгранични дейности.

Освен това възможността за неоптимално изготвяне или прилагане на [...] **мерки** за киберсигурност в една държава членка е вероятно да има последици по отношение на нивото на киберсигурност на държави членки, особено предвид интензивния трансграничен обмен. Прегледът на Директива (ЕС) 2016/1148 показва големи различия в прилагането ѝ от държавите членки, включително във връзка с нейния обхват, чието очертаване в много голяма степен бе оставено на преценката на държавите членки. Директива (ЕС) 2016/1148 предоставя на държавите членки и много широка свобода на преценка по отношение на прилагането на предвидените в нея задължения, свързани със сигурността и докладването за инциденти. Поради това тези задължения бяха приложени по значително различаващи се начини на национално равнище. Подобни различия в прилагането възникнаха и по отношение на разпоредбите на директивата относно надзора и правоприлагането.

(5) Всички тези различия водят до фрагментирането на вътрешния пазар и могат да имат вредно въздействие върху функционирането му, засягайки по-специално трансграничното предоставяне на услуги и нивото на устойчивост в областта на киберсигурността поради прилагането на различни [...] **мерки**. Настоящата директива има за цел да премахне тези големи различия между държавите членки, по-специално посредством предвиждането на минимални правила относно функционирането на координирана регулаторна рамка, установяването на механизми за ефективното сътрудничество между отговорните органи във всяка държава членка, актуализирането на списъка със сектори и дейности, подчинени на задълженията за киберсигурност, и предоставянето на ефективни правни средства за защита и санкции, способстващи за ефективното правоприлагане на тези задължения. Поради това Директива (ЕС) 2016/1148 следва да бъде отменена и заменена с настоящата директива.

(6) [...] Държавите членки **следва да могат** да вземат необходимите мерки, с които да гарантират защитата на основните интереси на своята сигурност, да опазват обществения ред и обществената сигурност и да създават условия за разследването, разкриването и наказателното преследване на престъпления[...]. [...]**Директивата следва да не се прилага за определени публичноправни или частноправни субекти, които извършват дейности в тези области. Тя следва да не се прилага и за дейностите на субектите, които се извършват в тези области. Нещо повече,** нито една държава членка не може да бъде задължавана да предоставя информация, чието разкриване би противоречало на основните интереси на нейната обществена сигурност. От значение са [...] националните правила **или** тези на Съюза за защита на класифицираната информация, споразуменията за неразкриване на информация и неформалните споразумения за неразкриване на информация като протокола за обмен на информация с цветен код за поверителност (Traffic Light Protocol)[14].

(6a) Правото на Съюза относно защитата на личните данни и неприкосновеността на личния живот се прилага за всяко обработване на лични данни съгласно настоящата директива. По-конкретно настоящата директива не засяга Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО на Европейския парламент и на Съвета и поради това по-специално следва да не засяга задачите и правомощията на независимите надзорни органи, компетентни да следят за спазването на съответното право на Съюза в областта на защитата на данните.

---

14 Протоколът за обмен на информация с цветен код за поверителност (TLP) е средство за обменящото информация лице да уведоми своята аудитория за евентуални ограничения за по-нататъшното разпространение на тази информация. Използва се в почти всички общности на ЕРИКС и в някои Центрове за анализ и обмен на информация (ЦАОИ).

(7) С отмяната на Директива (ЕС) 2016/1148 приложното поле следва да се разшири така, че да обхване по-голяма част от секторите на икономиката с оглед на доводите, изложени в съображения 4—6. Ето защо обхватът по отношение на секторите от Директива (ЕС) 2016/1148 следва да бъде разширен, за да се осигури пълно включване на секторите и услугите от жизненоважно значение за ключови обществени и икономически дейности във вътрешния пазар. Правилата не следва да се различават в зависимост от това дали субектите са оператори на основни услуги или доставчици на цифрови услуги. Това разграничаване е доказано остаряло, тъй като не отразява настоящата значимост на секторите или услугите за обществените и икономическите дейности във вътрешния пазар.

(8) В съответствие с Директива (ЕС) 2016/1148, държавите членки са отговорни за определянето на субектите, които отговарят на критериите и се квалифицират като оператори на основни услуги („процес по определяне“). За да се отстранят големите различия сред държавите членки в това отношение и да се гарантира правната сигурност относно изискванията за управление на риска и задълженията за докладване по отношение на всички относими субекти, следва да се установи еднакъв критерий, определящ субектите, попадащи в приложното поле на настоящата директива. Този критерий следва да се състои в прилагането на правилото за размер на предприятието, при което всички средни и големи предприятия, съгласно определението в Препоръка 2003/361/ЕО на Комисията[15], упражняващи дейност в секторите или предоставящи видовете услуги, обхванати от настоящата директива, попадат в нейния обхват. [...]

[15] Препоръка 2003/361/ЕО на Комисията от 6 май 2003 година относно определението за микро-, малки и средни предприятия (ОВ L 124, 20.5.2003 г., стр. 36).

(8a) За да се осигури ясен обзор на субектите, попадащи в обхвата на настоящата директива, държавите членки следва да могат да установят национални механизми за самоуведомяване, които да изискват от субектите, попадащи в обхвата на настоящата директива, да представят най-малко своето наименование, адрес и данни за контакт, както и сектора, в който извършват дейност, или вида услуги, които предоставят, и когато е приложимо, списък на държавите членки, в които субектът предоставя услугите си, на компетентните органи съгласно настоящата директива или на органите, определени за тази цел от държавите членки. Държавите членки могат да вземат решение относно подходящите механизми, когато съществуват регистри на национално равнище, които позволяват идентифицирането на субектите, попадащи в обхвата на настоящата директива.

(9) [...] **Микросубекти или** малки [...] субекти които изпълняват определени критерии, сочещи че те имат ключова роля за икономиките и обществата на държавите членки или за конкретни сектори или видове услуги, също следва да бъдат обхванати от настоящата директива. Държавите членки следва да отговарят за [...] предаването на [...] Комисията **най-малко на съответната информация относно броя на идентифицираните субекти, сектора, към който принадлежат, или вида на услугите, които предоставят, и специфичните критерии, въз основа на които са идентифицирани. Държавите членки могат още да решат, когато това е в съответствие с националните правила за сигурност, да представят на Комисията наименованията на тези субекти.**

(9a) Органите на публичната администрация, които извършват дейности в областта на националната сигурност, отбраната, обществената сигурност, правоприлагането, както и съдебната власт, парламентите и централните банки, са изключени от обхвата на настоящата директива. За целите на настоящата директива не се счита, че субектите с регулаторна компетентност извършват дейности в областта на правоприлагането и следователно те не са изключени на тези основания от обхвата на настоящата директива. Освен това структурите на публичната администрация на централното държавно управление, които са създадени съвместно с трета държава в съответствие с международно споразумение, не попадат в обхвата на настоящата директива.

(9аа) Държавите членки следва да могат да установят, че субектите, определени преди влизането в сила на настоящата директива като оператори на основни услуги в съответствие с Директива (ЕС) 2016/1148, следва да се считат за основни субекти.

(9ааа) Настоящата директива не се прилага за дипломатическите и консулските мисии на държавите членки в чужбина и за тяхната ИКТ инфраструктура, използвана от такива мисии, доколкото тази инфраструктура се намира в чужбина или се експлоатира за потребители в чужбина.

(10) Комисията, в сътрудничество с групата за сътрудничество, може да издава насоки за прилагането на критериите, приложими за микропредприятията и малки предприятия.

(11) [...] **Субектите, попадащи в обхвата на настоящата директива, следва да бъдат класифицирани в две категории: съществени и значими, като се отчитат степента на критичност на сектора или на вида на предоставяната от тях услуга, както и техният размер**. **В този смисъл следва надлежно да се вземат предвид и всички съответни секторни оценки на риска или насоки от компетентните органи, когато е приложимо.** Както съществените, така и значимите субекти следва да подлежат на [...] изискванията за управление на риска и задълженията за докладване. Режимите на надзор и санкции за тези две категории субекти следва да са различни, за да се гарантира справедлив баланс между **основаните на риска** изисквания и задължения, от една страна, и административната тежест, произтичаща от надзора на съответствието, от друга.

(12) **С настоящата директива се определя основата за мерките за управление на риска в областта на киберсигурността и задълженията за докладване във всички сектори от нейния обхват. С цел да се избегне фрагментирането на разпоредбите в областта на киберсигурността в правните актове на Съюза, когато се счита, че за да се гарантира високо равнище на киберсигурност, са необходими допълнителни секторни разпоредби**, отнасящи се до мерки за управление на риска за киберсигурността **и задължения за докладване, Комисията следва да прецени дали такива разпоредби биха могли да бъдат заложени в акт за изпълнение съгласно правомощията, предвидени в настоящата директива**. **Ако тези актове не са подходящи за тази цел**, специфично секторно законодателство би могло да допринесе за гарантиране на високо равнище [...] на киберсигурност, като същевременно се отчитат в пълна степен особеностите и сложността на [...] съответните сектори. **Основанията защо акт за изпълнение съгласно правомощието, предвидено в настоящата директива, не е подходящ, трябва да бъдат обяснени в специфичното за сектора законодателство. Същевременно такива специфични за отделните сектори разпоредби на правните актове на Съюза следва надлежно да бъдат съобразени с необходимостта от всеобхватна и хармонизирана рамка в областта на киберсигурността.** [...] Това [...] не засяга съществуващите изпълнителни правомощия, предоставени на Комисията в редица сектори, включително в транспорта и енергетиката.

(12a) Когато специфичен за сектора правен акт на Съюза **съдържа разпоредби**, [...] изискващи съществените или значимите субекти да приемат **мерки, които имат поне равностоен ефект на предвидените в настоящата директива задължения** за управление на риска за киберсигурността [...] **и задължения** за уведомяване за **значителни** инциденти или значителни киберзаплахи, [...] следва да се прилагат тези специфични за сектора разпоредби, **включително относно надзора и правоприлагането**. **При определянето на равностойния ефект на задълженията, предвидени в специфичните за сектора разпоредби на правен акт на Съюза, следва да се вземат предвид следните аспекти: i) мерките за управление на риска за киберсигурността следва да се състоят от подходящи и пропорционални технически и организационни мерки за управление на рисковете за сигурността на мрежите и информационните системи, които съответните субекти използват при предоставянето на своите услуги, и следва да включват като минимум всички елементи, определени в настоящата директива; ii) задължението за уведомяване за значителни инциденти и киберзаплахи следва да бъде най-малко равностойно на задълженията, установени в настоящата директива по отношение на съдържанието, формата и сроковете на уведомленията; iii) редът и условията за докладване от страна на субектите и съответните органи на специфичните за отделните сектори правни актове на Съюза следва да бъдат най-малко равностойни на изискванията, определени в настоящата директива по отношение на тяхното съдържание, формат и срокове, и следва да отчитат ролята на ЕРИКС; iv) изискванията за трансгранично сътрудничество за съответните органи следва да бъдат най-малко равностойни на определените в настоящата директива. Ако специфичните за сектора разпоредби на правен акт на Съюза не обхващат всички субекти в конкретен сектор, попадащ в обхвата на настоящата директива, съответните разпоредби на настоящата директива следва да продължат да се прилагат по отношение на субектите, които не са обхванати от тези специфични за сектора разпоредби.**

(12аа) Комисията **следва периодично да прави преглед на прилагането на изискването за равностоен ефект във връзка със специфичните за отделните сектори разпоредби на правните актове на Съюза** [...]. **Комисията ще се консултира с групата за сътрудничество при подготовката на периодичния преглед.**

(12ааа) Бъдещите специфични за сектора правни актове на Съюза следва надлежно да отчитат определенията, посочени в член 4 от настоящата директива, и рамката за надзор и правоприлагане, установена в глава VI от настоящата директива.

(12аб) Когато специфични за отделните сектори разпоредби на правните актове на Съюза изискват от основни или значими субекти да приемат мерки с най-малко равностоен ефект на предвидените в настоящата директива задължения за докладване, следва да се избягва припокриването на задълженията за докладване и следва да се гарантира съгласуваност и ефективност на обработването на уведомленията за киберзаплахи или киберинциденти. За тази цел тези специфични за отделните сектори разпоредби могат да позволят на държавите членки да създадат общ, автоматичен и пряк механизъм за съобщаване на значителни инциденти и киберзаплахи както на органите, чиито задачи са определени в съответните специфични за отделните сектори разпоредби, така и на компетентните органи, включително единното звено за контакт и ЕРИКС, по целесъобразност, отговарящи за задачите в областта на киберсигурността, предвидени в настоящата директива, или за механизъм, който гарантира систематичен и незабавен обмен на информация и сътрудничество между съответните органи и ЕРИКС относно обработката на такива уведомления. С цел опростяване на докладването и прилагане на общия, автоматичен и пряк механизъм за докладване държавите членки могат, в съответствие със специфичното за сектора законодателство, да използват единната входна точка, създадена от тях в съответствие с член 11, параграф 5а от настоящата директива. За да се гарантира хармонизация, задълженията за докладване съгласно специфичните за сектора правни актове на Съюза следва да бъдат приведени в съответствие с посочените в настоящата директива. Държавите членки могат да определят, че компетентните органи съгласно настоящата директива или националните ЕРИКС са адресати на докладването в съответствие със специфичното за сектора законодателство.

(13) Регламент XXXX/XXXX на Европейския парламент и на Съвета следва да се счита за специфичен за сектора правен акт на Съюза във връзка с настоящата директива с оглед на субектите във финансовия сектор. Разпоредбите на Регламент XXXX/XXXX във връзка с мерките за управление на риска в областта на информационните и комуникационните технологии (ИКТ), управлението на инцидентите при ИКТ и особено уведомяването за инциденти, както и тези относно изпитването на оперативната устойчивост на цифровите технологии, споразуменията за обмен на информация и риска при ИКТ, пораждан от участието на трети страни, следва да се прилагат вместо установените [...] **в** настоящата директива. Затова държавите членки не следва да прилагат разпоредбите на настоящата директива относно управлението на риска, свързан с киберсигурността, и задълженията за докладване, [...] и надзор и правоприлагането по отношение [...] финансови субекти, обхванати от Регламент XXXX/XXXX. Същевременно е от значение да се поддържат тясна връзка и обмен на информация с финансовия сектор съгласно настоящата директива. За тази цел Регламент XXXX/XXXX позволява на [...] Европейските надзорни органи (ЕНО) за финансовия сектор и националните компетентни органи съгласно Регламент XXXX/XXXX да участват в [...] **работата** на групата за сътрудничество, както и да обменят информация и да сътрудничат с единните звена за контакт, определени в изпълнение на настоящата директива, [...] **както** и с националните ЕРИКС. Компетентните органи съгласно Регламент XXXX/XXXX следва да предоставят подробности за големи инциденти с ИКТ **и значителни киберзаплахи** и на единните звена за контакт, **компетентните органи или националните ЕРИКС**, определени съгласно настоящата директива. **Това е постижимо чрез автоматично и пряко препращане на уведомленията за инциденти или чрез обща платформа за докладване.** Освен това държавите членки следва да продължат да включват финансовия сектор в своите стратегии за киберсигурност, а дейностите на националните ЕРИКС могат да обхващат и него.

(13а) За да се избегнат пропуски и дублиране на задълженията в областта на киберсигурността, наложени на субектите в сектора на въздухоплаването, посочени в точка 2, буква а) от приложение I, националните органи, определени съгласно регламенти (ЕО) № 300/2008[16] **и (ЕС) 2018/1139**[17] **на Европейския парламент и на Съвета, и компетентните органи съгласно настоящата директива следва да си сътрудничат във връзка с прилагането на мерките за управление на риска в областта на киберсигурността и надзора на тези мерки на национално равнище. Съответствието на даден субект с мерките за управление на риска за киберсигурността съгласно настоящата директива [...] може да се счита от националните органи, определени съгласно регламенти (ЕО) № 300/2008 и (ЕС) 2018/1139, за отговарящи на изискванията, предвидени в посочените регламенти, и съответните делегирани актове и актове за изпълнение, приети съгласно посочените регламенти.**

---

16 Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета от 11 март 2008 година относно общите правила в областта на сигурността на гражданското въздухоплаване и за отмяна на Регламент (ЕО) № 2320/2002 **(ОВ L 97, 9.4.2008 г., стр. 72).**

17 **Регламент (ЕС) 2018/1139 на Европейския парламент и на Съвета от 4 юли 2018 г. относно общи правила в областта на гражданското въздухоплаване и за създаването на Агенция за авиационна безопасност на Европейския съюз и за изменение на регламенти (ЕО) № 2111/2005, (ЕО) № 1008/2008, (ЕС) № 996/2010, (ЕС) № 376/2014 и на директиви 2014/30/ЕС и 2014/53/ЕС на Европейския парламент и на Съвета и за отмяна на регламенти (ЕО) № 552/2004 и (ЕО) № 216/2008 на Европейския парламент и на Съвета и Регламент (ЕИО) № 3922/91 на Съвета (ОВ L 212, 22.8.2018 г., стр. 1).**

(14) С оглед на взаимовръзките между киберсигурността и физическата сигурност на субектите следва да се осигури съгласуван подход между Директива (ЕС) XXX/XXX на Европейския парламент и на Съвета и настоящата директива. За постигането на тази цел държавите членки следва да гарантират, че критичните и равностойни на тях субекти съгласно Директива (ЕС) XXX/XXX се считат за съществени субекти по силата на настоящата директива. Държавите членки следва също така да гарантират, че стратегиите им за киберсигурност предвиждат рамка за политики за усъвършенствана координация между компетентния орган съгласно настоящата директива и компетентния орган съгласно Директива (ЕС) XXX/XXX в контекста на обмена на информация относно инциденти и киберзаплахи и упражняването на задачи по надзор. **Компетентните** [...] органи съгласно двете директиви следва да си сътрудничат и да обменят информация, по-специално във връзка с идентифицирането на критични субекти, киберзаплахи, рискове и инциденти, свързани с киберсигурността, **както и несвързани с киберсигурността рискове, заплахи и инциденти**, засягащи критичните субекти или **[субекти, еквивалентни на критични субекти]**, [...] **включително** мерките в областта на киберсигурността **и физическите** мерки, взети от критичните субекти, **и резултатите от надзорните дейности, извършени по отношение на тези субекти. Освен това, за да се рационализират надзорните дейности между компетентните органи, определени съгласно двете директиви, и за да се сведе до минимум административната тежест за засегнатите субекти, компетентните органи следва да се стремят да хармонизират образците за уведомяване за инциденти и надзорните процеси.** [...] **Когато е целесъобразно,** компетентните органи съгласно Директива (ЕС) XXX/XXX[...] **могат да поискат** от компетентните органи съгласно настоящата директива [...] да упражнят своите правомощия по надзор и правоприлагане [...] **по отношение на** съществен субект, идентифициран като критичен. [...]

(14a) Субектите, принадлежащи към сектора на цифровата инфраструктура, по същество се основават на мрежови и информационни системи и поради това задълженията, наложени на тези субекти с настоящата директива, следва да третират по всеобхватен начин физическата сигурност на тези системи като част от техните задължения за управление на риска и докладване в областта на киберсигурността. Тъй като тези въпроси са обхванати от настоящата директива, задълженията, предвидени в глави III—VI от Директива (ЕС) XXX/XXX [УКС], не се прилагат за такива субекти.

(15) Поддържането и запазването на надеждна, устойчива и сигурна система за имена на домейни (DNS) е ключов фактор за запазването на целостта на интернет и е от съществено значение за неговото непрекъснато и стабилно функциониране, от което зависят цифровата икономика и обществото. Ето защо настоящата директива следва да се прилага за доставчици на DNS услуги по **DNS** веригата на **обезпечаване и** преобразуване, **които са от значение за вътрешния пазар,** включително [...] **регистри** на имената на домейни от първо ниво (TLD) [...], **субектите, предоставящи услуги за регистрация на имена на домейни, оператори на** сървъри за окончателно или рекурсивно преобразуване на имена на домейни. **Терминът „доставчик на DNS услуги“ следва да не се прилага за DNS услуги, извършвани за собствени цели на съответния субект и свързаните с него субекти. Задълженията в областта на киберсигурността, произтичащи от настоящата директива за тази категория доставчици, са строго ограничени до мерките за управление на риска за киберсигурността и докладването и следователно не засягат управлението на глобалната DNS от страна на многостранната общност.**

(16) Компютърните услуги „в облак“ следва да обхващат услуги, позволяващи широк отдалечен достъп при поискване до променлив по мащаб и еластичен набор от разпределени компютърни ресурси, които могат да бъдат ползвани съвместно. Тези компютърни ресурси включват ресурси като мрежи, сървъри или друга инфраструктура, операционни системи, софтуер, средства за съхранение, приложения и услуги. **Моделите на услугите за изчисления в облак включват, наред с другото, инфраструктура като услуга (IaaS), платформа като услуга (PaaS), софтуер като услуга (SaaS) и мрежа като услуга (NaaS).** Моделите на внедряване на компютърни услуги „в облак“ следва да включват частен, общностен, публичен и хибриден облак. Горепосочените модели за внедряване и предоставяне на услуги имат същото значение като условията за ползване и моделите на внедряване, определени съгласно стандарта ISO/IEC 17788:2014. Възможността потребителят на компютърни услуги „в облак“ едностранно и самостоятелно да си набавя компютърен капацитет, като например сървърно време или мрежово хранилище, без каквато и да е човешка намеса от страна на доставчика на компютърни услуги „в облак“, може да се опише като администриране при поискване. Понятието „широк отдалечен достъп“ се използва, за да се опише, че услугите „в облак“ се предоставят в мрежата и достъпът до тях се осъществява чрез механизми, насърчаващи използването на разнородни платформи с „тънки“ и „дебели“ клиенти (включително мобилни телефони, таблети, лаптопи, работни станции).

Понятието „променлив по мащаб“ означава, че компютърните ресурси се предоставят гъвкаво от доставчиците на компютърни услуги „в облак“, независимо от географското местоположение на ресурсите, за да бъдат отразени промените в търсенето. Понятието „еластичен набор“ се използва за описание на компютърните ресурси, които се предоставят и използват в зависимост от търсенето, за да може бързо да се увеличават или намаляват ресурсите, които са на разположение, в зависимост от работното натоварване. Изразът „които могат да бъдат ползвани съвместно“ се използва за описание на компютърните ресурси, които се предоставят на множество ползватели, които имат общ достъп до услугата, но обработването се извършва отделно за всеки ползвател, въпреки че услугата се предоставя от едно и също електронно оборудване. Понятието „разпределен“ се използва, за да се опишат компютърни ресурси, които са разположени на различни свързани в мрежа компютри или устройства и които осъществяват комуникация и координация помежду си посредством съобщения.

(17) Предвид възникването на новаторски технологии и нови бизнес модели се очаква на пазара да се появят нови модели за внедряване и предоставяне на компютърни услуги „в облак“ в отговор на развиващите се потребителски нужди. В този контекст компютърните услуги „в облак“ могат да се предоставят под формата на силно „разпределени“ услуги, които се извършват още по-близо до мястото на генериране и събиране на данните, като по този начин техният традиционен модел ще бъде заменен от модел с висока степен на разпределеност („периферни изчисления“).

(18) Услугите, предлагани от доставчиците на услуги на центрове за данни, невинаги могат да бъдат предоставяни под формата на компютърна услуга „в облак“. Следователно центровете за данни невинаги съставляват част от инфраструктурата на компютърни услуги „в облак“. За да бъдат обхванати всички рискове за сигурността на мрежите и информационните системи, настоящата директива следва да обхваща също доставчици на услуги, специфични за центровете за данни, които не са компютърни услуги „в облак“. За целите на настоящата директива понятието „услуга на център за данни“ следва да обхваща предоставянето на услуга, включващо конструкции или групи конструкции, предназначени за централизирано разполагане, свързване и експлоатация на информационно и мрежово технологично оборудване, предоставящо услуги за съхранение, обработване и пренос на данни, заедно с всички съоръжения и инфраструктурата за електроразпределение и контрол на околната среда. Понятието „услуга на център за данни“ не се прилага по отношение на вътрешни, корпоративни центрове за данни, притежавани и използвани за собствени цели на съответния субект.

(19) Доставчиците на пощенски услуги по смисъла на Директива 97/67/ЕО на Европейския парламент и на Съвета[18], [...] **включително** доставчиците на [...] куриерски услуги, следва да са подчинени на настоящата директива, ако предоставят поне една от операциите от веригата на пощенски доставки, и по-специално събирането, сортирането или доставката, включително услугите за вземане от адрес. Превозът, когато не е предприет във връзка с някоя от тези операции, следва да попада извън обхвата на пощенските услуги.

---

18 Директива 97/67/ЕО на Европейския парламент и на Съвета от 15 декември 1997 година относно общите правила за развитието на вътрешния пазар на пощенските услуги в Общността и за подобряването на качеството на услугата (ОВ L 15, 21.1.1998 г., стр. 14).

(20) Тази нарастваща взаимозависимост е резултат от все по-трансграничния и взаимообвързан характер на мрежата за доставка на услуги, използваща ключови инфраструктури в целия Съюз, в секторите енергетика, транспорт, цифрова инфраструктура, питейна и отпадъчна вода, здравеопазване, някои аспекти на публичната администрация, както и космическото пространство, доколкото става въпрос за предоставянето на определени услуги, зависещи от наземни инфраструктури, притежавани, управлявани и използвани от държавите членки или от частноправни субекти (т.е. без инфраструктурите, притежавани, управлявани и използвани от Съюза или от негово име като част от космическите му програми). Тази взаимозависимост означава, че всяко смущение, дори и такова, което първоначално се свежда до един субект или сектор, може да има стъпаловидни ефекти в по-широк план, потенциално водещи до широкообхватни и трайни отрицателни последствия за доставката на услуги на вътрешния пазар. Пандемията от COVID-19 показа колко са уязвими нашите все по-взаимозависими общества за рискове с ниска вероятност.

(**20а**) **С цел постигане и поддържане на високо равнище на киберсигурност националните стратегии за киберсигурност, изисквани от настоящата директива, следва да се състоят от съгласувани рамки, които предвиждат управление в областта на киберсигурността. Тези стратегии могат да се състоят от един или няколко документа със законодателен или незаконодателен характер.**

(21) С оглед на различията в националните структури на управление и с цел да се запазят вече съществуващи секторни правила или надзорни и регулаторни органи на Съюза, държавите членки следва да могат да определят повече от един национален компетентен орган, отговарящ за изпълнение на задачите, свързани със сигурността на мрежите и информационните системи на съществени и значими субекти съгласно настоящата директива. Държавите членки следва да могат да възлагат тези функции на съществуващ орган.

(22) За да се улесни трансграничното сътрудничество и комуникация сред органите и да се осигури възможност за ефективно изпълнение на настоящата директива, е необходимо всяка държава членка да определи национално единно звено за контакт, което да отговаря за координацията на въпросите, свързани със сигурността на мрежите и информационните системи, и за трансграничното сътрудничество на равнището на Съюза.

(23) Компетентните органи или ЕРИКС следва да получават уведомления за инциденти от субектите по ефективен и ефикасен начин, **също така с цел да се улесни, когато е целесъобразно, своевременното реагиране на инциденти и да се предостави отговор на уведомяващия орган**. На единните звена за контакт следва да се възложи задачата да предават уведомленията за инциденти на единните звена за контакт на други засегнати държави членки. [...]

(23а) В специфичните за отделните сектори правни актове на Съюза, които изискват мерки за управление на риска за киберсигурността или задължения за докладване с най-малко равностоен ефект на предвидените в настоящата директива, може да се предвиди определените от тях компетентни органи да упражняват своите надзорни и правоприлагащи правомощия във връзка с такива мерки или задължения със съдействието на компетентните органи, определени в съответствие с настоящата директива. Съответните компетентни органи биха могли да установят договорености за сътрудничество за тази цел. В такива договорености за сътрудничество биха могли да се уточнят, наред с другото, процедурите за координиране на надзорните дейности, включително процедурите за разследвания и проверки на място в съответствие с националното право, както и да се предвиди механизъм за обмен на съответната информация между компетентните органи относно надзора и правоприлагането, включително достъп до информация, свързана с киберпространството, поискана от компетентните органи, определени в съответствие с настоящата директива.

(24) Държавите членки следва да разполагат с достатъчно технически и организационен капацитет, за да предотвратяват, идентифицират, реагират и ограничават инцидентите и рисковете в мрежите и информационните системи. Ето защо държавите членки следва да гарантират, че разполагат с добре функциониращи ЕРИКС, известни още като екипи за незабавно реагиране при компютърни инциденти (CERT), които да отговарят на основните изисквания, за да се гарантират ефективни и съвместими способности за справяне с инциденти и рискове и да се осигури ефективно сътрудничество на равнището на Съюза. С цел да се подобри връзката на доверие между субектите и ЕРИКС, когато ЕРИКС е част от компетентния орган, държавите членки [...] **може** да обмислят функционалното разделение между изпълняваните от ЕРИКС оперативни задачи, особено свързаните с обмена на информация и оказването на подкрепа за субектите, и надзорните дейности на компетентните органи.

(25) По отношение на личните данни ЕРИКС следва да могат да предоставят, в съответствие с Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета[19] във връзка с личните данни, от името на субект и при поискване от негова страна съгласно настоящата директива, активно сканиране на мрежите и информационните системи, използвани за предоставянето на техните услуги. **Когато е приложимо**, държавите членки следва да имат за цел да гарантират еднакво равнище на технически възможности за всички секторни ЕРИКС. Държавите членки могат да поискат помощ от Агенцията на Европейския съюз за киберсигурност (ENISA) при създаването на националните ЕРИКС.

(26) Предвид значението на международното сътрудничество в областта на киберсигурността, ЕРИКС следва да имат възможността да участват в мрежите за международно сътрудничество в допълнение към участието им в мрежата на ЕРИКС, създадена с настоящата директива. **Поради това ЕРИКС и компетентните органи биха могли да обменят информация, включително лични данни, с ЕРИКС на трети държави или с техните органи за целите на изпълнението на своите задачи в съответствие с Регламент (ЕС) 2016/679. В случай на липса на решение относно адекватното ниво на защита, прието в съответствие с член 45 от Регламент (ЕС) 2016/679, или на подходящи гаранции съгласно член 46 от същия регламент, обменът на лични данни, който се счита за необходим за смекчаване на значителните киберзаплахи и за реагиране на текущ значителен инцидент, може да се смята за важна причина от обществен интерес по смисъла на член 49, параграф 1, буква г) от Регламент (ЕС) 2016/679.**

[19] Регламент (ЕС) 2016/679 на Европейския парламент и на Съвета от 27 април 2016 година относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни и за отмяна на Директива 95/46/ЕО (Общ регламент относно защитата на данните) (ОВ L 119, 4.5.2016 г., стр. 1).

(27) В съответствие с приложението към Препоръка (ЕС) 2017/1548 на Комисията относно координирана реакция на мащабни киберинциденти и кризи („концепция“)[20], мащабен инцидент следва да означава инцидент със значително въздействие върху поне две държави членки или инцидент, смущението от който надхвърля капацитета за отговор на една държава членка. В зависимост от причината и въздействието си, мащабните инциденти може да се разраснат и да се превърнат в същински кризи, непозволяващи правилното функциониране на вътрешния пазар. Предвид широкомащабния обхват и, в повечето случаи, трансграничния характер на такива инциденти, държавите членки и съответните институции, органи и служби на Съюза следва да си сътрудничат на техническо, оперативно и политическо равнище за правилно координиране на отговора в Съюза.

(28) Тъй като злонамереното използване на уязвимостите в мрежите и информационните системи може да причини значителни смущения и вреди, бързото установяване и отстраняване на тези уязвимости е важен фактор за намаляване на риска за киберсигурността. Затова субектите, които изграждат **или администрират** такива системи, следва да установят подходящи процедури за справяне с уязвимостите, които са открити. Тъй като уязвимостите често се откриват и докладват (оповестяват) от трети страни (докладващи субекти), производителят или доставчикът на ИКТ продукти или услуги следва да въведе и необходимите процедури за получаване на информация за уязвимости от трети страни. В това отношение международните стандарти ISO/IEC 30111 и ISO/IEC [...] **29147** предоставят насоки съответно за справянето с уязвимости и за тяхното оповестяване. По отношение на оповестяването на уязвимости от особено значение е координацията между докладващите субекти и производителите или доставчиците на ИКТ продукти или услуги. С координираното оповестяване на уязвимостите се определя структуриран процес, чрез който те се докладват на организациите по начин, позволяващ на последните да диагностицират и отстранят уязвимостта преди разкриването на подробна информация за нея на трети страни или на обществеността. Координираното оповестяване на уязвимостите следва да включва и координиране между докладващия субект и организацията по отношение на графика за отстраняване и публикуване на уязвимостите.

---

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

(29) Ето защо държавите членки следва да предприемат мерки за улесняване на координираното оповестяване на уязвимостите, като установят съответна национална политика. **Като част от националната си политика държавите членки следва да се стремят да вземат мерки, доколкото е възможно, срещу предизвикателствата, пред които са изправени изследователите в областта на уязвимостта, включително потенциалната опасност да им бъде търсена наказателна отговорност, в съответствие с националния си правен ред.** [...] Държавите членки следва да определят ЕРИКС, който да поеме ролята на „координатор“, при необходимост действащ като посредник между докладващите субекти и производителите или доставчиците на ИКТ продукти или услуги. Задачите на координиращия ЕРИКС следва по-специално да включват установяването на съответните субекти и осъществяването на контакт с тях, подпомагането на докладващите субекти, договарянето на графици за оповестяване и управлението на уязвимостите, засягащи множество организации (многостранно **координирано** оповестяване на уязвимостите). Когато **докладваната** уязвимост **би могла потенциално да окаже значително въздействие върху субекти** [...] в повече от една държав**а** членка, определените ЕРИКС [...] следва да си сътрудничат в рамките мрежата на ЕРИКС**, когато е целесъобразно**.

(30) Достъпът до вярна и своевременна информация относно уязвимостите, засягащи ИКТ продукти и услуги, допринася за подобрено управление на риска, свързан с киберсигурността. В това отношение източниците на публично достъпна информация относно уязвимостите са важен инструмент за субектите и техните потребители, но също и за националните компетентни органи и ЕРИКС. Поради тази причина ENISA следва да създаде регистър на уязвимостите, където съществените и значимите субекти и техните доставчици, както и субектите, които не попадат в приложното поле на настоящата директива, **или определените ЕРИКС** могат доброволно да разкриват уязвимости и да предоставят информация за тях, позволяваща на потребителите да предприемат подходящи ограничаващи мерки.

(31) При все че подобни регистри или бази данни за уязвимости съществуват, те се предоставят и поддържат от установени извън ЕС субекти. Един поддържан от ENISA Европейски регистър на уязвимостите би осигурил повишена прозрачност относно процеса на публикуване преди официалното разкриване на уязвимостта, както и устойчивост в случаи на смущения или прекъсвания при предоставянето на подобни услуги. За да се избегне дублиране на усилията и да се постигне взаимно допълване във възможно най-висока степен, ENISA следва да разгледа възможността за сключване на споразумения за структурирано сътрудничество с подобни регистри под юрисдикцията на трети страни. **По-специално ENISA следва да проучи възможността за тясно сътрудничество с операторите на системата на общите уязвимости и експозиции (CVE), включително възможността да се превърне в главен орган за издаване на идентификационен номер на уязвимостите в системата на CVE.**

(32) **Групата за сътрудничество следва да продължава да подкрепя и улеснява стратегическото сътрудничество и обмена на информация, както и изграждането на доверие между държавите членки.** Групата за сътрудничество следва да съставя работна програма на всеки две години, включваща действията, които да предприема за изпълнение на своите цели и задачи. Времевата рамка на първата програма, приета съгласно настоящата директива, следва да е синхронизирана с времевата рамка на последната програма, приета съгласно Директива (ЕС) 2016/1148, за да се избегнат потенциални смущения в работата на групата.

(33) При разработването на документите с насоки групата за сътрудничество следва постоянно: да картографира националните решения и опит, да извършва оценка на въздействието на резултатите от своята работа върху националните подходи, да обсъжда предизвикателствата при изпълнението и да формулира конкретни препоръки, които да се следват посредством по-доброто прилагане на съществуващите правила.

(34) Групата за сътрудничество следва да остане гъвкав форум и да може да реагира на променящите се и новите приоритети на политиките и предизвикателствата пред тях, като същевременно взема предвид наличността на ресурсите. Тя следва да организира редовни съвместни заседания с относимите частни заинтересованите страни от Съюза с цел обсъждане на дейностите, извършвани от групата, и събиране на информация относно възникващите предизвикателства пред политиките. С цел подобряване на сътрудничество на равнището на Съюза групата следва да разгледа възможността да покани работещите в областта на политиките за киберсигурност органи и служби на Съюза, като например Европейския център за борба с киберпрестъпността (ЕС3), Агенцията за авиационна безопасност на Европейския съюз (ЕААБ) и Агенцията на Европейския съюз за космическата програма (EUSPA), да участват в нейната работа.

(35) На компетентните органи и ЕРИКС следва да бъдат предоставени правомощия да участват в схеми за обмен на длъжностни лица от други държави членки с цел подобряване на сътрудничеството. Компетентните органи следва да предприемат необходимите мерки, за да дадат възможност на длъжностните лица от други държави членки да играят ефективна роля в действията на приемащия компетентен орган.

(35a) Мрежата на ЕРИКС следва да продължи да допринася за укрепване на доверието и да насърчава бързото и ефективно оперативно сътрудничество между държавите членки. За да се засили оперативното сътрудничество на равнището на Съюза, мрежата на ЕРИКС следва да обмисли възможността да покани органи и агенции на Съюза, участващи в политиката в областта на киберсигурността, като например Европол, да участват в нейната работа.

(36) [...]

(36а) С цел да се улесни ефективното прилагане на разпоредбите на настоящата директива, като например управлението на уязвимостите, управлението на риска за киберсигурността, мерките за докладване и договореностите за обмен на информация, държавите членки могат да си сътрудничат с трети държави и да предприемат дейности, които се считат за подходящи за тази цел, включително обмен на информация относно заплахи, инциденти, уязвимости, средства и методи, тактики, техники и процедури, подготвеност и учения за управление на кризи в областта на киберсигурността, обучение, изграждане на доверие и структурирани договорености за обмен на информация. Тези споразумения за сътрудничество следва да са в съответствие с правото на Съюза в областта на защитата на данните.

(37) Държавите членки следва да допринасят за създаването на Механизма на ЕС за реакция при кризи в областта на киберсигурността, предвиден в Препоръка (ЕС) 2017/1584, посредством съществуващите мрежи за сътрудничество, особено **европейската** мрежа за връзка на организациите при кибернетични кризи (EU-CyCLONe), мрежата на ЕРИКС и групата за сътрудничество. EU-CyCLONe и мрежата на ЕРИКС следва да си сътрудничат въз основа на процедурни правила, определящи реда и условията на това сътрудничество**, и да избягват всякакво дублиране на задачите**. В процедурния правилник на EU-CyCLONe следва допълнително да бъдат посочени редът и условията, при които следва да функционира мрежата, включително (но не само) ролите, режимите на сътрудничество, взаимодействията с други относими действащи лица и образците за обмена на информация, както и средствата за комуникация. При управлението на кризи на **политическото** равнище на Съюза съответните страни следва да се основават на Интегрираните договорености за реакция на политическо равнище при кризи (IPCR). За целта Комисията следва да използва процеса ARGUS за многосекторна координация на кризи на високо равнище. Ако кризата засяга важно измерение на външната дейност или общата политика за сигурност и отбрана (ОПСО), следва да бъде активиран Механизмът за реакция при кризи (CRM) на Европейската служба за външна дейност (ЕСВД).

(37a) EU-CyCLONe следва да функционира като междинна мрежа между техническото и политическото равнище при мащабни инциденти и кризи в областта на киберсигурността. Тя следва да засили сътрудничеството на оперативно равнище, като се основава на констатациите на мрежата на ЕРИКС и използва собствени способности за изготвяне на анализ на въздействието на мащабните инциденти и кризи, и като подпомага вземането на решения на политическо равнище. Компетентен орган, отговарящ за управлението на мащабни инциденти и кризи, свързани със сигурността, следва да бъде определен от институциите, органите и агенциите на ЕС за член на EU-CyCLONe.

(38) [...]

(39) [...]

(39a) Отговорността по гарантиране на сигурността на мрежите и информационните системи е в голяма степен на съществени и значими субекти. Следва да се насърчава и развива култура на управление на риска, част от която са оценката на риска и изпълнението на мерки за сигурност, съобразени със съществуващите рискове.

(40) Мерките за управление на риска **следва да отчитат степента на зависимост на субекта от мрежите и информационните системи и** следва да включват мерки за идентифициране на всякакви рискове от инциденти с цел предотвратяване, откриване и справяне с инциденти, както и ограничаване на тяхното въздействие. Сигурността на мрежите и информационните системи следва да включва сигурността на данните, които се съхраняват, предават и обработват.

(40а) Тъй като заплахите за сигурността на мрежите и информационните системи могат да имат различен произход, настоящата директива прилага подход, обхващащ всички опасности, който включва защитата на мрежите и информационните системи и тяхната физическа среда от всякакви събития като кражба, пожар, наводнение, телекомуникационни повреди или прекъсване на захранването, или от всякакъв неразрешен физически достъп и щети и намеса в информацията на субекта и неговите съоръжения за обработка на информация, които биха могли да застрашат наличността, автентичността, целостта или поверителността на съхраняваните, предаваните или обработваните данни или на услугите, предлагани от мрежи и информационни системи или достъпни чрез тях. Поради това мерките за управление на риска следва да са насочени и към физическата сигурност и сигурността на средата, като включват мерки за защита на мрежите и информационните системи на субекта от сривове в системата, човешка грешка, злонамерени действия или природни явления в съответствие с европейските или международнопризнати стандарти, като включените в серията ISO 27000. В това отношение, като част от своите мерки за управление на риска, субектите следва също така да обърнат внимание на сигурността на човешките ресурси и да разполагат с подходящи политики за контрол на достъпа. Тези мерки следва да са в съответствие с Директива XXXX [Директивата за УКС].

(40б) При липсата на подходящи европейски схеми за сертифициране на киберсигурността, приети в съответствие с Регламент (ЕС) 2019/881, държавите членки могат да изискват от субектите да използват сертифицирани ИКТ продукти, услуги и процеси или да получат сертификат съгласно наличните национални схеми за киберсигурност с цел спазване на изискванията за управление на риска за киберсигурността съгласно настоящата директива.

(41) С цел да се избегне налагането на непропорционална финансова и административна тежест върху съществените и значимите субекти, изискванията за управление на риска, свързан с киберсигурността, следва да бъдат пропорционални на риска, който съществува [...] **за** съответната мрежа и информационна система, като се отчитат последните достижения в областта на тези мерки **и разходите за тяхното изпълнение**. **Следва също така надлежно да се вземат предвид размерът на субекта, както и вероятността от настъпване на инциденти и тяхната сериозност.**

(41a) С оглед облекчаване на регулаторната тежест изискванията за прилагане на мерки за управление на риска за киберсигурността за средни, малки или микросубекти следва по принцип да бъдат по-леки, освен ако критериите за критичност или националните оценки на риска не оправдават по-строги изисквания, по-специално по отношение на субектите, които отговарят на критериите, свързани със степента на критичност, определени в настоящата директива.

(42) Съществените и значимите субекти следва да гарантират сигурността на мрежите и информационните системи, които използват в своите дейности. Това са предимно частни мрежи и информационни системи, управлявани от вътрешен ИТ персонал или чиято сигурност е възложена на външни изпълнители. Изискванията за управлението на риска, свързан с киберсигурността, и за докладване съгласно настоящата директива следва да се прилагат по отношение на съответните съществени и значими субекти без оглед на това дали те извършват вътрешно поддръжка на своите мрежи и информационни системи или я възлагат на външни изпълнители.

(42аа) Като се има предвид трансграничният им характер, доставчиците на DNS услуги, регистрите на имената на домейни и субектите, предоставящи услуги за регистрация на имена на домейни от първо ниво, доставчиците на компютърни услуги „в облак“, доставчиците на услуги на центрове за данни, доставчиците на мрежи за предоставяне на съдържание, доставчиците на управлявани услуги и доставчиците на управлявани услуги за сигурност следва да подлежат на по-висока степен на хармонизация на равнището на Съюза. Поради това изпълнението на мерките за киберсигурност следва да бъде улеснено от акт за изпълнение.

(43) Справянето с рискове за киберсигурността, коренящи се във веригата на доставки на даден субект и отношенията му с доставчиците, е от особено значение предвид преобладаващия брой на инцидентите, при които субекти стават жертва на кибератаки или сигурността на техните мрежи и информационни системи бива компрометирана от злонамерено действащи лица благодарение на уязвимостите, засягащи продукти и услуги на трети страни. Затова субектите следва да преценяват и вземат предвид цялостното качество на продуктите и практиките на своите доставчици на продукти и услуги в областта на киберсигурността, включително техните процедури за сигурно разработване.

(44) Сред доставчиците на услуги тези, предоставящи услуги за управление на сигурността в области като реагиране при инциденти, проверка за прониквания, одити за сигурността и консултантски услуги, играят особено важна роля в оценката на усилията на субектите за идентифициране и реагиране на инциденти. Самите тези доставчици на услуги за управление на сигурността обаче също са цел на кибератаки и посредством тяхното тясно интегриране в дейностите на операторите пораждат особен риск за киберсигурността. Ето защо субектите следва да подхождат с повишено внимание към избора на доставчик на услуги за управление на сигурността.

(44a) В контекста на своите надзорни задачи националните компетентни органи могат също да се ползват от услуги в областта на киберсигурността, като например одити на сигурността и проверка за проникване или реагиране при инциденти. За да подпомогне субектите, както и националните компетентни органи при подбора на квалифицирани и надеждни доставчици на услуги в областта на киберсигурността, Комисията, със съдействието на групата за сътрудничество и ENISA, следва да обмисли възможността да поиска изготвянето на проекти за европейски схеми за сертифициране на киберсигурността в съответствие с член 48 от Регламент (ЕС) 2019/881.

(45) Субектите следва да намерят решения и за рискове за киберсигурността, произтичащи от взаимодействията и отношенията им с други заинтересовани страни в рамките на една по-широка екосистема. Субектите по-специално следва да предприемат подходящи мерки, за да гарантират, че сътрудничеството им с академичните и научноизследователските институции е в съответствие с техните политики в областта на киберсигурността и следва добрите практики по отношение на сигурния достъп до информация и нейното разпространение като цяло, както и по-специално по отношение на защитата на интелектуалната собственост. По подобен начин, с оглед на важността и стойността на данните за дейността на субектите, те трябва да предприемат всички необходими мерки за киберсигурност, когато ползват услуги на трети страни за преобразуването и анализа на данните.

(46) За да се отговори допълнително на рисковете по веригата на доставка и да се подпомогнат субектите, упражняващи дейност в обхванати от настоящата директива сектори, правилно да управляват веригата на доставка и свързаните с доставчика рискове за киберсигурността, групата за сътрудничество, включваща съответните национални органи, в сътрудничество с Комисията и ENISA, следва да извърши координирани секторни оценки на веригата на доставка, както това бе вече направено за 5G мрежите в съответствие с Препоръка (ЕС) 2019/534 относно киберсигурността на 5G мрежите[21], с цел да се установи за всеки сектор кои са критичните ИКТ услуги, системи или продукти, относимите заплахи и уязвимости.

[21] Препоръка (ЕС) 2019/534 на Комисията от 26 март 2019 година относно киберсигурността на 5G мрежите (ОВ L 88, 29.3.2019 г., стр. 42).

(47) С оглед на характеристиките на съответния сектор, в секторните оценки на веригата на доставка следва да се вземат предвид техническите и, когато е уместно, нетехническите фактори, включително определените в Препоръка (ЕС) 2019/534 относно киберсигурността на 5G мрежите, в координираната в целия ЕС оценка на риска на сигурността на 5G мрежите и в инструментариума на ЕС за киберсигурност на 5G технологиите, договорен от групата за сътрудничество. За да се установят веригите на доставки, които следва да са предмет на координирана оценка на риска, следва да бъдат взети предвид следните критерии: i) степента, в която съществените и значимите субекти използват и разчитат на конкретни критични ИКТ услуги, системи или продукти; ii) значението на конкретни критични ИКТ услуги, системи или продукти за изпълнението на критични или чувствителни функции, включително обработването на лични данни; iii) наличието на алтернативни ИКТ услуги, системи или продукти; iv) устойчивостта на цялостната верига на доставки на ИКТ услуги, системи или продукти срещу смущаващи събития и v) за възникващи ИКТ услуги, системи или продукти, тяхната потенциална бъдеща значимост за дейностите на субектите.

(48) С цел да се облекчат правните задължения, наложени на доставчиците на обществени електронни съобщителни мрежи или общественодостъпни електронни съобщителни услуги и на доставчиците на удостоверителни услуги, свързани със сигурността на техните мрежи и информационни системи, както и за да се даде възможност на тези субекти и съответните компетентни органи да се възползват от установената с настоящата директива правна рамка (включително определяне на ЕРИКС, отговарящ за управлението на рисковете и инцидентите, участие на компетентните органи и служби в работата на групата за сътрудничество и мрежата на ЕРИКС), те следва да бъдат включени в приложното поле на настоящата директива. Ето защо съответстващите разпоредби, предвидени в Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета[22] и Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета[23], отнасящи се до налагането на мерки за сигурност и уведомяване по отношение на тези видове субекти, следва да бъдат отменени.

---

[22] Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 година относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ L 257, 28.8.2014 г., стр. 73).

[23] Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета от 11 декември 2018 година за установяване на Европейски кодекс за електронни съобщения (ОВ L 321, 17.12.2018 г., стр. 36).

(48a) Задълженията, свързани със сигурността, предвидени в настоящата директива, следва да се считат за допълващи изискванията, наложени на доставчиците на удостоверителни услуги съгласно Регламент (ЕС) № 910/2014 (Регламент относно електронната идентификация и удостоверителните услуги). От доставчиците на удостоверителни услуги следва да се изисква да предприемат всички подходящи и пропорционални мерки за управление на рисковете за техните услуги, включително по отношение на клиентите и доверяващите се трети страни, и да докладват за инциденти, свързани със сигурността, съгласно настоящата директива. Тези задължения за сигурност и докладване следва да се отнасят и до физическата защита на предоставяната услуга. Член 24 от Регламент (ЕС) № 910/2014 продължава да се прилага.

(48aa) Държавите членки могат да възложат ролята на компетентни органи за удостоверителни услуги на надзорните органи по Регламента относно електронната идентификация и удостоверителните услуги, за да се гарантира продължаването на действащите практики и да се надгражда върху знанията и опита, придобити при прилагането на Регламента относно електронната идентификация и удостоверителните услуги. Когато тази роля е възложена на друг орган, националните компетентни органи съгласно настоящата директива следва да си сътрудничат тясно и своевременно чрез обмен на съответната информация, за да се гарантира ефективен надзор и спазване от страна на доставчиците на удостоверителни услуги на изискванията, посочени в настоящата директива и Регламент [XXXX/XXXX].

Когато е приложимо, националният компетентен орган съгласно настоящата директива следва незабавно да информира надзорния орган по Регламента относно електронната идентификация и удостоверителните услуги за всяка значителна киберзаплаха или киберинцидент с въздействие върху удостоверителните услуги, за която/който е подадено уведомление, както и за всяко несъответствие на доставчик на удостоверителни услуги с изискванията по настоящата директива. За целите на докладването държавите членки могат да използват, когато е приложимо, единната входяща точка, създадена за постигане на общо и автоматично докладване на инциденти както пред надзорния орган по Регламента относно електронната идентификация и удостоверителните услуги, така и пред компетентния орган съгласно настоящата директива. Правилата относно задълженията за докладване не следва да засягат Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО на Европейския парламент и на Съвета[24].

---

[24] Директива 2002/58/ЕО на Европейския парламент и на Съвета от 12 юли 2002 година относно обработката на лични данни и защита на правото на неприкосновеност на личния живот в сектора на електронните комуникации (Директива за правото на неприкосновеност на личния живот и електронни комуникации) (ОВ L 201, 31.7.2002 г., стр. 37).

(49) Когато е целесъобразно и за да се избегнат ненужни смущения, съществуващите национални насоки [...], приети за транспониране на правилата, свързани с мерките за сигурност по член**ове** 40 [...] и 41 от Директива (ЕС) 2018/1972, [...] **следва да се вземат предвид в мерките за транспониране, прилагани от държавите членки във връзка с настоящата директива, като по този начин се надгражда върху знанията и опита, вече придобити в рамките на Директива (ЕС) 2018/1972 във връзка с мерките за управление на риска за сигурността и уведомяването за инциденти**. **ENISA може също така да разработи насоки относно изискванията за сигурност и докладване за доставчиците на обществени електронни съобщителни мрежи или обществено достъпни електронни съобщителни услуги с цел улесняване на хармонизацията, прехода и свеждането до минимум на смущенията. Държавите членки могат да възложат ролята на компетентни органи в областта на електронните съобщения на националните регулаторни органи, за да се гарантира продължаването на действащите практики и да се надгражда върху знанията и опита, придобити в рамките на Директива (ЕС) 2018/1972.**

(50) Предвид нарастващото значение на междуличностните съобщителни услуги без номерà, е необходимо да се гарантира, че и за тях се прилагат подходящи изисквания за сигурност с оглед на тяхната специфика и икономическо значение. Така доставчиците на такива услуги следва също да осигурят ниво на сигурност на мрежите и информационните системи, съответстващо на съществуващия риск. Като се има предвид, че доставчиците на междуличностни съобщителни услуги без номерà обикновено не упражняват действителен контрол върху преноса на сигнали по мрежи, степента на риск за такива услуги в някои отношения може да се разглежда като по-ниска от тази за традиционните електронни съобщителни услуги. Същото се отнася и за междуличностните съобщителни услуги, при които се използват номерà и не се упражнява действителен контрол върху преноса на сигнали.

(51) Вътрешният пазар разчита на функционирането на интернет повече от всякога. Услугите на практически всички съществени и значими субекти са зависими от предоставяните по интернет услуги. За да се осигури гладкото предоставяне на услуги от страна на съществените и значимите субекти, от значение е обществените електронни съобщителни мрежи, като например опорните мрежи на интернет или подводните комуникационни кабели, да имат въведени подходящи мерки за киберсигурност и да докладват за свързаните с тях инциденти.

(52) Когато е [...] **приложимо**, субектите следва да уведомяват получателите на техните услуги за конкретните [...] мерки, които тези получатели могат да предприемат за ограничаване на произтичащия за тях риск **от значителна киберзаплаха**. **Субектите следва, когато е целесъобразно и по-специално в случаите, когато може да се материализира значителна киберзаплаха, да уведомяват и получателите на техните услуги, успоредно с компетентните органи или ЕРИКС за самата заплаха.** Изискването да се уведомяват тези получатели за такива заплахи не следва да освобождава субектите от задължението да предприемат за своя сметка подходящи и незабавни мерки за предотвратяване или отстраняване на каквито и да било киберзаплахи и да възстановят нормалното ниво на сигурност на услугата. Предоставянето на получателите на такава информация относно [...] **киберзаплахи** следва да бъде безплатно.

(53) Доставчиците на обществени електронни съобщителни мрежи или на общественодостъпни електронни съобщителни услуги следва по-специално да информират получателите на услуги за конкретни и значителни киберзаплахи и за мерките, които те могат да предприемат, за да защитят сигурността на своите съобщения, например чрез използване на специални типове софтуер или технологии за криптиране.

(54) С цел да се защити сигурността на електронните съобщителни мрежи и услуги следва да се насърчи използването на криптиране, и по-специално на криптиране от край до край, като при необходимост то следва да стане задължително за доставчиците на такива услуги и мрежи в съответствие с принципите за сигурност и поверителност по подразбиране и на етапа на проектиране на целите по член 18. Използването на криптиране от край до край следва да е съобразено с правомощията на държавите членки да гарантират защитата на своите съществени свързани със сигурността интереси и обществена сигурност, а също и да дава възможност за разследване, установяване и наказателно преследване на престъпления в съответствие с правото на Съюза. Решенията по отношение на законосъобразния достъп до информация при комуникации с криптиране от край до край следва да запазват ефективността на криптирането при защитата на неприкосновеността и сигурността на комуникациите и същевременно да дават ефективен отговор на престъпността.

(55) С настоящата директива се определя двуетапен подход по отношение на докладването на инциденти с цел да се постигне подходящ баланс между бързото докладване, което подпомага ограничаването на потенциалното разпространение на инциденти и позволява на субектите да потърсят подкрепа, от една страна, и задълбоченото докладване, което подпомага извличането на ценни изводи от отделни инциденти и подобряването с течение на времето на устойчивостта на киберзаплахи на отделни дружества или цели сектори, от друга. От субектите следва да се изисква да направят първоначално уведомление в рамките на 24 часа, след като са узнали за инцидент, и да изготвят окончателен доклад в срок от един месец. В първоначалното уведомление следва да се посочва само информацията, която е строго необходима на компетентните органи и позволява на субекта да потърси подкрепа, ако е необходимо. В такова уведомление, когато е приложимо, се посочва дали се предполага, че инцидентът се дължи на незаконосъобразно или злонамерено действие. Държавите членки следва да гарантират, че изискването за подаване на такова първоначално уведомление не отклонява ресурсите на докладващия субект от дейностите по справяне с инцидента, които следва да имат приоритет. За да се гарантира още по-добре, че задълженията за докладване на инциденти нито отклоняват ресурси от дейностите по справяне с инцидента, нито затормозяват по някакъв друг начин на усилията на субекта в това отношение, държавите членки следва да предвидят разпоредба, че в надлежно обосновани случаи и при споразумение с компетентните органи или ЕРИКС съответният субект може да се отклони от 24-часовия срок за първоначалното уведомление и едномесечния срок за окончателния доклад.

(55a) Проактивният подход към киберзаплахите е жизненоважен компонент на управлението на риска за киберсигурността, който следва да даде възможност на компетентните органи ефективно да предотвратяват материализирането на киберзаплахи в действителни инциденти, които могат да причинят значителни материални или нематериални загуби. За тази цел уведомяването за значителни киберзаплахи е от ключово значение.

(56) Съществените и значимите субекти често се оказват в положение, при което, даден инцидент трябва да бъде докладван, поради конкретните му характеристики, на различни органи в резултат на задължения за уведомяване, включени в различни правни инструменти. Подобни случаи пораждат допълнителни пречки и могат да доведат и до несигурност с оглед на формата и процедурите на такива уведомления. С оглед на това и с цел опростяване на докладването за инциденти със сигурността държавите членки [...] **могат** да установят *единна входяща точка* за всички уведомления, изисквани съгласно настоящата директива, както и съгласно останалото право на Съюза, като например Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО. ENISA следва да разработи съвместно с групата за сътрудничество общи образци на уведомления посредством насоки, които биха опростили и оптимизирали изискваната съгласно правото на Съюза докладвана информация и биха намалили тежестите за дружествата.

(57) Когато съществуват подозрения, че даден инцидент е свързан с тежки престъпления — съобразно правото на Съюза или националното право, държавите членки следва да насърчават съществените и значимите субекти, на основание на приложими наказателнопроцесуални правила в съответствие с правото на Съюза, да докладват за такива инциденти на съответните правоприлагащи органи. Когато е целесъобразно и без да се засягат приложимите за Европол правила за защита на личните данни, е желателно координацията между компетентните органи и правоприлагащите органи на различни държави членки да бъде улеснявана от Европейския център за борба с киберпрестъпността (ЕС3) и ENISA.

(58) В много случаи вследствие на инциденти се засягат лични данни. В този контекст компетентните органи следва да си сътрудничат и да обменят информация относно всички съответни въпроси с органите за защита на личните данни и надзорните органи съгласно Директива 2002/58/ЕО.

(59) Поддържането на точни и пълни бази данни с имена на домейни и данни за регистрация (т. нар. „данни WHOIS“) и предоставянето на законен достъп до такива данни са от съществено значение за гарантиране на сигурността, стабилността и устойчивостта на DNS, което на свои ред допринася за по-високо ниво на киберсигурност в Съюза. Когато обработването включва лични данни, то следва да е в съответствие с правото на Съюза в областта на защитата на данните.

(60) Наличността и своевременната достъпност на тези данни за публичните органи, включително за компетентните органи съгласно правото на Съюза или националното право за предотвратяване, разследване или наказателно преследване на престъпления, CERT, ЕРИКС, и — по отношение на данните на техните клиенти — за доставчиците на електронни комуникации мрежи и услуги и на технологии и услуги в областта на киберсигурността, действащи от името на тези клиенти, са от съществено значение за предотвратяването и борбата със злоупотребите по отношение на системата за имена на домейни, по-специално за предотвратяване, разкриване и реагиране на инциденти с киберсигурността. Този достъп следва да е в съответствие с правото на Съюза за защита на личните данни, доколкото е свързан с този вид данни.

(61) За да се гарантира наличността на точни и пълни данни за регистрация на домейни, регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистриране на имена на домейни от първо ниво (т. нар. регистратори), следва да събират и гарантират целостта и наличността на данните за регистрация на имената на домейни. **По отношение на регистрационните данни субектите следва по-специално да проверят името и електронния адрес на регистранта.** [...] Регистрите на имена на домейни от първо ниво и субектите, предоставящи услуги за регистриране на имена на домейни от първо ниво, следва да установят политики и процедури за събиране и поддържане на точни и пълни данни за регистрация, както и да предотвратяват и поправят неточни такива данни в съответствие с правилата на Съюза за защита на данните.

(62) Регистрите на имена на домейни от първо ниво и субектите, предоставящи за тях услуги за регистрация на имена на домейни, следва да правят публично достъпни данните за този вид регистрация, попадащи извън обхвата на правилата на Съюза за защита на данните, като например отнасящите се до юридическите лица[25]. Регистрите на имена на домейни от първо ниво и субектите, предоставящи за тях услуги за регистрация на имена на домейни, следва да позволяват също законосъобразен достъп до конкретни данни за регистрация на имена на домейни относно физическите лица на законно търсещите достъп, в съответствие с правото на Съюза за защита на данните. Държавите членки следва да гарантират, че регистрите на имена на домейни от първо ниво и субектите, предоставящи за тях услуги за регистрация на имена на домейни, следва да отговарят незабавно на искания [...]за разкриване на данни за регистрация на имена на домейни **от законно търсещи достъп, като компетентните органи съгласно правото на Съюза или националното право в областта на националната сигурност и наказателното правосъдие или ЕРИКС.** Регистрите на имена на домейни от първо ниво и субектите, предоставящи за тях услуги за регистрация на имена на домейни, следва да установят политики и процедури за публикуването и разкриването на данни за регистрация, включително клаузи за нивото на обслужване за отговаряне на искания за достъп от законно търсещите достъп. Процедурите за достъп може да включват и използването на интерфейс, портал или друг технически инструмент за предоставяне на ефикасна система за заявяване и получаване на достъп до данни за регистрация. **Държавите членки следва да гарантират, че всички видове достъп до данни за регистрация на домейни (както лични, така и нелични) са безплатни.** С цел насърчаване на хармонизираните практики във вътрешния пазар Комисията може да приеме насоки относно такива процедури, без да се засягат правомощията на Европейския комитет по защита на данните, **в съответствие с международните стандарти, разработени от многостранната общност, и в допълнение към тях**.

---

25 Регламент (ЕС) 2016/679 **от** [...] на Европейския парламент и [...] **на** Съвета, съображение 14, съгласно което „[н]астоящият регламент не обхваща обработването на лични данни, които засягат юридически лица, и по-специално предприятия, установени като юридически лица, включително наименованието и правната форма на юридическото лице и данните за връзка на юридическото лице“.

(63) […] **С**ъществените и значимите субекти съгласно настоящата директива следва да попадат под юрисдикцията на държавата членка, в която предоставят своите услуги. **Субектите, посочени в точки 1–7 и 10 от приложение I, доставчиците на удостоверителни услуги и доставчиците на точки за обмен в интернет, посочени в точка 8 от приложение I и точки 1–5 от приложение II към настоящата директива, следва да попадат под юрисдикцията на държавата членка, в която са установени.** Ако предоставя услуги **или е установен** в повече от една държава членка, даден субект следва да попада под отделните и успоредни юрисдикции на всяка от тези държави членки. Компетентните органи на тези държави членки следва да си сътрудничат, да се подпомагат взаимно и, когато е подходящо, да провеждат съвместни действия по надзор. **Когато държавите членки решат да упражнят своята юрисдикция, те следва да избягват едно и също поведение да бъде санкционирано повече от веднъж за нарушение на задълженията, предвидени в настоящата директива.**

(64) За да се вземат предвид трансграничният характер на услугите и операциите на доставчиците на DNS услуги, регистрите на имената на домейни от първо ниво, **субектите, предоставящи услуги за регистрация на имена на домейни от първо ниво**, доставчиците на мрежи за предоставяне на съдържание, доставчиците на компютърни услуги „в облак“, доставчиците на услуги на центрове за данни и доставчици на цифрово съдържание, само една държава членка следва да има юрисдикция по отношение на тези субекти. Юрисдикцията следва да се предоставя на държавата членка, в която съответният субект има своето основно място на установяване в Съюза. Критерият за място на установяване за целите на настоящата директива предполага ефективно и действително упражняване на дейност въз основа на стабилни правила. Правната форма на тези договорености, независимо дали става въпрос за клон или дъщерно дружество с правосубектност, не е определящ фактор в това отношение.

Изпълнението на този критерий не следва да зависи от това дали съответните мрежи и информационни системи са физически разположени на определено място. Наличието и използването на тези системи не представляват сами по себе си такова основно място на установяване и следователно не са решаващ критерии за определяне на основното място на установяване. Основното място на установяване следва да бъде мястото в Съюза, където **преимуществено** се вземат решенията във връзка с мерките по управлението на риска за киберсигурността. То обикновено съответства на мястото на централното управление на дружествата в Съюза. Ако **мястото, където преимуществено се вземат решенията, не може да бъде определено или** тези решения не се вземат в Съюза, за основно място на установяване следва се считат държавите членки, в които субектът се е установил с най-голям брой служители в Съюза. Когато услугите се извършват от група предприятия, основното място на установяване на контролиращото предприятие следва да се счита за основно място на установяване на групата предприятия.

(64a) Когато рекурсивна DNS услуга се предоставя от доставчик на обществени електронни съобщителни мрежи или обществено достъпни електронни съобщителни услуги само като част от услугата за достъп до интернет, следва да се счита, че субектът попада под юрисдикцията на всички държави членки, в които се предоставят неговите услуги.

(64aa) С цел да се осигури ясен преглед на доставчиците на DNS услуги, регистрите на имената на домейни от първо ниво, субектите, предоставящи услуги за регистрация на имена на домейни от първо ниво, доставчиците на мрежи за предоставяне на съдържание, доставчиците на компютърни услуги „в облак“, доставчиците на услуги на центрове за данни и доставчици на цифрово съдържание, предоставящи услуги в Съюза в рамките на обхвата на настоящата директива, ENISA следва да създаде и поддържа регистър на тези субекти въз основа на уведомленията, получени от държавите членки, когато е приложимо, чрез техните национални механизми за самоуведомяване. С цел да се гарантира точността и пълнотата на информацията, която следва да бъде включена в този регистър, държавите членки следва да представят на ENISA информацията за тези субекти, наличната в техните национални регистри. ENISA и държавите членки следва да предприемат мерки за улесняване на оперативната съвместимост на тези регистри, като същевременно гарантират защитата на поверителната или класифицираната информация.

(65) В случаи, при които доставчик на DNS услуги, регистър на имена на домейни от първо ниво, доставчик на мрежи за предоставяне на съдържание, доставчик на компютърни услуги „в облак“, доставчик на услуги на център за данни и цифров доставчик, които не са установени в Съюза, предлагат услуги на негова територия, те следва да определят представител. За да се установи дали този субект предлага услуги в Съюза, следва да се установи дали е видно, че той възнамерява да предлага услуги на лица на територията на една или повече държави членки. Сама по себе си достъпността в Съюза на уебсайт на субект или на негов посредник или на адрес на електронна поща и други данни за контакт, или използването на език, който широко се използва в третата държава, в която е установен субектът, не е достатъчна, за да бъде потвърдено подобно намерение. Въпреки това фактори като използване на език или валута, които широко се използват в една или повече държави членки, с възможност за поръчване на услуги на този друг език, или посочването на потребители или ползватели на територията на Съюза, може да указват, че субектът възнамерява да предлага услуги в Съюза. Представителят следва да действа от името на субекта, а компетентните органи или ЕРИКС следва да имат възможност да се свържат с представителя. Представителят следва да е определен изрично чрез упълномощаване в писмена форма от доставчика да действа от негово име във връзка със задълженията му съгласно настоящата директива, включително за докладването на инциденти.

(66) Когато информация, считана за класифицирана съгласно правото на Съюза, се обменя, докладва или споделя по друг начин съгласно разпоредбите на настоящата директива, следва да се прилагат съответните конкретни правила относно предприемането на действия по нея.

(67) Предвид нарастването на сложността и професионализма на киберзаплахите качеството на мерките за разкриване и предотвратяване в голяма степен зависи от редовното споделяне между субектите на информация за заплахите и уязвимостите. Обменът на информация допринася за повишаването на осведомеността за киберзаплахите, което на свой ред подобрява капацитета на субектите да предотвратяват материализирането на заплахи в действителни инциденти и позволява на субектите по-добре да ограничават въздействието на инцидентите и да възстановяват функциите си по-ефикасно. При липсата на насоки на равнището на Съюза редица фактори изглежда са възпрепятствали такъв обмен на информация, по-специално несигурността относно съвместимостта с правилата за конкуренцията и отговорността.

(68) Субектите следва да бъдат насърчавани колективно да вложат своите лични познания и практически опит на стратегическо, тактическо и оперативно равнище с цел подобряване на способностите си за адекватен достъп, наблюдение, защита срещу и отговор на киберзаплахи. Затова е необходимо на равнището на Съюза да се даде възможност за възникването на механизми за договорености за доброволен обмен на информация. За тази цел държавите членки следва активно да подкрепят и насърчават и съответните субекти, които не попадат в обхвата на настоящата директива, да участват в тези механизми за споделяне на информация. Въпросните механизми следва да бъдат използвани в пълно съответствие с правилата за конкуренцията на Съюза, както и с правилата на Съюза за защита на данните.

(69) […] **Обработването на личните данни**, в степента, строго необходима и пропорционална за гарантиране на сигурността на мрежите и информацията от **значими и важни** субекти […] и от доставчици на технологии и услуги в областта на сигурността, **може да се счита за необходимо за спазване на правно задължение или** […] да представлява законен интерес на съответния администратор на данни **[...]**, както е посочено в Регламент (ЕС) 2016/679. Това **може** […] да включва мерки, свързани с предотвратяването, разкриването, анализирането и отговора на инциденти, мерки за повишаване на осведомеността във връзка с конкретни киберзаплахи, обмен на информация в контекста на отстраняване на уязвимостите и координирано разкриване, както и доброволния обмен на информация за тези инциденти, за киберзаплахи и уязвимости, показатели за нарушена сигурност, тактики, техники и процедури, предупреждения във връзка с киберсигурността и инструменти за конфигуриране. Тези мерки може да изискват обработването на […] **различни** видове лични данни, **като например**: IP адреси, унифицирани указатели на ресурс (URL), имена на домейни и адреси на електронна поща. **Обработването на лични данни от компетентните органи, SPOC и ЕРИКС следва да бъде установено в националното право и да се счита за необходимо за спазването на правно задължение или за изпълнението на задача от обществен интерес, или при упражняването на официални правомощия, предоставени на администратора на данни, както е посочено в член 6, параграф 1, буква в) или д) от Регламент (ЕС) 2016/679**.

(69а) В законите на държавите членки може да бъдат определени правила, които позволяват на компетентните органи, SPOC и ЕРИКС, доколкото това е строго необходимо и пропорционално за целите на гарантирането на сигурността на мрежите и информационните системи на съществените и значимите субекти, да обработват специални категории лични данни в съответствие с член 9[…] от Регламент (ЕС) 2016/679, по-специално чрез предвиждане на подходящи и конкретни мерки за гарантиране на основните права и интереси на физическите лица, включително технически ограничения за повторното използване на такива данни и използването на високотехнологични мерки за сигурност и защита на неприкосновеността на личния живот, като например псевдонимизация или криптиране, когато анонимизирането може да засегне значително постигането на поставената цел.

(70) За да се засилят правомощията и действията по надзор, подпомагащи осигуряването на ефективно изпълнение, настоящата директива следва да предостави минимален списък с действия и средства по надзор, чрез които компетентните органи **могат** […] да осъществяват надзор върху съществените и значимите субекти. Освен това с настоящата директива следва да се разграничат режимите на надзор за съществените и за значимите субекти, за да гарантира справедлив баланс на задълженията както за субектите, така и за компетентните органи. Така съществените субекти следва да са подчинени на напълно изразен режим на надзор (предхождащ и последващ), докато значимите субекти следва да са подчинени на по-лек режим, включващ само последващ надзор. Това означава, че във втория случай от значимите субекти не следва **да се изисква** […] **да документират** систематично изпълнението на изискванията за управлението на риска, свързан с киберсигурността, а компетентните органи следва да прилагат подход с последващ надзор, поради което няма да имат общо задължение за осъществяване на надзор върху тези субекти. **За значимите субекти последващият надзор може да бъде задействан от доказателства или всякакви признаци или информация, доведени до знанието на компетентните органи, по силата на които тези органи да счетат, че е налице потенциално неспазване на задълженията, предвидени в настоящата директива. Например тези доказателства, признаци или информация могат да бъдат такива, които са предоставени на компетентните органи от други органи, субекти, граждани, медии или други източници, да бъдат публично достъпна информация или да произтичат от други дейности, извършвани от компетентните органи при изпълнението на техните задачи.**

(70a) При упражняването на предварителен надзор компетентните органи следва да могат да вземат решения относно приоритизирането по пропорционален начин на използването на надзорните действия и средства, с които разполагат. Това предполага компетентните органи да могат да вземат решение за такова приоритизиране въз основа на методологии за надзор, които да следват основан на риска подход. По-конкретно, тези методологии биха могли да включват критерии или стойностни показатели за класифициране на съществените субекти в рискови категории и на съответните надзорни действия и средства, препоръчвани за всяка рискова категория, като например използване, честота или вид на проверките на място или целеви одити на сигурността, или сканирания на сигурността, вид на информацията, която трябва да се изисква, и степен на изчерпателност на тази информация. Тези надзорни методологии могат също да бъдат придружени от работни програми и да бъдат оценявани и преразглеждани редовно, включително по аспекти като разпределението на ресурсите и нуждите.

(70aa) По отношение на субектите на публичната администрация надзорните правомощия следва да се упражняват в съответствие с националните рамки и правен ред. Държавите членки следва да могат да вземат решения относно налагането на подходящи, пропорционални и ефективни мерки за надзор и правоприлагане по отношение на тези субекти.

(70aaa) За да докажат съответствието с определени мерки за управление на риска в областта на киберсигурността, държавите членки могат да изискват от съществените и значимите субекти да използват квалифицирани удостоверителни услуги или схеми за електронна идентификация, за които е извършено уведомяване, съгласно Регламент (ЕС) № 910/2014.

(71) За да се осъществи ефективното правоприлагане, следва да бъде създаден минимален списък с административни санкции за нарушение на управлението на риска, свързан с киберсигурността, и задълженията за докладване, предвидени от настоящата директива, като се установи ясна и последователна рамка за такива санкции в Съюза. Дължимо внимание следва да се обърне на естеството, тежестта и продължителността на нарушението, действително причинените вреди или понесените загуби, потенциалните вреди или загуби, преднамерения или неумишлен характер на нарушението, действията, предприети за предотвратяване или намаляване на претърпените вреди и/или загуби, степента на отговорност или евентуални относими предходни нарушения, степента на сътрудничество с компетентния орган и всякакъв друг утежняващ или смекчаващ фактор. Налагането на санкции, включително административни глоби, следва да подлежи на подходящи процедурни гаранции в съответствие с общите принципи на правото на Съюза и Хартата на основните права на Европейския съюз, включително ефективна съдебна защита и справедлив съдебен процес.

(71a) Разпоредбите, свързани с отговорността на физическите лица с определени отговорности в рамките на дадено образувание по отношение на нарушаване на задължението им да гарантират спазването на задълженията, предвидени в настоящата директива, не изискват от държавите членки да осигуряват наказателно преследване или търсенето на гражданска отговорност за вреди, причинени на трети страни в резултат на такова нарушение.

(72) За да се гарантира ефективното прилагане на предвидените съгласно настоящата директива задължения, всеки компетентен орган следва да разполага с правомощието да налага или изисква налагането на административни глоби.

(73) Когато административната глоба се налага на предприятие, понятието „предприятие“ следва да се разбира като предприятие в съответствие с членове 101 и 102 от ДФЕС за тези цели. При налагане на административни глоби на лица, които не са предприятие, надзорният орган следва да има предвид общото равнище на доход в съответната държава членка, както и икономическото състояние на лицето, за да определи подходящия размер на глобата. Държавите членки следва да определят дали и до каква степен публичните органи следва да подлежат на административни глоби. Налагането на административна глоба не засяга прилагането на други правомощия от компетентните органи или на други санкции, предвидени съгласно националните разпоредби, транспониращи настоящата директива.

(74) Държавите членки […] **могат** да определят правилата относно санкциите за нарушения на националните правила, транспониращи настоящата директива. Налагането на наказателни санкции за нарушения на тези национални правила и на свързани с това административни наказания обаче не следва да води до нарушаване на принципа *ne bis in idem* съгласно тълкуването на Съда.

(75) Когато административните наказания не са хармонизирани в настоящата директива или при необходимост в други случаи, например при сериозни нарушения на задълженията по настоящата директива, държавите членки следва да прилагат система, която предвижда ефективни, пропорционални и възпиращи санкции. Естеството на тези санкции, наказателни или административни, следва да бъде определено съгласно правото на държавата членка.

(76) За допълнително засилване на ефективността и убедителността на санкциите, приложими за нарушенията на задълженията съгласно настоящата директива, компетентните органи следва да разполагат с правомощия да прилагат санкции, състоящи се в прекратяване на удостоверение или разрешение за всички или част от услугите, предоставяни от съществен субект, и налагането на временна забрана за упражняване на управленски функции от физическо лице. Предвид тежестта и въздействието върху дейностите на субектите и в крайна сметка върху техните потребители, тези санкции следва да се прилагат само пропорционално на тежестта на нарушението и да отчитат конкретните за всеки случай обстоятелства, включително предумишлен или непредумишлен характер на нарушението, действията, предприети за предотвратяване или ограничаване на претърпените щети и/или загуби. Тези санкции следва да се прилагат единствено като ultima ratio, т.е. само след като останалите относими действия по правоприлагане, предвидени от настоящата директива, са били изчерпани, и само докато субектите, към които те се прилагат, предприемат необходимото действие за отстраняване на недостатъците или изпълнение на изискванията на компетентния орган, за които се отнасят тези санкции. Налагането на такива санкции подлежи на подходящи процедурни гаранции в съответствие с общите принципи на правото на Съюза и Хартата на основните права на Европейския съюз, включително ефективна съдебна защита, справедлив процес, презумпция за невиновност и право на защита.

(76a) За да се гарантира ефективен надзор и правоприлагане, особено в случаи с трансгранично измерение, държавите членки, които са получили искане за взаимна помощ, следва, в рамките на искането, да вземат подходящи надзорни и правоприлагащи мерки по отношение на съответния субект, който предоставя услуги или притежава мрежата и информационната система на тяхна територия.

(77) Настоящата директива следва да установи правила за сътрудничество между компетентните органи и надзорните органи в съответствие с Регламент (ЕС) 2016/679 с цел справяне със свързаните с личните данни нарушения.

(78) Настоящата директива следва да има за цел да гарантира високо равнище на отговорност при мерките за управление на риска, свързан с киберсигурността, и задълженията за докладване на равнището на организациите. Поради тези съображения управителните органи на субектите, попадащи в обхвата на настоящата директива, следва да одобряват мерките за управление на рисковете за киберсигурността и да осъществяват надзор върху тяхното изпълнение.

(79) Следва да се въведе **система за партньорско обучение** […], **за да се подпомогне укрепването на взаимното** доверие **и да се извлекат поуки от добрите практики и опит**, като се даде възможност […] за **партньорски обмен** на оценки от експерти, определени от държавите членки, във връзка с […] изпълнението на политиките в областта на киберсигурността. **При прилагането на системата за партньорско обучение следва да се обърне специално внимание на това да се гарантира, че тя не създава ненужна или непропорционална тежест за съответните органи на държавите членки. Комисията следва да проучи всички възможности за потенциалното гарантиране на финансовото покритие на разходите, които могат да възникнат в резултат на организирането на мисии за партньорско обучение. Освен това системата за партньорско обучение следва да отчита резултатите от подобни механизми, като например системата за партньорски проверки на мрежата на ЕРИКС, да добавя стойност и да избягва дублирането. Прилагането на системата за партньорско обучение следва да не засяга националните закони или законодателството на Съюза в областта на защитата на поверителната и класифицираната информация. Преди началото на кръговете за партньорско обучение държавите членки могат да извършват самооценка на съответните аспекти. По искане на Групата за сътрудничество ENISA може да предостави насоки относно самооценката и съответните образци, ако е необходимо. Държавите членки могат да решат да направят своите доклади публично достояние.**

(80) [...]

(81) За да се осигурят еднакви условия за прилагането на относимите разпоредби на настоящата директива във връзка с процедурните правила, необходими за функционирането на групата за сътрудничество, техническите елементи, свързани с мерките за управление на риска или вида на информацията, формата и процедурата за уведомяване за инциденти, **категориите субекти, от които да се изисква използването на определени ИКТ продукти, услуги и процеси**, на Комисията следва да бъдат предоставени изпълнителни правомощия. Тези правомощия следва да бъдат упражнявани в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета[26].

(82) Комисията следва периодично да извършва преглед на настоящата директива, като се консултира със заинтересованите страни, по-специално с цел установяване на необходимостта от изменения предвид промените в обществените, политически, технологични или пазарни условия.

[26] Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета от 16 февруари 2011 г. за установяване на общите правила и принципи относно реда и условията за контрол от страна на държавите членки върху упражняването на изпълнителните правомощия от страна на Комисията (ОВ L 55, 28.2.2011 г., стр. 13).

(83) Тъй като целта на настоящата директива, а именно постигане на високо общо ниво на киберсигурност в Съюза, не може да бъде постигната в достатъчна степен от държавите членки, а поради последиците от действието може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приеме мерки в съответствие с принципа на субсидиарност, уреден в член 5 от Договора за Европейски съюз. В съответствие с принципа на пропорционалност, уреден в същия член, настоящата директива не надхвърля необходимото за постигане на тази цел.

(84) Настоящата директива зачита основните права и спазва принципите, признати в Хартата на основните права на Европейския съюз, и по-специално правото на зачитане на личния живот и тайната на съобщенията, защитата на личните данни, свободата на стопанската инициатива, правото на собственост, правото на ефективни правни средства за защита и правото на изслушване. Настоящата директива следва да бъде прилагана в съответствие с посочените права и принципи,

ПРИЕХА НАСТОЯЩАТА ДИРЕКТИВА:

ГЛАВА I

Общи разпоредби

Член 1

Предмет

1. С настоящата директива се установяват мерки с цел осигуряване на високо общо ниво на киберсигурност в Съюза, **така че да се подобри функционирането на вътрешния пазар**.

2. За тази цел с настоящата директива:

   а) се установяват задължения за държавите членки да приемат национални стратегии за киберсигурност, да определят компетентни национални органи, единни звена за контакт и екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС);

   б) се установяват задължения за управление на риска, свързан с киберсигурността, и за докладване за субекти от вида, посочен в [...] приложени**я I и II**[...];

   в) се установяват **правила и** задължения относно обмена на информация за киберсигурността.

Член 2

Обхват

1. Настоящата директива се прилага за публичноправните и частноправните субекти от видовете, **посочени** [...] в [...] приложени**я I и II** [...], **които отговарят на таваните за средни предприятия** [...] по смисъла на Препоръка 2003/361/ЕО на Комисията[27] **или ги надвишават**. **Член 3, параграф 4 и член 6, параграф 2, втора и трета алинея от приложението към посочената препоръка не се прилагат за целите на настоящата директива.**

2. [...]**Н**езависимо от[...] размера **на субектите, посочени в параграф 1**, настоящата директива се прилага също и **когато:** [...]

   а) услугите са предоставяни от някой от следните субекти:

      (i) доставчици на обществени електронни съобщителни мрежи или общественодостъпни електронни съобщителни услуги, посочени в точка 8 от приложение I;

      (ii) доставчици на квалифицирани удостоверителни услуги, посочени в точка XX от приложение I;

      iii) доставчици на неквалифицирани удостоверителни услуги, посочени в точка XX от приложение I;

      iv) регистри на имена на домейни от първо ниво, [...] посочени в точка 8 от приложение I;

   б) [...]

[27] Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. относно определението за микро-, малки и средни предприятия (ОВ L 124, 20.5.2003 г., стр. 36).

в) субектът е единствен доставчик **в дадена държава членка** на услуга[...]**, която е от съществено значение за поддържането на обществените и икономическите дейности от основно значение**;

г) потенциално смущение на предоставяната от субекта услуга би могло да окаже [...] **значително** въздействие върху обществената безопасност, обществената сигурност или общественото здраве;

д) потенциално смущение на предоставяната от субекта услуга би могло да предизвика [...] **значителни** системни рискове, по-специално за секторите, в които такова нарушаване би могло да има трансгранично въздействие;

е) [...];

ж) субектът е определен като критичен съгласно Директива (ЕС) XXXX/XXXX на Европейския парламент и на Съвета[28] [Директива относно устойчивостта на критичните субекти] **[**или като равностоен на критичен съгласно член 7 от същата директива**]**.

2а. **Независимо от техния размер, настоящата директива се прилага и за субекти на публичната администрация на централни правителства, признати като такива в държава членка в съответствие с националното право и посочени в точка 9 от приложение I. Държавите членки могат да предвидят настоящата директива да се прилага и за субекти на публичната администрация на регионално и местно равнище.**

28 [да се добавят пълното заглавие и препратка към публикацията в ОВ, когато станат известни].

3. [...]

Настоящата директива не засяга отговорностите на държавите членки да опазят националната сигурност или правомощието им да гарантират други основни функции на държавата, включително да осигуряват нейната териториална цялост и да поддържат законността и реда.

3а. (1) Настоящата директива не се прилага по отношение на:

а) субекти, които попадат извън обхвата на правото на Съюза, и във всички случаи по отношение на всички субекти, които основно извършват дейности в областта на отбраната, националната сигурност, обществената сигурност или правоприлагането, независимо от това кой субект извършва тези дейности и дали той е публичен или частен субект, без да се засяга параграф 2;

б) субекти, които извършват дейности в областта на съдебната власт, парламентите или централните банки.[...]

(2) Когато субектите на публичната администрация извършват дейности в тези области само като част от цялостната си дейност, те се изключват изцяло от обхвата на настоящата директива.

3аа. Настоящата директива не се прилага по отношение на:

i) дейности на субекти, които попадат извън обхвата на правото на Съюза, и във всички случаи не по отношение на дейностите, които се отнасят до националната сигурност или отбраната, независимо от това кой субект ги извършва и дали той е публичен или частен субект;

ii) дейности на органите на съдебната власт, парламентите, централните банки и в областта на обществената сигурност, включително органите на публичната администрация, извършващи дейности по правоприлагане за целите на предотвратяването, разследването, разкриването или наказателното преследване на престъпления или изпълнението на наказателни санкции.

3ааа. Задълженията, предвидени в настоящата директива, не водят до предоставянето на информация, разкриването на която противоречи на основните интереси на държавите членки, свързани с националната сигурност, обществената сигурност или отбраната.

3аааа.Настоящата директива не засяга правото на Съюза относно защитата на личните данни, по-специално Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО.

3б. Настоящата директива не се прилага за субекти, които са освободени от Регламент (ЕС) XXXX/XXXX на Европейския парламент и на Съвета [Регламента DORA] в съответствие с член 2, параграф 4 от Регламента DORA.

4. Настоящата директива се прилага, без да се засягат [...][29] [...] Директиви 2011/93/ЕС[30] и 2013/40/ЕС[31] на Европейския парламент и на Съвета.

5. Без да се засяга член 346 от ДФЕС, информация, която е поверителна съгласно правилата на Съюза и националните правила, например правилата за търговската тайна, се обменя с Комисията и други съответни органи **съгласно настоящата директива** само когато този обмен е необходим за прилагането на настоящата директива. Обменяната информация се ограничава до информацията, която има значение за целите на този обмен и която е пропорционална на тези цели. При обмена на информация се запазва поверителността на информацията, както и сигурността и търговските интереси на съществените и значимите субекти.

---

29 [...]

30 Директива 2011/93/ЕС на Европейския парламент и на Съвета от 13 декември 2011 г. относно борбата със сексуалното насилие и със сексуалната експлоатация на деца, както и с детската порнография и за замяна на Рамково решение 2004/68/ПВР на Съвета (ОВ L 335, 17.12.2011 г., стр. 1).

31 Директива 2013/40/ЕС на Европейския парламент и на Съвета от 12 август 2013 г. относно атаките срещу информационните системи и за замяна на Рамково решение 2005/222/ПВР на Съвета (ОВ L 218, 14.8.2013 г., стр. 8).

Член 2а

Съществени и значими субекти

1. Следните субекти, за които се прилага настоящата директива, се считат за съществени:

i) субекти от видовете, предвидени в точки 1—8а и 10 от приложение I към настоящата директива, които надвишават таваните за средни предприятия, определени в Препоръка 2003/361/ЕО на Комисията;

ii) средни предприятия, посочени в член 2, параграф 2, буква а), подточка i);

iii) субекти, посочени в член 2, параграф 2, буква а), подточки ii) и iv) от настоящата директива, независимо от размера;

iv) субекти, посочени в член 2, параграф 2, буква ж) и член 2, параграф 2а от настоящата директива, независимо от размера;

v) ако е предвидено от държавите членки, субекти, които държавите членки са определили преди влизането в сила на настоящата директива като оператори на основни услуги в съответствие с Директива (ЕС) 2016/1148 или националното право;

vi) субекти, които надвишават таваните за средни предприятия съгласно определението в Препоръка 2003/361/ЕО на Комисията от вида, предвиден в приложение II, за които държавите членки определят, че са от съществено значение въз основа на критериите, посочени в член 2, параграф 2, букви в)—д);

vii) средни предприятия по смисъла на Препоръка 2003/361/ЕО на Комисията, за които държавите членки определят, че са от съществено значение въз основа на критериите, посочени в член 2, параграф 2, букви в)—д);

viii) микро- или малки предприятия по смисъла на Препоръка 2003/361/ЕО на Комисията, предвидени в параграф 2, буква а), подточка i) или идентифицирани съгласно параграф 2, букви в)—д) от настоящия член, за които държавите членки определят, че са от съществено значение въз основа на националните оценки на риска.

2. Следните субекти, за които се прилага настоящата директива, се считат за съществени:

i) субекти от видовете, предвидени в приложение I към настоящата директива, които се определят като средни предприятия по смисъла на Препоръка 2003/361/ЕО на Комисията, и субекти от вида, предвиден в приложение II, които отговарят на таваните за средни предприятия по смисъла на Препоръка 2003/361/ЕО на Комисията[32] или ги надвишават;

ii) субекти, посочени в член 2, параграф 2, подточка iii) от настоящата директива, независимо от размера;

iii) малки и средни предприятия, посочени в член 2, параграф 2, буква а), подточка i);

iv) малки и микросубекти, за които държавите членки определят, че са важни субекти въз основа на член 2, параграф 2, букви в)—д).

---

32 **Препоръка 2003/361/ЕО на Комисията от 6 май 2003 г. относно определението за микро-, малки и средни предприятия (ОВ L 124, 20.5.2003 г., стр. 36).**

Член 2а

Механизми за уведомяване

1. **Държавите членки могат да установят национален механизъм за самоуведомяване, което изисква от всички субекти от обхвата но настоящата директива да представят най-малко своето наименование, адрес, данни за контакт, сектора, в който развиват дейност, или вида услуга, която предоставят, и, когато е приложимо, списъка на държавите членки, в които предоставят услуги в съответствие с условията по настоящата директива, на компетентните органи съгласно настоящата директива или органите, определени за тази цел от държавите членки.**

2. Държавите членки [...] представят на Комисията **по отношение на субектите, които са идентифицирали съгласно член 2, параграф 2, букви б)—д), най-малко следната информация относно номера на идентифицираните субекти, сектора, към който те се числят, или вида услуга, която те предоставят съгласно приложенията, и конкретната(ите) разпоредба(и) на член 2, параграф 2, въз основа на която(които) те са били идентифицирани до [12 месеца след срока за транспонирането на настоящата директива].** Държавите членки извършват редовен преглед на [...] **тази информация**[...] и поне на всеки две години след това и когато е подходящо я актуализират.

Член 2б

Специфични секторни законодателни актове на Съюза

1. Когато [...] **специфични секторни законодателни актове на Съюза** изискват съществените или значимите субекти да приемат мерки за управление на риска, свързан с киберсигурността, или да уведомяват за **значителни** инциденти или [...] киберзаплахи, и когато тези изисквания имат поне равностоен ефект на предвидените в настоящата директива задължения, съответните разпоредби на настоящата директива, **включително разпоредбите относно надзора и правоприлагането, предвидени в глава VI,** не се прилагат за **такива субекти**. **Ако специфични секторни законодателни актове на Съюза не обхващат всички субекти в конкретен сектор, попадащ в обхвата на настоящата директива, съответните разпоредби на настоящата директива продължават да се прилагат по отношение на субектите, които не са обхванати от тези специфични за сектора разпоредби.**

2. Изискванията, посочени в параграф 1 от настоящия член, се считат за равностойни по сила на задълженията, установени в настоящата директива, ако съответният специфичен секторен законодателен акт на Съюза предвижда незабавен достъп, когато е целесъобразно — автоматичен и пряк, до уведомленията за инциденти от компетентните органи съгласно настоящата директива или от определените ЕРИКС и ако:

а) мерките за управление на риска, свързан с киберсигурността, са най-малкото равностойни по сила на мерките, определени в член 18, параграфи 1 и 2 от настоящата директива; или

б) изискванията за уведомяване за значителни инциденти са най-малко равностойни по сила на изискванията, определени в член 20, параграфи 1—6.

3. Комисията периодично прави преглед на прилагането на изискванията за равностоен ефект, предвидени в параграфи 1 и 2 от настоящия член във връзка със специфичните за отделните сектори разпоредби на правните актове на Съюза. Комисията се консултира с групата за сътрудничество и ENISA при подготовката на тези периодични прегледи.

Член 3

Минимална хармонизация

Без да се засягат техните други задължения съгласно правото на Съюза, държавите членки могат[...] да приемат или поддържат разпоредби, осигуряващи по-високо ниво на киберсигурност **в областите, обхванати от настоящата директива**.

Член 4

Определения

За целите на настоящата директива се прилагат следните определения:

(1) „мрежа и информационна система“ означава:

а) електронна съобщителна мрежа по смисъла на член 2, параграф 1 от Директива (ЕС) 2018/1972;

б) всяко устройство или всяка група взаимосвързани или имащи връзка помежду си устройства, едно или няколко от които по програма обработват автоматично цифрови данни;

в) цифрови данни, съхранявани, обработвани, извличани или пренасяни от елементи, обхванати от букви а) и б), с цел обработване, използване, защита и поддръжка;

(2) „сигурност на мрежите и информационните системи“ означава способността на мрежите и информационните системи да издържат — при дадено равнище на увереност — на **събития**, които **могат** да засегнат**[...]** отрицателно наличието, истинността, целостта или поверителността на съхранявани, пренасяни или обработвани данни или **на** свързаните с тях услуги, предлагани от тези мрежи и информационни системи или достъпни чрез тях;

(2a) „електронна съобщителна мрежа“ означава електронна[...] съобщителна мрежа по смисъла на член 2, параграф 4 от Директива (ЕС) 2018/1972;

(3) „киберсигурност“ означава киберсигурност по смисъла на член 2, параграф 1 от Регламент (ЕС) 2019/881 на Европейския парламент и на Съвета[33];

(4) „национална стратегия за **киберсигурност**“ [...] означава съгласувана рамка на държава членка, съдържаща насоки за постигането на стратегически цели и приоритети **в областта на** [...]**киберсигурността** [...] в тази държава членка;

(5) „инцидент“ означава всяко събитие, компрометиращо наличието, автентичността, целостта или поверителността на съхранявани, предавани или обработвани данни или на [...] услуги, предлагани или направени достъпни чрез мрежи и информационни системи;

(5a) „мащабен киберинцидент“ означава инцидент със значително въздействие върху поне две държави членки, или при който причиненото смущение надхвърля капацитета на дадена държава членка да реагира.

---

33 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).

(6) „действия при инцидент“ означава всички действия и процедури, имащи за цел установяването, анализа, ограничаването и реагирането на инцидент;

(6a) „риск“ се отнася до потенциала за възникване на загуба или смущение в резултат на инцидент и се изразява като комбинация от мащаба на загубата или смущението и вероятността за настъпване на посочения инцидент.

(7) „киберзаплаха“ означава киберзаплаха по смисъла на член 2, точка 8 от Регламент (ЕС) 2019/881;

(7а) **„значителна киберзаплаха“ означава киберзаплаха, за която въз основа на техническите ѝ характеристики може да се предположи, че има потенциал да окаже сериозно въздействие върху мрежата и информационните системи на даден субект или неговите ползватели, като причини значителни материални или нематериални загуби;**

(8) „уязвимост“ означава слабост, предразположеност или недостатък на ИКТ актив или система[...], които могат да бъдат използвани при киберзаплаха;

(8a) „ситуации, близки до инцидент“ означава събитие, което потенциално е можело да причини вреда на мрежата и информационните системи на даден субект или на потребителите, но неговото пълно проявяване е било успешно предотвратено;

(9) „представител“ означава всяко установено в Съюза физическо или юридическо лице, изрично определено да действа от името на i) доставчик на DNS услуги, регистър на имената на домейни от първо ниво (TLD), доставчик на компютърни услуги „в облак“, доставчик на услуги на център за данни, доставчик на мрежи за предоставяне на съдържание съгласно посоченото в точка 8 от приложение I или ii) субекти, неустановени в Съюза, които са посочени в точка [...] **6** от приложение II и към които, по отношение на задълженията на даден субект съгласно настоящата директива, национален компетентен орган или ЕРИКС може да се обръща вместо към самия субект;

(10) „стандарт“ означава стандарт по смисъла на член 2, параграф 1 от Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета[34];

(11) „техническа спецификация“ означава техническа спецификация по смисъла на член 2, параграф 4 от Регламент (ЕС) № 1025/2012;

(12) „точка за обмен в интернет (ТОИ)“ означава мрежово съоръжение, което дава възможност за свързване на повече от две независими мрежи (автономни системи), преди всичко с цел улесняване на обмена на интернет трафик; чрез ТОИ се осъществява свързване само на автономни системи; свързването чрез ТОИ не изисква интернет трафикът, преминаващ между които и да е две участващи автономни системи, да преминава през трета автономна система, нито изменя или засяга този трафик по друг начин;

(13) „система за имена на домейни (DNS)“ означава йерархична разпределена система за именуване на домейни, позволяваща на крайните потребители да достигат до услугите и ресурсите в интернет;

(14) „доставчик на DNS услуги“ означава субект, който предоставя рекурсивни или окончателни услуги по преобразуване на имена на домейни **за** [...] **използване от трета страна, с изключение на коренови сървъри за имена** [...];

---

34 Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета от 25 октомври 2012 г. относно европейската стандартизация, за изменение на директиви 89/686/ЕИО и 93/15/ЕИО на Съвета и на директиви 94/9/ЕО, 94/25/ЕО, 95/16/ЕО, 97/23/ЕО, 98/34/ЕО, 2004/22/ЕО, 2007/23/ЕО, 2009/23/ЕО и 2009/105/ЕО на Европейския парламент и на Съвета и за отмяна на Решение 87/95/ЕИО на Съвета и на Решение № 1673/2006/ЕО на Европейския парламент и на Съвета (ОВ L 316, 14.11.2012 г., стр. 12).

(15) „регистър на имена на домейни от първо ниво“ означава субект, на който е поверен конкретен домейн от първо ниво и който е отговорен за администрирането на този домейн, включително за регистрацията на имена на домейни на нива под домейна от първо ниво и техническото функциониране на домейна от първо ниво, включително функционирането на неговите сървъри за имена, поддръжката на неговите бази данни и разпределението на файловете на зоните на домейна от първо ниво в сървърите за имена, **като се изключат ситуациите, при които имената на домейни от първо ниво се използват от регистър единствено за собствена употреба**;

(15a) „субекти, предоставящи услуги за регистриране на имена на домейни от първо ниво“ означава регистри на имена на домейни от първо ниво, регистратори на домейни от първо ниво и представители на регистратори като препродавачи и доставчици на прокси услуги;

(16) „цифрова услуга“ означава услуга по смисъла на член 1, параграф 1, буква б) от Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета[35];

(16a) „удостоверителни услуги“ означава удостоверителни услуги по смисъла на член 3, точка 16 от Регламент (ЕС) № 910/2014;

[35] Директива (ЕС) 2015/1535 на Европейския парламент и на Съвета от 9 септември 2015 г., установяваща процедура за предоставянето на информация в сферата на техническите регламенти и правила относно услугите на информационното общество (ОВ L 241, 17.9.2015 г., стр. 1).

(16б) „доставчик на квалифицирани удостоверителни услуги“ означава доставчик на квалифицирани удостоверителни услуги по смисъла на член 3, точка 20 от Регламент (ЕС) № 910/2014;

(17) „онлайн място за търговия“ означава цифрова услуга по смисъла на член 2 буква н) от Директива 2005/29/ЕО на Европейския парламент и на Съвета[36];

(18) „онлайн търсачка“ означава цифрова услуга по смисъла на член 2, параграф 5 от Регламент (ЕС) 2019/1150 на Европейския парламент и на Съвета[37];

(19) „компютърна услуга „в облак“ означава цифрова услуга, която дава възможност за администриране при поискване и широк отдалечен достъп до променлив по мащаб и еластичен набор от [...] компютърни ресурси, които могат да бъдат ползвани съвместно**, включително когато те са разпределени на няколко места**;

(20) „услуга на център за данни“ означава услуга, включваща конструкции или групи конструкции, предназначени за централизирано разполагане, свързване и експлоатация на информационно и мрежово технологично оборудване, предоставящо услуги за съхранение, обработване и пренос на данни, заедно с всички съоръжения и инфраструктури за електроразпределение и контрол на околната среда;

---

36 Директива 2005/29/ЕО на Европейския парламент и на Съвета от 11 май 2005 г. относно нелоялни търговски практики от страна на търговци към потребители на вътрешния пазар и изменение на Директива 84/450/ЕИО на Съвета, Директиви 97/7/ЕО, 98/27/ЕО и 2002/65/ЕО на Европейския парламент и на Съвета, и Регламент (ЕО) № 2006/2004 на Европейския парламент и на Съвета („Директива за нелоялни търговски практики“) (ОВ L 149, 11.6.2005 г., стр. 22).

37 Регламент (ЕС) 2019/1150 на Европейския парламент и на Съвета от 20 юни 2019 г. за насърчаване на справедливост и прозрачност за бизнес ползвателите на посреднически онлайн услуги (ОВ L 186, 11.7.2019 г., стр. 57).

(21) „мрежа за доставяне на съдържание“ означава мрежа от географски разпределени сървъри, с цел да се осигури висока степен на наличност, достъпност или бързо доставяне на цифрово съдържание и услуги на интернет потребителите от страна на доставчиците на съдържание и услуги;

(22) „платформа на услуги за социална мрежа“ означава платформа, позволяваща на крайните потребители да се свързват, споделят, откриват и общуват помежду си посредством множество устройства, и по-специално, чрез чатове, публикации, видеоклипове и препоръки[...];

(23) „орган на публичната администрация“ означава орган, който е **признат като такъв в държава членка в съответствие с националното право**, [...] който отговаря на следните критерии:

а) създаден е с цел да задоволява нужди от общ интерес и няма промишлен или търговски характер;

б) притежава правосубектност **или е оправомощен от закона да действа от името на друг субект с правосубектност**;

в) финансира се основно от държавата, регионален орган или други публичноправни организации; или е обект на управленски надзор от страна на тези органи или организации; или има административен, управителен или надзорен съвет, повечето от половината от членовете на който са назначени от държавните, регионалните органи или от други публичноправни организации;

г) има правомощието да налага на физически или юридически лица административни или регулаторни решения, засягащи техните права в трансграничното движение на хора, стоки, услуги или капитали.

(24) „субект“ означава всяко физическо или юридическо лице, създадено и признато за такова съгласно националното право в своето място на установяване, което може, като действа от свое име, да упражнява права и да бъде обект на задължения;

(25) „съществен субект“ означава всеки субект от вид [...]**, посочен в приложение I и определен като „съществен“ в съответствие с член 2а, параграф 1**;

(26) „значим субект“ означава всеки субект от вид [...]**, посочен в приложения I и II и определен като „значим“ в съответствие с член 2а, параграф 2**.

(26а) „ИКТ продукт“ означава ИКТ продукт по смисъла на член 2, точка 12 от Регламент (ЕС) № 2019/881;

(26аа) „ИКТ услуга“ означава ИКТ услуга по смисъла на член 2, точка 13 от Регламент (ЕС) 2019/881;

(26аб) „ИКТ процедура“ означава ИКТ процедура по смисъла на член 2, точка 14 от Регламент (ЕС) 2019/881;

(26ав) „доставчик на управлявани услуги“ означава всеки субект, който доставя услуги, например мрежа, приложение, инфраструктура и сигурност, чрез текущо и редовно управление, подпомагане и активно администриране в помещенията на клиентите, в центъра за данни на техния доставчик на управлявани услуги (хостинг), или в център за данни в трета страна.

(26аг) „доставчик на услуги по управление на сигурността“ означава всеки субект, който предоставя наблюдение и управление на устройства и системи за сигурност, възложени на външни изпълнители. Общите услуги включват управлявана защитна стена, откриване на проникване, виртуална частна мрежа, сканиране за уязвимости и противовирусни услуги.

Това включва и използването на оперативни центрове за сигурност с висока степен на достъпност (от собствените им съоръжения или от други доставчици на центрове за данни) за предоставяне на услуги 24 часа в денонощието, 7 дни в седмицата, предназначени да намалят броя на оперативния персонал по сигурността, който предприятието трябва да наеме, да обучи и да задържи, за да поддържа приемливо състояние на киберсигурността.

ГЛАВА II

Координирани регулаторни рамки в областта на киберсигурността

Член 5

Национална стратегия за киберсигурност

1. Всяка държава членка приема национална стратегия за киберсигурност, в която са определени стратегическите цели и подходящи мерки на политиката, както и подходящи регулаторни мерки за постигане и поддържане на високо ниво на киберсигурност. Националната стратегия за киберсигурност включва по-специално следното:

   а) [...] целите и приоритетите на стратегията на държавата членка относно киберсигурността;

   б) управленска рамка за постигане на тези цели и приоритети, включително посочените в параграф 2 политики и ролите и отговорностите на различните органи и заинтересовани лица, участващи в изпълнението на стратегията [...];

   в) [...] **насоки** за установяване на относимите активи и **оценка на** рискове за киберсигурността в съответната държава членка[…]

   г) набелязване на мерките, гарантиращи подготвеността, реагирането и възстановяването при инциденти, включително сътрудничеството между публичния и частния сектор;

   д) [...]

е) рамка на политиките за подобрена координация между компетентните органи съгласно настоящата директива и Директива (ЕС) XXXX/XXXX на Европейския парламент и на Съвета[38] [Директива относно устойчивостта на критичните субекти] с цел обмен на информация относно **рискове за киберсигурността**, [...] киберзаплахи и **инциденти, както и относно несвързани с киберсигурността рискове, заплахи и инциденти** и упражняването на задачи по надзор, **по целесъобразност**;

еа) рамка на политиките за координация и сътрудничество между компетентните органи съгласно настоящата директива и компетентните органи, определени съгласно специфичното за сектора законодателство.

2. Като част от националната стратегия за киберсигурност държавите членки по-специално приемат следните политики:

а) политика за разрешаване на въпросите с киберсигурността по веригата за доставки на ИКТ продукти и услуги, използвана от [...] субектите за предоставянето на техните услуги;

б) **политика** [...] относно включването и посочването на свързани с киберсигурността изисквания за ИКТ продуктите и услугите при възлагането на обществени поръчки, **включително сертифициране на киберсигурността**;

в) политика **за управление на уязвимости, включваща насърчаване и улесняване на доброволното** координирано оповестяване на уязвимости по смисъла на член 6, **параграф 1**;

г) политика, свързана с поддържането на общата наличност, [...] цялост **и поверителност** на общественото ядро на отворения интернет;

д) политика за насърчаване и развитие на **образование, обучение и** умения в областта на киберсигурността, повишаване на осведомеността и инициативи за научноизследователска и развойна дейност;

---

38 [*да се добавят пълното заглавие и препратка към публикацията в ОВ, когато станат известни]*

е) политика за подпомагане на академичните и научноизследователските институции за разработване на инструменти за киберсигурност и сигурна мрежова инфраструктура;

ж) политика, съответни процедури и подходящи инструменти за обмен на информация, подпомагащи доброволния обмен на информация за киберсигурността между дружествата в изпълнение на правото на Съюза;

з) политика, намираща решения за специфичните нужди на малките и средните предприятия, по-специално на изключените от обхвата на настоящата директива, във връзка с насоки и подкрепа за подобряване на тяхната устойчивост на киберзаплахи [...].

3. Държавите членки уведомяват Комисията за своите национални стратегии за киберсигурност в рамките на три месеца от приемането им. **При това** държавите членки могат да изключат **някои елементи на стратегията, свързани с** [...] националната сигурност.

4. Държавите членки извършват оценка на своите национални стратегии за киберсигурност редовно и поне на всеки [...] **пет** години въз основа на ключови показатели за ефективност и при необходимост внасят изменения в тях. По искане на държавите членки Агенцията на Европейския съюз за киберсигурност (ENISA) ги подпомага при разработването на национална стратегия и на ключови показатели за ефективност за оценката на стратегията.

Член 6

Координирано оповестяване на уязвимости и Европейски регистър на уязвимостите

1. Всяка държава членка определя един от своите екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС) съгласно посоченото в член 9 като координатор за целите на координираното оповестяване на уязвимости. Определеният ЕРИКС действа като доверен посредник, улесняващ при необходимост взаимодействието между докладващия субект**, отговорника за противодействие на потенциалните уязвимости** и производителя или доставчика на ИКТ продукти или услуги. **Всяко физическо или юридическо лице може да докладва, евентуално анонимно, за уязвимост, посочена в член 4, параграф 8, на определения ЕРИКС. Определеният ЕРИКС гарантира предприемането на надлежни последващи действия във връзка с докладваната информация и поверителността на самоличността на лицето, което докладва за уязвимостта.** Когато докладваната уязвимост [...] **би могла потенциално да окаже значително въздействие върху субекти в повече от една държава членка**, определеният ЕРИКС на всяка засегната държава членка си сътрудничи **с други определени ЕРИКС в рамките на** мрежата на ЕРИКС, **когато е целесъобразно**.

2. ENISA разработва и поддържа Европейски регистър на уязвимостите**, в консултация с групата за сътрудничество**. За тази цел ENISA създава и поддържа подходящите информационни системи, политики и процедури, по-специално за да даде възможност на значимите и съществените субекти и техните доставчици на мрежи и информационни системи **доброволно** да оповестяват и регистрират **публично известни** уязвимости, налични в ИКТ продукти или услуги, както и да предоставят достъп до съдържащата се в регистъра информация на всички заинтересовани страни. Регистърът по-специално включва описваща уязвимостта информация, засегнатите ИКТ продукти или услуги и тежестта на уязвимостта с оглед на обстоятелствата, при които тя може да бъде използвана злонамерено, наличието на съответни корекции и, ако такива липсват – насоки **от националните компетентни органи или ЕРИКС** за потребителите на уязвимите продукти и услуги как да бъде ограничен рискът, произтичащ от оповестените уязвимости. **ENISA гарантира, че Европейският регистър на уязвимостите използва сигурна и устойчива комуникационна и информационна инфраструктура.**

Член 7

Национални рамки за управление на кризи в областта на киберсигурността

1. Всяка държава членка определя един или повече компетентни органи, отговарящи за управлението на мащабните инциденти и кризи в областта на **киберсигурността**. Държавите членки гарантират, че компетентните органи разполагат с адекватни ресурси за изпълнение на възложените им задачи по ефективен и ефикасен начин. **Държавите членки гарантират съгласуваност със съществуващите рамки за общо управление на кризи.**

2. Всяка държава членка набелязва способности, активи и процедури, които могат да бъдат разгърнати в случай на криза за целите на настоящата директива.

3. Всяка държава членка приема национален план за реакция при инциденти и кризи в областта на киберсигурността, в който се предвиждат целите и условията и редът за управлението на мащабни инциденти и кризи в областта на киберсигурността. Планът обхваща по-специално следното:

   а) цели на националните мерки и дейности за подготвеност;

   б) задачи и отговорности на националните компетентни органи;

   в) процедури за управление на кризи в областта на киберсигурността**, включително тяхното интегриране в общата национална рамка за управление на кризи** и канали за обмен на информация;

   г) мерки за подготвеност, включително редовни дейности по учения и обучения;

   д) съответните публичноправни и частноправни [...] страни и засегнатата инфраструктура;

   е) национални процедури и договорености между съответните национални органи и служби за осигуряване на ефективно участие и подкрепа от страна на държавата членка за координираното управление на мащабни инциденти и кризи в областта на киберсигурността на равнището на Съюза.

4. Държавите членки [...] **информират** Комисията **за** определянето на своите компетентни органи, посочени в параграф 1, и представят **съответната информация, свързана с изискванията по параграф 3 от настоящия член, за** своите национални планове за реакция при инциденти и кризи в областта на киберсигурността [...] в рамките на три месеца от определянето и приемането на тези планове. Държавите членки може да изключат конкретна информация [...], когато и доколкото това е [...] необходимо за тяхната национална сигурност, **обществения ред или отбраната**.

Член 8

Национални компетентни органи и единни звена за контакт

1. Всяка държава членка определя един или повече компетентни органи, отговарящи за киберсигурността и за задачите по надзор, посочени в глава VI от настоящата директива. Държавите членки могат да определят за тази цел вече съществуващ орган или органи.

2. Компетентните органи, посочени в параграф 1, наблюдават прилагането на настоящата директива на национално равнище.

3. Всяка държава членка определя едно национално единно звено за контакт в областта на киберсигурността („единно звено за контакт“). Когато държава членка определи само един компетентен орган, този компетентен орган изпълнява функцията и на единно звено за контакт за тази държава членка.

4. Всяко единно звено за контакт изпълнява функцията на свръзка, за да гарантира трансграничното сътрудничество на органите на своята държава членка със съответните органи в други държави членки, както и за да осигури междусекторно сътрудничество с други национални компетентни органи в рамките на своята държава членка.

5. Държавите членки гарантират, че компетентните органи, посочени в параграф 1, и единните звена за контакт разполагат с достатъчно ресурси, за да изпълняват ефективно и ефикасно възложените им задачи и по този начин да постигат целите на настоящата директива. Държавите членки осигуряват ефективно, ефикасно и сигурно сътрудничество на определените представители в групата за сътрудничество, посочена в член 12.

6. Всяка държава членка уведомява Комисията без излишно забавяне за определянето на компетентния орган по параграф 1 и на единното звено за контакт по параграф 3, за техните задачи и за евентуални последващи промени в тях. Всяка държава членка оповестява публично своето определяне. Комисията публикува списъка на определените единни звена за контакт.

Член 9

Екипи за реагиране при инциденти с компютърната сигурност (ЕРИКС)

1. Всяка държава членка определя един или повече ЕРИКС, отговарящи на изискванията, посочени в член 10, параграф 1, които обхващат най-малко секторите, подсекторите или субектите, посочени в приложения I и II, които отговарят за предприемането на действия при инциденти в съответствие с подробно определена процедура. ЕРИКС може да бъде създаден в рамките на компетентен орган, посочен в член 8.

2. Държавите членки гарантират, че всеки ЕРИКС разполага с достатъчни ресурси, за да изпълнява ефективно задачите си, установени в член 10, параграф 2. **При изпълнението на тези задачи ЕРИКС могат да дадат приоритет на предоставянето на конкретни услуги на субектите, следвайки основан на риска подход.**

3. Държавите членки гарантират, че всеки ЕРИКС разполага с подходяща, сигурна и устойчива комуникационна и информационна инфраструктура за обмен на информация със съществените и значимите субекти, както и с други относими заинтересовани страни. За тази цел държавите членки гарантират, че ЕРИКС допринасят за внедряването на сигурни инструменти за обмен на информация.

4. ЕРИКС си сътрудничат и, когато е подходящо, обменят относима информация в съответствие с член 26 с доверени секторни и междусекторни общности на съществените и значимите субекти.

5. ЕРИКС участват в партньорско [...]**обучение**, организирано в съответствие с член 16.

6. Държавите членки гарантират, че чрез мрежата на ЕРИКС, посочена в член 13, техните ЕРИКС си сътрудничат ефективно, ефикасно и сигурно.

7. Държавите членки съобщават на Комисията без излишно забавяне определените съгласно параграф 1 ЕРИКС, координатора на ЕРИКС, определен съгласно член 6, параграф 1, и техните съответни задачи, предвидени във връзка със субектите, посочени в приложения I и II.

8. Държавите членки може да поискат помощ от Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA) при създаването на националните ЕРИКС.

Член 10

Изисквания към ЕРИКС и задачи на ЕРИКС

1. ЕРИКС отговарят на следните изисквания:

   а) ЕРИКС гарантират високо ниво на достъпност на своите комуникационни [...] **канали**, като не допускат съществуването на точки, повредата в които може да доведе до общ срив, и разполагат с различни средства, чрез които могат да установяват връзка и да бъдат търсени във всеки един момент. ЕРИКС посочват ясно комуникационните канали и ги оповестяват на заинтересованите страни и на партньорите от сътрудничеството;

   б) Помещенията и поддържащите дейността на ЕРИКС информационни системи се разполагат в зони за сигурност;

в) ЕРИКС разполагат с подходяща система за управление и разпределяне на заявките, по-специално за да се улесни ефективното и ефикасно предаване на задачите от един на друг изпълнител;

г) ЕРИКС разполагат с достатъчно персонал, за да гарантират разполагаемост по всяко време;

д) ЕРИКС разполагат с резервни системи и резервно работно пространство, за да гарантират непрекъснатост своите услуги;

е) ЕРИКС имат възможността да участват в мрежи за международно сътрудничество.

2. ЕРИКС имат следните задачи:

а) наблюдение на киберзаплахи, уязвимости и инциденти на национално равнище;

б) подаване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за киберзаплахи, уязвимости и инциденти до съществените и значимите субекти, както и до **компетентните органи и** други относими заинтересовани страни;

в) реагиране на инциденти;

г) събиране и анализиране на криминалистични данни и осигуряване на динамичен анализ на рисковете и инцидентите и ситуационна осведоменост за киберсигурността;

д) осигуряване **[...]** на активно сканиране на мрежите и информационните системи […] **с цел откриване на уязвимости с потенциално значително въздействие, при условие че при липса на съгласие на този субект, не се прониква в мрежовите и информационните системи или не се накърнява функционирането им**;

е) участие в мрежата на ЕРИКС и предоставяне **според техните способности и компетенции** на взаимопомощ на останалите членове на мрежата при заявка от тяхна страна.

еа) когато е приложимо, изпълняване на ролята на координатор за целите на процеса на координирано оповестяване на уязвимости съгласно член 6, параграф 1, който включва по-специално улесняване на взаимодействието между докладващите субекти, отговорника за противодействие на потенциалните уязвимости и производителя или доставчика на ИКТ продукти или услуги в случаите, когато това е необходимо, идентифициране и установяване на контакт със съответните субекти, подпомагане на докладващите субекти, договаряне на срокове за оповестяване и управление на уязвимостите, засягащи множество организации (многостранно координирано оповестяване на уязвимостите).

3. ЕРИКС изграждат отношения на сътрудничество с относими действащи лица в частния сектор, с цел по-добро постигане на целите на директивата.

3а. ЕРИКС могат да установят отношения на сътрудничество с националните ЕРИКС на трети държави. Като част от това сътрудничество те могат да обменят съответна информация, включително лични данни, в съответствие с правото на Съюза в областта на защитата на данните.

4. За да улеснят сътрудничеството, ЕРИКС насърчават приемането и използването на общи или стандартизирани практики, схеми за класификация и таксономии във връзка със следното:

а) процедури за предприемане на действия при инциденти;

б) управление на кризи в областта на киберсигурността;

в) координирано оповестяване на уязвимости.

Член 11

Сътрудничество на национално равнище

1. Ако са отделени, компетентните органи по член 8, единното звено за контакт и ЕРИКС на една и съща държава членка си сътрудничат по отношение на изпълнението на задълженията, предвидени в настоящата директива.

2. Държавите членки гарантират, че техните компетентни органи или ЕРИКС получават уведомления за инциденти, и съществени киберзаплахи и ситуации, близки до инциденти, подадени съгласно настоящата директива. Когато държава членка реши, че нейните ЕРИКС няма да получават тези уведомления, на ЕРИКС — до степента, необходима за изпълнението на техните задачи, се предоставя достъп до данните за инциденти, за които са постъпили уведомления от съществените или значимите субекти съгласно член 20.

3. Всяка държава членка гарантира, че нейните компетентни органи или ЕРИКС информират нейното единно звено за контакт за уведомления за инциденти, съществени киберзаплахи и ситуации, близки до инциденти, подадени съгласно настоящата директива.

4. В степента, необходима за ефективното изпълнение на задачите и задълженията, предвидени в настоящата директива, държавите членки гарантират подходящо сътрудничество между компетентните органи, **ЕРИКС** и единните звена за контакт, както и правоприлагащите органи, органите за защита на личните данни и **компетентните** органи, **определени** [...] съгласно Директива (ЕС) XXXX/XXXX [Директивата относно устойчивостта на критичните субекти] [...], **компетентните органи съгласно Регламент за изпълнение (ЕС) 2019/1583 на Комисията, националните регулаторни органи, определени в съответствие Директива (ЕС) 2018/1972, националните органи, определени съгласно член 17 от Регламент (ЕС) № 910/2014,** [...] националните финансови органи, определени в съответствие с Регламент (ЕС) XXXX/XXXX на Европейския парламент и на Съвета [Регламента DORA], **както и компетентните органи, определени съгласно други специфични за сектора правни актове на Съюза,** в рамките на тази държава членка.

5. Държавите членки гарантират, че техните компетентни органи **съгласно настоящата директива и компетентните органи, определени съгласно Директива (ЕС) XXXX/XXXX [Директивата относно устойчивостта на критичните субекти]** редовно [...] **обменят [...]** информация [...] във връзка с **идентифицирането на критични субекти**, рисковете за киберсигурността, **киберзаплахите и киберинцидентите, както и несвързаните с киберсигурността рискове, заплахи и инциденти**, които засягат съществените субекти, определени като критични **[**или като субекти, равностойни на критични субекти,**]** съгласно Директива (ЕС) XXXX/XXXX [Директивата относно устойчивостта на критичните субекти], както и във връзка с мерките [...] в отговор на тези рискове и инциденти. **Държавите членки гарантират редовния обмен на съответната информация между компетентните органи съгласно настоящата директива и компетентните органи, определени съгласно Регламент XXXX/XXXX [Регламента DORA], Директива 2018/1972 и Регламент (ЕС) 910/2014.**

По отношение на доставчиците на удостоверителни услуги, и [...]по-специално[...] когато надзорната роля съгласно настоящата директива е възложена на орган, различен от надзорните органи, определени съгласно Регламент (ЕС) 910/2014, националните компетентни органи съгласно настоящата директива си сътрудничат тясно и своевременно чрез обмен на съответната информация, за да се гарантира ефективен надзор и спазване от страна на доставчиците на удостоверителни услуги на изискванията, посочени в настоящата директива и Регламент [XXXX/XXXX], **и когато е приложимо, националният компетентен орган съгласно настоящата директива информира без излишно забавяне надзорния орган по Регламента относно електронната идентификация и удостоверителните услуги за всяка нотифицирана значителна киберзаплаха или киберинцидент с въздействие върху удостоверителните услуги**.

5а. С цел [...] опростяване на докладването за инциденти държавите членки могат да установят единна входяща точка за всички уведомления, изисквани съгласно настоящата директива, както и съгласно Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО, когато е целесъобразно. Държавите членки могат да използват единната входяща точка за уведомленията, изисквани съгласно други специфични за сектора правни актове на Съюза. Тази единна входяща точка не засяга прилагането на разпоредбите на Регламент (ЕС) 2016/679 и Директива 2002/58/ЕО, по-специално на разпоредбите, отнасящи се до независимите надзорни органи.

ГЛАВА III

*Сътрудничество в **ЕС***

Член 12

Група за сътрудничество

1. С цел подкрепа и улесняване на стратегическото сътрудничество и обмена на информация между държавите членки**, както и [...] с цел укрепване на доверието,** [...]се създава група за сътрудничество.

2. Групата за сътрудничество изпълнява задачите си въз основа на двугодишните работни програми, посочени в параграф 6.

3. Групата за сътрудничество се състои от представители на държавите членки, Комисията и ENISA. Европейската служба за външна дейност участва в дейностите на групата за сътрудничество като наблюдател. Европейските надзорни органи (ЕНО) **и компетентните органи, определени съгласно Регламент (ЕС) XXXX/XXXX [Регламента DORA]**[...] могат да участват в дейностите на групата за сътрудничество **в съответствие с член 42, параграф 1 от Регламент (ЕС) XXXX/XXXX [Регламента DORA].**

   Групата за сътрудничество може да кани представители на съответните заинтересовани страни да участват в нейната работа, когато това е целесъобразно.

   Комисията осигурява административното обслужване.

4. Групата за сътрудничество изпълнява следните задачи:

   а) предоставяне на насоки на компетентните органи във връзка с транспонирането и прилагането на настоящата директива**;**

   аа) предоставяне на насоки във връзка с разработването и прилагането на политики за координирано оповестяване на уязвимости, както е посочено в член 5, параграф 2, буква в) и член 6, параграф 1;

б) обмен на най-добри практики и информация във връзка с прилагането на настоящата директива, включително във връзка с киберзаплахи, инциденти, уязвимости, ситуации, близки до инциденти, инициативи за повишаване на осведомеността, обучения, учения и умения, изграждане на капацитет, както и стандарти и технически спецификации;

в) взаимни консултации и сътрудничество с Комисията по възникващи инициативи за политики в областта на киберсигурността;

г) взаимни консултации и сътрудничество с Комисията по нейни проекти за актове за изпълнение[...], приети съгласно настоящата директива;

д) обмен на най-добри практики и информация с относимите институции, органи, служби и агенции на Съюза;

да) обмен на мнения относно прилагането на секторното законодателство с аспекти на киберсигурността;

е) обсъждане на доклади от партньорското [...] **обучение** съгласно посоченото в член 16, параграф 7;

ж) обсъждане на **опита** [...] от съвместни дейности по надзор при трансгранични случаи съгласно посоченото в член 34;

з) предоставяне на стратегически насоки на мрежата на ЕРИКС **и EU-CyCLONe** по конкретни възникващи въпроси;

за) обмен на мнения относно последващите действия в рамките на политиката във връзка с мащабни инциденти в областта на киберсигурността въз основа на поуките, извлечени от мрежата на ЕРИКС и EU-CyCLONe;

и) допринасяне за способностите в областта на киберсигурността в Съюза посредством улесняване на обмена на национални длъжностни лица чрез програма за изграждане на капацитет, включваща персонал от компетентните органи или ЕРИКС на държавите членки;

й) организиране на редовни съвместни заседания с относими частни заинтересовани страни от Съюза за обсъждане на дейностите, извършвани от групата, и събиране на приноса във връзка с възникващите предизвикателства пред политиките;

к) обсъждане на работата, предприета във връзка с ученията в областта на киберсигурността, включително извършената от ENISA работа**;**

ка) създаване на механизъм за партньорско обучение в съответствие с член 16 от настоящата директива.

5. Групата за сътрудничество може да изисква от мрежата на ЕРИКС технически доклади по избрани теми.

6. До … [24 месеца след датата на влизане в сила на настоящата директива] и на всеки две години след това групата за сътрудничество изготвя работна програма за действията, които трябва да бъдат предприети за изпълнение на нейните цели и задачи. Времевата рамка на първата програма, приета съгласно настоящата директива, се синхронизира с времевата рамка на последната програма, приета съгласно Директива (ЕС) 2016/1148.

7. Комисията може да установи чрез актове за изпълнение процедурните правила, необходими за работата на групата за сътрудничество. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 37, параграф 2.

8. Групата за сътрудничество провежда заседания редовно и поне веднъж годишно с групата за устойчивост на критичните субекти, създадена съгласно Директива (ЕС) XXXX/XXXX [Директивата относно устойчивостта на критичните субекти], за да се насърчава стратегическото сътрудничество и **да се улеснява** обменът на информация.

Член 13

Мрежа на ЕРИКС

1. Създава се мрежа на националните ЕРИКС, с цел да се допринесе за изграждането на доверие между държавите членки и да се насърчи бързото и ефективно оперативно сътрудничество между тях.

2. Мрежата на ЕРИКС се състои от представители на ЕРИКС на държавите членки, **определени в съответствие с член 9**, и екипите за незабавно реагиране при компютърни инциденти (CERT) на ЕС. Комисията участва в мрежата на ЕРИКС като наблюдател. ENISA осигурява административното обслужване и активно подкрепя сътрудничеството между ЕРИКС.

3. Мрежата на ЕРИКС изпълнява следните задачи:

   а) обмен на информация относно способностите на ЕРИКС;

   б) обмен на относима информация за инциденти, ситуации, близки до инциденти, киберзаплахи, рискове и уязвимости;

ба) обмен на информация във връзка с публикации и препоръки в областта на киберсигурността;

бб) споделяне на технически решения, улесняващи техническото справяне с инциденти;

бв) обмен на най-добри практики, инструменти и процеси по отношение на задачите на ЕРИКС;

в) по искане на потенциално засегнат от инцидент [...] **член** на мрежата на ЕРИКС — обмен и обсъждане на информация във връзка с този инцидент и свързаните киберзаплахи, рискове и уязвимости;

г) по искане на [...] **член** на мрежата на ЕРИКС — обсъждане и при възможност, осъществяване на координирана реакция на инцидент, констатиран в рамките на юрисдикцията на тази държава членка;

д) предоставяне на държавите членки на подкрепа за справянето с трансгранични инциденти съгласно настоящата директива;

е) сътрудничество, **обмен на най-добри практики** и предоставяне на помощ на определените ЕРИКС по член 6 с оглед на управлението на [...] координираното оповестяване на уязвимости, засягащи няколко производители или доставчици на ИКТ продукти, услуги и процедури, установени в различни държави членки;

ж) обсъждане и набелязване на допълнителни форми на оперативно сътрудничество, включително по отношение на:

i) категории киберзаплахи и инциденти;

ii) ранни предупреждения;

iii) взаимопомощ;

iv) принципи, условия и ред за координация при реакция на трансгранични рискове и инциденти;

v) допринасяне за националния план за реакция при инциденти и кризи в областта на киберсигурността, посочен в член 7, параграф 3**, по искане на държава членка**;

з) информиране на групата за сътрудничество относно дейностите на мрежата на ЕРИКС и допълнителните форми на оперативно сътрудничество, обсъдени в съответствие с буква ж), **и** при необходимост искане на насоки във връзка с това;

и) извършване на равносметка от ученията в областта на киберсигурността, включително от организираните от ENISA;

й) по искане на отделен ЕРИКС — обсъждане на способностите и подготвеността на същия този ЕРИКС;

к) сътрудничество и обмен на информация с регионални и центрове за операции по сигурността (ЦОС) и такива на равнището на Съюза с цел подобряване на общата ситуационна осведоменост за инциденти и заплахи в Съюза;

л) обсъждане на доклади от партньорското [...] **обучение** съгласно посоченото в член 16, параграф 7;

м) издаване на насоки, с цел да се улесни сближаването на оперативните практики по отношение на прилагането на разпоредбите на настоящия член във връзка с оперативното сътрудничество.

4. За целите на посочения в член 35 преглед и до [24 месеца след датата на влизане в сила на настоящата директива], както и на всеки две години след това, мрежата на ЕРИКС извършва оценка на напредъка, постигнат при оперативното сътрудничество, и представя доклад. В доклада по-специално се правят заключения за резултатите от партньорското **обучение** [...] по член 16, извършено във връзка с националните ЕРИКС, в това число заключения и препоръки съгласно настоящия член. Този доклад се представя и на групата за сътрудничество.

5. Мрежата на ЕРИКС приема свой процедурен правилник.

6. Мрежата на ЕРИКС си сътрудничи с EU-CyCLONe въз основа на договорени процедурни правила.

Член 14

Европейска мрежа за връзка на организациите при кибернетични кризи (EU — CyCLONe)

1. С цел подпомагане на координираното управление на мащабни инциденти и кризи в областта на киберсигурността, на оперативно равнище и осигуряване на редовния обмен на информация сред държавите членки и институциите, службите и агенциите на Съюза, се създава Европейската мрежа за връзка на организациите при кибернетични кризи (EU — CyCLONe).

2. EU-CyCLONe се състои от представителите на органите на държавите членки за управление на кризи в областта на киберсигурността, определени в съответствие с член 7[...]. **Комисията участва в дейностите на мрежата като наблюдател.** ENISA осигурява административното обслужване на мрежата и оказва подкрепа за сигурния обмен на информация**, а също и предоставя необходимите инструменти в подкрепа на сътрудничеството между държавите членки, като гарантира сигурен обмен на информация.**

EU-CyCLONe може да кани представители на съответните заинтересовани страни да участват в нейната работа, когато това е целесъобразно.

3. EU-CyCLONe има следните задачи:

а) повишаване на степента на подготвеност при управлението на мащабни инциденти и кризи в областта на киберсигурността;

б) развиване на споделена ситуационна осведоменост [...] за мащабни инциденти и кризи в областта на киберсигурността;

ба) оценка на последиците и въздействието на съответните мащабни инциденти в областта на киберсигурността и предлагане на възможни мерки за смекчаването им;

в) координиране **на управлението на** мащабни инциденти и кризи в областта на киберсигурността [...] и подпомагане на процеса на вземане на решения на политическо равнище във връзка с такива инциденти и кризи;

г) **по искане на държава членка,** обсъждане на националните **ѝ** планове за реакция при инциденти **и кризи** в областта на киберсигурността, посочени в член 7, параграф **3**[...]**;**[...]

4. EU-CyCLONe приема свой процедурен правилник.

5. EU-CyCLONe докладва редовно на групата за сътрудничество относно **управлението на мащабните инциденти и кризи** в областта на киберсигурността, [...] като се фокусира по-специално върху тяхното въздействие върху съществените и значимите субекти.

6. EU-CyCLONe си сътрудничи с мрежата на ЕРИКС въз основа на договорени процедурни правила.

7. До [24 месеца след датата на влизане в сила на настоящата директива] EU-CyCLONe представя на Европейския парламент и на Съвета доклад за оценка на нейната работа.

Член 14а

Международно сътрудничество

При необходимост Съюзът може да сключва международни споразумения в съответствие с член 218 от ДФЕС с трети държави или международни организации, които допускат и уреждат участието им в някои дейности на групата за сътрудничество, мрежата на ЕРИКС и EU-CyCLONe, в съответствие с правото на Съюза в областта на защитата на данните.

Член 15

Доклад за състоянието на киберсигурността в Съюза

1. В сътрудничество с Комисията **и групата за сътрудничество** ENISA издава двугодишен доклад за състоянието на киберсигурността в Съюза. **По-специално,** [...]докладът [...] включва [...] следното:

   аа) оценка на риска за киберсигурността на равнището на Съюза, като се отчита картината на заплахите;

   а) [...] **оценка на** развитието на способностите в областта на киберсигурността в публичния и частния сектор в Съюза;

   б) [...]

   в) **обобщена оценка въз основа на количествени и качествени показатели** [...] в областта на киберсигурността, предоставяща **преглед** на степента на зрялост на способностите в областта на киберсигурността**, включително на специфичните за сектора способности**.

2. В доклада се включват конкретни препоръки за политиките във връзка с повишаването на степента на киберсигурността в Съюза, както и резюме на констатациите за конкретния период от докладите на Агенцията за техническото състояние на киберсигурността на ЕС, издавани от ENISA в съответствие с член 7, параграф 6 от Регламент (ЕС) 2019/881.

Член 16

Партньорско обучение

1. **С оглед на укрепването на взаимното доверие, постигането на високо общо равнище на киберсигурност, както и укрепването на способностите и политиките на държавите членки в областта на киберсигурността, необходими за ефективното прилагане на настоящата директива,** [...]**групата за сътрудничество** [...] определя, **с подкрепата на Комисията и след** консултации с [...] ENISA **и когато е уместно, с мрежата на ЕРИКС**, и най-късно до **24 [...]** месеца след влизането в сила на настоящата директива, методологията [...] **за обективна, недискриминационна и справедлива система за** партньорско [...] **обучение** [...] **по отношение на прилагането** от държавите членки [...] **на настоящата директива**. **Участието в партньорското обучение е доброволно. Системата се състои от кръгове на оценки,** [...] провеждани от [...] експерти по киберсигурност, подбрани от държави членки, [...] и обхваща [...] **един или няколко от** следните аспекти:

   i) [...] прилагането на изискванията за управлението на риска, свързан с киберсигурността, и задълженията за докладване по членове 18 и 20;

   ii) [...] способностите, включително наличните [...] ресурси, и [...] изпълнението на задачите на националните компетентни органи, **посочени в член 8, и ЕРИКС, посочени в член 9**;

[...]

i**ii**[...]) [...] **прилагането** на взаимопомощта по член 34;

iv) [...] **прилагането** на рамката за обмен на информация по член 26[...] .

2. **Критериите, въз основа на които държавите членки трябва да определят експерти, отговарящи на условията за участие в кръговете на партньорско обучение, са** [...] обективни, недискриминационни, справедливи и прозрачни [...] **и се включват в методологията, посочена в параграф 1.** ENISA и Комисията [...] **могат да** определят експерти, които да участват като наблюдатели в **кръговете на партньорско** [...] **обучение**. [...]

3. [...] .

3а. Преди началото на кръговете на партньорско обучение държавите членки могат да извършват самооценка на аспектите, обхванати от този конкретен кръг на партньорско обучение, и да представят тази самооценка на определените експерти, посочени в параграф 2.

4. Партньорското [...] **обучение може да** [...] включва **физически** или виртуални посещения на място, както и дистанционен обмен. С оглед на принципа на доброто сътрудничество държавите членки, [...] **участващи в партньорското обучение,** предоставят на определените експерти [...] информацията, необходима за оценката [...]**, без да се засягат националните закони или законодателството на Съюза относно защитата на поверителна или класифицирана информация или защитата на основните функции на държавата, като например националната сигурност.** Всяка информация, получена в процеса на партньорско [...] **обучение**, се използва единствено за тази цел. Участващите в партньорско [...] **обучение** експерти не оповестяват никаква чувствителна или поверителна информация, получена в [...] **този контекст**, на които и да е трети страни. **Държавата членка, участваща в партньорското обучение, може да възрази срещу определянето на конкретни експерти по надлежно обосновани причини, съобщени на групата за сътрудничество.**

5. Веднъж **разгледани на** даден кръг на **партньорско** [...] обучение, същите аспекти не се разглеждат на допълнителни **кръгове на** партньорско [...]**обучение за участващите** държав**и** членк**и** в рамките на [...] **четири** години след приключването на **въпросния** [...] **кръг на партньорско [...]обучение, освен ако съответните държави членки не поискат това или не изразят съгласие по предложение** на **групата за сътрудничество [...]**.

6. [...]

7. Участващите в **кръговете на** партньорско [...] **обучение** експерти изготвят доклади за констатациите и заключения от [...] **оценките**. **Държавите членки имат право да представят коментари по съответните си проектодоклади, които се прилагат към доклада. Окончателните** доклади се предават на [...] групата за сътрудничество [...]. **Държавите членки могат да решат да направят своите доклади публично достояние.**

ГЛАВА IV

Управление на риска, свързан с киберсигурността, и задължения за докладване

РАЗДЕЛ I

Управление на риска, свързан с киберсигурността, и докладване

Член 17

Управление

1. Държавите членки гарантират, че управителните органи на съществените и значимите субекти одобряват мерките за управление на риска, свързан с киберсигурността, предприети от тези субекти с цел спазване на член 18, […] **наблюдават** прилагането му и […] **могат да бъдат подведени под** отговорност за неизпълнението на задълженията по този член от страна на субектите.

   Прилагането на настоящия параграф не засяга националното право на държавата членка по отношение на правилата за отговорност в публичните институции, както и отговорността на държавните служители и на избраните и назначените длъжностни лица.

2. Държавите членки гарантират, че **от членовете на управителния орган** […] **се изисква** да преминават редовно през […] обучения за придобиване на достатъчно познания и умения, с цел да могат да разбират и оценяват рисковете за киберсигурността и управленските практики и тяхното въздействие върху операциите на субекта.

Член 18

Мерки за управление на риска, свързан киберсигурността

1а. **Настоящата директива прилага подход, обхващащ всички опасности, който включва защитата на мрежовите и информационните системи и тяхната физическа среда от всяко събитие, което би могло да застраши наличността, автентичността, целостта или поверителността на съхраняваните, предаваните или обработваните данни или на услугите, предлагани от или достъпни чрез мрежови и информационни системи.**

1. Държавите членки гарантират, че съществените и значимите субекти предприемат подходящи и пропорционални технически и организационни мерки за управление на рисковете за сигурността на мрежите и информационните системи, които тези субекти използват при предоставянето на своите услуги. Тези мерки осигуряват ниво на сигурност на мрежите и информационните системи, съответстващо на съществуващия риск, съобразно последните постижения в тази област **и разходите за прилагане**. **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. Като се имат предвид равнището и видът на риска за обществото в случай на инциденти, засягащи съществени или значими субекти, мерките за управление на риска за киберсигурността, наложени на значимите субекти, могат да бъдат по-малко строги от тези, наложени на съществените субекти.**

2. Мерките, посочени в параграф 1, включват най-малко следното:

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

б) действия при инциденти (предотвратяване, установяване, […] реакция на инциденти **и възстановяване от инциденти**);

в) непрекъснатост на стопанската дейност и управление на кризи;

г) сигурност на веригата за доставка, включително свързани със сигурността аспекти относно взаимовръзките между всеки субект и неговите **преки** снабдители или доставчици на услуги, като например доставчиците на услуги за съхранение и обработване на данни или услуги за управление на сигурността;

д) сигурност при придобиването на мрежи и информационни системи, разработване и поддръжка, включително предприемане на действия при уязвимости и оповестяването им;

е) политики и процедури (проверки и одити) за оценяване на ефективността на мерките за управление на риска, свързан с киберсигурността;

ж) **политика за** използването на криптография и криптиране;

жа) сигурност на човешките ресурси, политики за контрол на достъпа и управление на активи.

3. Държавите членки гарантират, че когато разглеждат подходящи мерки по параграф 2, буква г), […] от субектите **се изисква да** вземат предвид уязвимостите, специфични за всеки **пряк** снабдител или доставчик на услуги, както и цялостното качество на продуктите и практиките в областта на киберсигурността на своите снабдители или доставчици на услуги, включително техните процедури за сигурно разработване. **Държавите членки гарантират също така, че когато се обмислят подходящи мерки като посочените в параграф 2, буква г), от субектите се изисква да вземат предвид резултатите от координираните оценки на риска, извършени в съответствие с член 19, параграф 1.**

4. Държавите членки гарантират, че когато един субект установи, че неговите услуги или задачи не са в съответствие с изискванията по параграф 2, той без излишно забавяне предприема всички необходими коригиращи мерки за привеждането на въпросната услуга в съответствие.

5. Комисията може да приема актове за изпълнение, с цел да определи техническите и методологическите спецификации, **както и при необходимост секторните особености,** на елементите по параграф 2 **от настоящия член**. **Комисията приема до [18 месеца след влизането в сила на настоящата директива] актове за изпълнение, за да определи техническите и методологическите спецификации за субектите, посочени в член 24, параграф 1, и доставчиците на удостоверителни услуги, посочени в точка 8 от приложение I. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 37, параграф 2.** При […] изготвянето на […] тези актове **за изпълнение** Комисията […] във възможно най-голяма степен **следва** международните и европейските стандарти, както и съответните технически спецификации, **и обменя становища с групата за сътрудничество и ENISA относно проекта на акт за изпълнение в съответствие с член 12, параграф 4, буква г).**

6. [...]

Член 19

Координирана на равнището на ЕС оценка на критични вериги за доставка

1. Групата за сътрудничество, в сътрудничество с Комисията и ENISA, може да извършва координирани оценки на риска на конкретни критични вериги за доставка на ИКТ услуги, системи или продукти, при които се вземат предвид техническите и, когато е уместно, нетехническите рискови фактори.

2. След консултиране с групата за сътрудничество и ENISA Комисията установява конкретните критични ИКТ услуги, системи или продукти, които може да бъдат предмет на координирана оценка на риска по параграф 1.

Член 20

Задължения за докладване

1. Държавите членки гарантират, че съществените и значимите субекти уведомяват без излишно забавяне компетентните органи или ЕРИКС в съответствие с параграфи 3 и 4 за всякакви инциденти, имащи значително въздействие върху предоставянето на техните услуги. Когато е подходящо, тези субекти уведомяват без излишно забавяне получателите на техните услуги за **въпросните** инциденти, които има вероятност неблагоприятно да засегнат предоставянето на тези услуги. Държавите членки гарантират, че тези субекти докладват, наред с друго, всяка информация, позволяваща на компетентните органи или на ЕРИКС да определи всякакво трансгранично въздействие на инцидентите. **Актът на уведомяване сам по себе си не води до повишена отговорност за уведомяващия субект.**

2. [...]

Когато е приложимо, […] **съществените и значимите** субекти уведомяват без излишно забавяне получателите на техните услуги, които са потенциално засегнати от значителна киберзаплаха, за всички мерки или средства за защита, които тези получатели могат да предприемат като реакция на тази заплаха. Когато е подходящо, субектите следва да уведомят тези получатели за самата заплаха. **Актът на** уведомяване **сам по себе си** не води до повишена отговорност за уведомяващия субект.

3. Даден инцидент се счита за значителен, ако:

а) е причинил или има потенциала да причини **сериозно** […] оперативно смущение **на услугата** или финансови загуби за съответния субект;

б) е засегнал или има потенциала да засегне други физически или юридически лица, причинявайки значителни материални или нематериални загуби.

4. Държавите членки гарантират, че за целите на уведомяването по параграф 1 съответните субекти представят на компетентните органи или ЕРИКС:

а) без излишно забавяне и при всички случаи в рамките на 24 часа след узнаването за даден инцидент – първоначално уведомление **като ранно предупреждение**, в което, когато е приложимо, се посочва дали се предполага, че инцидентът се дължи на незаконосъобразно или злонамерено действие;

б) по искане на компетентен орган или на ЕРИКС — междинен доклад за съответните новости на състоянието;

в) **окончателен** доклад не по-късно от един месец след подаването на […] **първоначалното уведомление** по буква а), включващ най-малко следното:

i) подробно описание на инцидента, неговата тежест и въздействие;

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

iii) приложените и текущите мерки за ограничаване.

Държавите членки гарантират, че в надлежно обосновани случаи и при споразумение с компетентните органи или ЕРИКС съответният субект може да се отклони от сроковете по букви а) и в). **По-специално, отклонение от срока, посочен в буква в), може да бъде обосновано в случаи, когато инцидентът все още продължава.**

5. Компетентните национални органи или ЕРИКС предоставят […] **без ненужно забавяне** след получаването на първоначалното уведомление по параграф 4, буква а), отговор на уведомяващия субект, включително първоначална обратна информация за инцидента и, при искане от субекта, насоки за прилагането на възможни мерки за ограничение. Когато ЕРИКС не е получил уведомлението, посочено в параграф 1, насоките се предоставят от компетентния орган в сътрудничество с ЕРИКС. ЕРИКС предоставя допълнителна техническа подкрепа, ако съответният субект изиска това. Когато има подозрения, че инцидентът е с престъпно естество, компетентните национални органи или ЕРИКС предоставят насоки относно докладването на инцидента на правоприлагащите органи.

6. Когато е целесъобразно и особено когато инцидентът по параграф 1 засяга две или повече държави членки, компетентният орган, ЕРИКС или **единното звено за контакт** информира другите засегнати държави членки и ENISA за инцидента. **Тази информация включва най-малко елементите, предвидени в параграф 4 от настоящия член.** При това компетентните органи, ЕРИКС и единните звена за контакт запазват сигурността и търговските интереси на субекта, както и поверителността на предоставената информация в съответствие с правото на Съюза или с националното законодателство, което е в съответствие с правото на Съюза.

7. При необходимост от обществено уведомяване с цел предотвратяване на инцидент или справяне с текущ инцидент или когато оповестяването на инцидента е в обществен интерес по друга причина, компетентният орган или ЕРИКС, и когато е уместно, органите или ЕРИКС на други засегнати държави членки могат, след като се консултират със засегнатия субект, да уведомят обществеността за инцидента или да изискат от него на направи това.

8. По искане на компетентния орган или ЕРИКС единното звено за контакт предава уведомленията, получени съгласно параграф 1 […], на единните звена за контакт на други засегнати държави членки.

9. Единното звено за контакт представя […] **на всеки шест месеца** на ENISA обобщаващ доклад, включващ анонимизирани и обобщени данни за инцидентите, значителните киберзаплахи и ситуации, близки до инциденти, за които е изпратено уведомление в съответствие с параграф 1 […] и съгласно член 27. За да допринесе за предоставянето на сравнима информация, ENISA може да издава технически насоки за параметрите на включената в обобщителния доклад информация. **На всеки шест месеца ENISA информира групата за сътрудничество и мрежата на ЕРИКС за своите констатации относно получените уведомления.**

10. Компетентните органи предоставят на компетентните органи, определени съгласно Директива (ЕС) XXXX/XXXX [Директива относно устойчивостта на критичните субекти], информация относно инцидентите и киберзаплахите, за които е изпратено уведомление в съответствие с параграфи 1 и 2 от съществените субекти, определени като критични **[**или като субекти, равностойни на критични субекти,**]** съгласно Директива (ЕС) XXXX/XXXX [Директива относно устойчивостта на критичните субекти].

11. Комисията може да приема актове за изпълнение, в които допълнително се уточняват видът на информацията, форматът и процедурата на изпратено по параграфи 1 и 2 уведомление. Комисията може да приема актове за изпълнение, в които допълнително се уточняват случаите, при които даден инцидент се счита за значителен съгласно посоченото в параграф 3. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 37, параграф 2.

Член 21

Използване на европейски схеми за сертифициране на киберсигурността

1. За да се докаже съответствие с някои изисквания по член 18, **държавите членки могат да изискат от субектите да използват конкретни ИКТ продукти, […] услуги и […] процеси, сертифицирани** съгласно конкретни европейски схеми за сертифициране на киберсигурността, приети съгласно член 49 от Регламент (ЕС) 2019/881. Подлежащите на сертифициране **ИКТ** продукти, услуги и процеси могат да бъдат разработени от съществен или значим субект или да бъдат предоставени от трети страни.

2. Комисията може да […] приема […] актове за изпълнение, с които се определя от кои категории съществени **или значими** субекти се изисква **да използват определени сертифицирани ИКТ продукти, услуги и процеси или** да получат сертификат […] по европейските схеми за сертифициране на киберсигурността, **приети съгласно член 49 от Регламент (ЕС) 2019/881.** […] **Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 37, параграф 2. При изготвянето на тези актове за изпълнение Комисията, в съответствие с член 56 от Регламент (ЕС) 2019/881:**

   i) отчита въздействието на мерките върху производителите или доставчиците на такива ИКТ продукти, услуги или процеси, както и върху ползвателите, от гледна точка на разходите за тези мерки и социалните или икономическите ползи от очакваното повишено ниво на сигурност на ИКТ продуктите, услугите или процесите, както и на техните налични на пазара алтернативи;

   ii) провежда отворен, прозрачен и приобщаващ процес на консултиране с всички заинтересовани страни и държави членки;

(i) отчита сроковете за изпълнение, необходимостта от преходни мерки и срокове, по-специално по отношение на възможното въздействие на мярката върху производителите или доставчиците на ИКТ продукти, услуги или процеси, или върху техните ползватели, по-специално МСП;

(ii) взема предвид наличието и прилагането на имащи отношение закони на държавите членки.

3. Комисията може да изиска от ENISA да изготви проект на схема за сертифициране **или да направи преглед на съществуваща европейска схема за сертифициране на киберсигурността** съгласно член 48, параграф 2 от Регламент (ЕС) 2019/881 в случаите, при които не е налична подходяща европейска схема за сертифициране на киберсигурността за целите на параграф 2 **от настоящия член**.

Член 22

Стандартизация

1. С цел насърчаване на еднообразното прилагане на член 18, параграфи 1 и 2 държавите членки, без да налагат употребата на определен тип технология или да упражняват дискриминация в нейна полза, насърчават използването на европейско или международно приетите стандарти и спецификации от значение за сигурността на мрежите и информационните системи.

2. В сътрудничество с държавите членки ENISA изготвя препоръки и насоки по отношение на техническите области, които да се вземат под внимание във връзка с параграф 1, както и по отношение на вече съществуващите стандарти, включително националните стандарти на държавите членки, което да позволи обхващането на тези области.

Член 23

Бази данни с имена на домейни и регистрационни данни

1. С цел допринасяне за сигурността, стабилността и устойчивостта на системата за имена на домейни държавите членки гарантират, че регистрите на **имена** на домейни от първо ниво и субектите, предоставящи за тях услуги за регистрация на такива имена на домейни, надлежно събират и поддържат точни и пълни данни за регистрацията на имената на домейни в специално предназначено съоръжение за база данни **съгласно** […] правото на Съюза за защита на данните по отношение на личните данни.

2. Държавите членки гарантират, че базите данни за съхранение на данните за регистрация на имена на домейни по параграф 1, съдържат относима информация за установяване и осъществяване на връзка с притежателите на имена на домейни и точките за контакт, администриращи имената на домейните в домейни от първо ниво, **в т.ч. поне следните данни:**

   а) име на домейна

   б) дата на регистрация

   в) данни за регистранта, включително:

      i) за физически лица – име, фамилия и имейл адрес;

      ii) за юридически лица – име и имейл адрес.

3. Държавите членки гарантират, че регистрите на **имена** на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни от първо ниво, имат установени политики и процедури, за да осигурят, че базите данни включват точна и пълна информация. Държавите членки гарантират, че тези политики и процедури са направени публично достъпни.

4. Държавите членки гарантират, че регистрите на **имена** на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни от първо ниво, публикуват, без излишно забавяне след регистрацията на име на домейн, данните за нея, които не са лични.

5. Държавите членки гарантират, че регистрите на **имена** на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни от първо ниво, предоставят достъп до конкретни данни за регистрация на имена на домейни при законосъобразни и надлежни искания от законно търсещите достъп, в изпълнение на правото на Съюза за защита на данните. Държавите членки гарантират, че регистрите на **имена** на домейни от първо ниво и субектите, предоставящи услуги за регистрация на имена на домейни от първо ниво, отговарят без излишно забавяне **и при всички случаи в рамките на 72 часа** на всички искания за достъп. Държавите членки гарантират, че политиките и процедурите за оповестяване на такива данни са направени публично достъпни.

Раздел II

Юрисдикция и регистрация

Член 24

Юрисдикция и териториалност

1а. За субектите по смисъла на настоящата директива се смята, че са под юрисдикцията на държавата членка, в която предоставят услугите си. Субектите, посочени в точки 1–7 и 10 от приложение I, доставчиците на удостоверителни услуги и доставчиците на точки за обмен в интернет, посочени в точка 8 от приложение I и точки 1–5 от приложение II, се смятат за попадащи под юрисдикцията на държавата членка, на чиято територия са установени.

1. Доставчиците на DNS услуги, регистрите на имена на домейни от първо ниво […] **и субектите, предоставящи услуги за регистриране на имена на домейни от първо ниво**, доставчиците на компютърни услуги в облак, доставчиците на услуги на центрове за данни, […] доставчиците на мрежи за предоставяне на съдържание, **доставчиците на управлявани услуги и доставчиците на управлявани услуги за сигурност**, посочени в точки 8 **и 8а** от приложение I, както и доставчиците на цифрово съдържание, посочени в точка 6 от приложение II, се считат за попадащи под юрисдикцията на държавата членка, в която се намира основното им място на установяване в Съюза.

2. За целите на настоящата директива се счита, че основното място на установяване в Съюза на субектите, посочени в параграф 1, е в държавата членка, в която **преимуществено** се вземат решенията относно мерките за управление на риска, свързан с киберсигурността. Ако **мястото, където преимуществено се вземат решенията, не може да бъде определено или** тези решения не се вземат на никое място на установяване в Съюза, за основно място на установяване се счита държавата членка, в която субектите са се установили с най-голям брой служители в Съюза. **Когато услугите се предоставят от група предприятия, основното място на установяване се счита за основно място на установяване на групата предприятия.**

3. Ако субект по параграф 1 не е установен в Съюза, но предлага услуги в него, той посочва представител в Съюза. Представителят трябва да е установен в една от държавите членки, в които се предлагат услугите. Приема се, че този субект е под юрисдикцията на държавата членка, в която е установен представителят. При липсата на определен представител в Съюза съгласно настоящия член всяка държава членка, в която субектът предоставя услуги, може да предприеме правни действия срещу него за неизпълнение на задълженията съгласно настоящата директива.

4. Определянето на представител от страна на субект по параграф 1 не засяга правните действия, които биха могли да се предприемат срещу самия субект.

4а. Държавите членки, които са получили искане за взаимопомощ по отношение на субектите, посочени в параграф 1, могат, в рамките на искането, да предприемат подходящи надзорни и правоприлагащи мерки по отношение на съответния субект, който предоставя услуги или на когото принадлежи мрежовата и информационната система на тяхна територия.

Член 25

Регистър за някои субекти на цифрова инфраструктура и доставчици на цифрови услуги

1. […] **Държавите членки гарантират, че […] субектите, посочени в член 24, параграф 1, чието основно място на установяване е на тяхна територия, или ако не са установени в Съюза, чиито определени представители в Съюза са установени на тяхна територия, трябва** […] да представят **на компетентните органи** [най-късно до 12 месеца след влизането в сила на директивата] следната информация :

а) наименованието на субекта;

аа) вида на субекта съгласно приложения I и II към настоящата директива;

б) адреса на основното място на установяване и на останалите законови места на установяване в Съюза или, при липсата на място на установяване в Съюза, на неговия представител, определен съгласно параграф 3 от член 24;

в) актуални данни за контакт, включително имейл адреси и телефонни номера на субектите **и на техните представители**;

г) държавите членки, в които субектът предоставя услугата.

Когато е приложимо, тази информация се подава чрез националния механизъм за самоуведомяване, посочен в член 2а.

2. **Държавите членки гарантират, че** субектите по параграф 1 **уведомяват** без забавяне **и за** всякакви промени в изпратените от тях данни съгласно параграф 1, и при всички положения, в рамките на три месеца от датата, на която е влязла в сила промяната.

3. […] **Единните звена за контакт на държавите членки** изпращат на **ENISA информацията, посочена в параграфи 1 и 2**. [...]

3а. Въз основа на информацията, получена съгласно параграф 3 от настоящия член, ENISA създава и поддържа регистър на субектите, посочени в параграф 1. По искане на държавите членки ENISA дава възможност за достъп на съответните компетентни органи до регистъра, като същевременно осигурява необходимите гаранции за защита на поверителността на информацията, когато е приложимо.

4. [...]

ГЛАВА V

Обмен на информация

Член 26

Споразумения за обмен на информация в областта на киберсигурността

1. […] Държавите членки гарантират, че съществените и значимите субекти могат **доброволно** да обменят помежду си важна информация за киберсигурността, включително такава относно киберзаплахи, **ситуации, близки до инцидент,** уязвимости, признаци за нарушена сигурност, тактики, техники и процедури, предупреждения във връзка с киберсигурността, както и инструменти за конфигуриране, когато този обмен на информация:

   а) има за цел предотвратяване, откриване, реакция или ограничаване на инциденти с киберсигурността;

б) подобрява нивото на киберсигурност, по-специално посредством повишаване на осведомеността във връзка с киберзаплахи, ограничаване или възпрепятстване на такива заплахи, способност за разпространение, поддържане на набор от отбранителни способности, отстраняване и оповестяване на уязвимости, техники за откриване на заплахи, стратегии за ограничаване или етапи за реакция или възстановяване.

2. Държавите членки гарантират, че обменът на информация се осъществява в рамките на […] общности на съществените и значимите субекти. Този обмен се осъществява чрез споразумения за обмен на информация с оглед на потенциално чувствителния характер на споделяната информация […].

3. Държавите членки […] **могат да** установяват правилата, определящи процедурата, оперативните елементи (включително използването на специално предназначени ИКТ платформи), съдържанието и условията по споразуменията за обмен на информация по параграф 2. В тези правила […] **могат да** се определят и подробностите за участието на публичните органи в такива споразумения, както и оперативните елементи, включително използването на специално предназначени ИТ платформи. Държавите членки предлагат подкрепа за прилагането на такива споразумения в съответствие със своите политики, посочени в член 5, параграф 2, буква ж).

4. Съществените и значимите субекти уведомяват компетентните органи за своето участие в споразуменията за обмен на информация по параграф 2 при присъединяването им към такива споразумения или, когато е приложимо, за оттеглянето им от тях, след като то влезе в сила.

5. […] ENISA осигурява подкрепа за установяването на споразуменията за обмен на информация в областта на киберсигурността по параграф 2, като предоставя най-добри практики и насоки.

Член 27

Доброволно уведомяване за относима информация

1. Без да се засяга член 20, държавите членки гарантират, че съществените и значимите субекти могат да уведомяват доброволно компетентните органи или ЕРИКС за всякакви съответни инциденти, киберзаплахи или ситуации, близки до инцидент.

2. Държавите членки гарантират, че без да се засягат разпоредбите на член 3, субектите извън обхвата на настоящата директива могат доброволно да изпращат уведомления за значителни инциденти, киберзаплахи или ситуации, близки до инциденти. При обработването на уведомленията държавите членки действат в съответствие с процедурата по член 20. Държавите членки могат да обработват задължителните уведомления с предимство пред доброволните уведомления. **Без да се засягат разследването, разкриването и наказателното преследване на престъпления,** доброволното докладване не води до налагането на никакви допълнителни задължения за докладващия субект, на които той не би бил предмет, ако не подаде уведомлението.

3. Доброволните уведомления се обработват само когато обработването им не представлява несъразмерна или неоправдана тежест за съответната държава членка.

ГЛАВА VI

Надзор и правоприлагане

Член 28

Основни аспекти относно надзора и правоприлагането

1. Държавите членки гарантират, че компетентните органи ефективно следят и предприемат мерки, необходими за осигуряване на съвместимостта с настоящата директива, по-специално задълженията по членове 18, […] 20 **и 23**. **Държавите членки могат да разрешат на компетентните органи да дадат приоритет на надзора, който следва основан на риска подход.**

2. При справянето с киберинциденти компетентните органи работят в тясно сътрудничество с органите за защита на данните, **компетентните органи, определени съгласно Директива (ЕС) XXXX/XXXX [Директивата относно устойчивостта на критичните субекти], надзорните органи, определени съгласно Регламент (ЕС) 910/2014, и другите компетентни органи, определени съгласно специфичните за отделните сектори правни актове на Съюза**. [...]

3. Без да се засягат националните законодателни и институционални рамки, държавите членки гарантират, че при надзора на спазването на настоящата директива от органите на публичната администрация и прилагането на евентуални санкции за неспазване, компетентните органи разполагат с необходимите правомощия да изпълняват тези задачи с оперативна независимост по отношение на субектите, над които се упражнява надзор. Държавите членки могат да вземат решение за налагането на подходящи, пропорционални и ефективни мерки за надзор и правоприлагане по отношение на тези субекти в съответствие със своите националните рамки и правен ред.

Член 29

Надзор и правоприлагане за съществените субекти

1. Държавите членки гарантират, че мерките за надзор или правоприлагане, наложени на съществените субекти по отношение на определените в настоящата директива задължения, са ефективни, пропорционални и възпиращи, като се вземат предвид обстоятелствата по всеки отделен случай.

2. Държавите членки гарантират, че когато изпълняват своите задачи по надзора във връзка със съществените субекти, компетентните органи **следват основан на риска подход и** са упълномощени да подлагат тези субекти **най-малко** на:

   а) проверки на място или дистанционни проверки, включително случайни;

   б) редовно одитиране **на сигурността**;

   в) целеви одити на сигурността въз основа на оценки на риска или свързана с риска налична информация;

   г) проверки за сигурност, основани на обективни, недискриминационни, справедливи и прозрачни критерии за оценка на риска, **когато това е необходимо по технически причини, със съдействието на съответния субект**;

   д) искания за информация, необходима за оценка на мерките за киберсигурност, приети от субекта, включително документирани политики за киберсигурност […];

   е) искания за достъп до данни, документи или всякаква информация, необходими за изпълнението на техните задачи по надзор;

   ж) искания за доказателства за изпълнение на политиките в областта на киберсигурността, като например резултатите от одитите на сигурността, извършени от квалифициран одитор, и съответните подкрепящи доказателства.

2а. При изпълнението на надзорните си задачи, предвидени в параграф 2 от настоящия член, компетентните органи могат да установят надзорни методологии, които дават възможност за приоритизиране на тези задачи, следвайки основан на риска подход.

3. При упражняване на своите правомощия по параграф 2, букви д)—ж) компетентните органи заявяват целта на своето искане и уточняват исканата информация.

4. Държавите членки гарантират, че в рамките на своите правомощия по правоприлагане във връзка със съществените субекти компетентните органи са упълномощени **най-малкото**:

а) да издават предупреждения при неизпълнение на задълженията по настоящата директива от субектите;

б) да изискват посредством обвързващи указания или разпореждане от тези субекти да поправят установените пропуски или нарушения на задълженията по настоящата директива;

в) да разпореждат на тези субекти да преустановяват поведение, което не е в съответствие със задълженията по настоящата директива и да се въздържат от повтарянето на такова поведение;

г) да разпореждат на тези субекти да привеждат своите мерки за управление на риска и/или задължения за докладване в съответствие със задълженията по членове 18 и 20 по конкретизиран начин и в рамките на посочен период;

д) да разпореждат на тези субекти да уведомяват физическото или юридическото лице или лица, на които предоставят услуги или дейности, потенциално засегнати от значителна киберзаплаха, **за естеството на заплахата, както и** за възможните защитни или коригиращи мерки, които могат да бъдат предприети от това физическо или юридическо лице или лица в отговор на тази заплаха;

е) да разпореждат на тези субекти да изпълняват препоръките, предвидени в резултат на одит на сигурността в рамките на разумен срок;

ж) [...]

з) да разпореждат на тези субекти да оповестяват по определен начин аспектите на неспазване на задълженията, предвидени в настоящата директива, **когато такова публично оповестяване не води до вредна експозиция на съответния субект**;

и) [...]

й) да налагат или изискват налагането от съответните органи или съдилища съгласно националното право на административна глоба по член 31 в допълнение към или вместо мерките по букви а)—и) от настоящия параграф, в зависимост от обстоятелствата по всеки отделен случай.

5. Когато действията по правоприлагане, приети съгласно параграф 4, букви а)—г) и е), се окажат неефективни, държавите членки гарантират, че компетентните органи разполагат с правомощие да определят срок, в който от съществения субект се изисква да предприеме необходимото действие за отстраняване на недостатъците или за привеждане в съответствие с изискванията на тези органи. Ако изисканото действие не се предприеме в определения срок, държавите членки гарантират, че компетентните органи разполагат с правомощия:

а) да прекратят или да изискат от сертифициращ или разрешаващ орган, **или съд, според националното право,** да прекрати сертификат или разрешение относно всички или част от услугите или дейностите, предоставяни от съществен субект;

б) да наложат или изискат от съответните органи или съдилища налагането съгласно националното право на временна забрана спрямо всяко лице, изпълняващо ръководни функции на равнището на главно изпълнително длъжностно лице или законен представител в този съществен субект, както и спрямо всяко друго физическо лице, отговарящо за нарушението, да упражнява управленски функции в този субект.

Тези санкции се прилагат само докато субектът предприеме необходимото действие за отстраняване на недостатъците или за изпълнение на изискванията на компетентния орган, за които са приложени такива санкции.

Санкциите, предвидени в настоящия параграф, не се прилагат за субекти на публичната администрация, които са предмет на настоящата директива.

6. Държавите членки гарантират, че всяко физическо лице, отговорно за съществен субект или действащо като негов представител въз основа на правомощие да го представлява, да взема решения от негово име или да упражнява контрол върху него, има необходимите правомощия, за да осигури спазването на задълженията, предвидени в настоящата директива, от страна на този субект. Държавите членки гарантират, че тези физически лица могат да бъдат подвеждани под отговорност за неизпълнението на своите задължения да осигурят спазването на задълженията, предвидени в настоящата директива. **Що се отнася до органите на публичната администрация, настоящата разпоредба не засяга законите на държавите членки по отношение на отговорността на държавните служители и на избраните и назначените длъжностни лица.**

7. При предприемане на действията по правоприлагане или прилагане на санкции съгласно параграфи 4 и 5 компетентните органи се съобразяват с правата на защита и отчитат обстоятелствата по всеки отделен случай и, като минимум, вземат предвид:

   а) сериозността на нарушението и значимостта на нарушените разпоредби. Сред нарушенията, които следва да се смятат за сериозни: повторни нарушения, неуведомяване или несправяне с инциденти със значително смущаващо въздействие, неотстраняване на недостатъци съгласно обвързващи указания от компетентните органи, възпрепятстване на одити или дейности по мониторинг от компетентния орган след констатация на нарушение, предоставяне на невярна или грубо неточна информация във връзка с изискванията за управление на риска или задълженията за докладване по членове 18 и 20.

б) продължителността на нарушението, включително елемента на повторни нарушения;

в) причинената действителна вреда, или възникналите загуби, или потенциалната вреда, която е можело да възникне, доколкото могат да бъдат определени. При оценката на този аспект се вземат предвид, наред с друго, действителните или потенциалните икономически загуби, въздействия върху други услуги, броят на засегнатите или потенциалните потребители;

г) дали нарушението е извършено умишлено или по небрежност;

д) предприетите от субекта мерки за предотвратяване или ограничаване на вредите и/или загубите;

е) придържането към одобрени кодекси на поведение или одобрени механизми за сертифициране;

ж) равнището на съдействие, което носещото отговорност физическо или юридическо лице или лица оказват на компетентните органи.

8. Компетентните органи излагат подробни мотиви за своите решения по правоприлагането. Преди вземането на такива решения компетентните органи уведомяват засегнатите субекти за своите предварителни констатации и предоставят разумен срок на тези субекти да представят становище, **с изключение на случаите на непосредствена опасност**.

9. Държавите членки гарантират, че техните компетентни органи **съгласно настоящата директива** уведомяват съответните компетентни органи **в същата тази** държава членка […], определени съгласно Директива (ЕС) XXXX/XXXX [Директива относно устойчивостта на критичните субекти], когато упражняват своите правомощия по надзор и правоприлагане, имащи за цел да гарантират изпълнението на задълженията съгласно настоящата директива от съществен субект, определен като критичен или като субект, равностоен на критичен субект, съгласно Директива (ЕС) XXXX/XXXX [Директива относно устойчивостта на критичните субекти]. **Когато е целесъобразно**, […] компетентните органи съгласно Директива (ЕС) XXXX/XXXX [Директивата относно устойчивостта на критичните субекти] […] **могат да поискат** от компетентните органи **съгласно настоящата директива да** упражнят своите надзорни и правоприлагащи **правомощия по отношение на** съществен субект, попадащ в обхвата на настоящата директива, който е идентифициран и като критичен [или еквивалентно] **съгласно Директива (ЕС) XXXX/XXXX [Директивата относно устойчивостта на критичните субекти].**

10. Държавите членки гарантират, че техните компетентни органи съгласно настоящата директива информират Форума за надзор съгласно член 29, параграф 1 от Регламент (ЕС) XXXX/XXXX [Регламента за ОУЦТ], когато упражняват своите надзорни и правоприлагащи правомощия, насочени към гарантиране на спазването на задълженията съгласно настоящата директива от страна на съществен субект, определен като критичен доставчик на ИКТ от трета страна съгласно член 28 от Регламент (ЕС) XXXX/XXXX [Регламента за ОУЦТ].

10а. Държавите членки гарантират, че техните компетентни органи съгласно настоящата директива информират съответните компетентни органи, определени съгласно Регламент (ЕС) № 910/2014, когато упражняват своите надзорни и правоприлагащи правомощия, насочени към гарантиране на спазването на задълженията по настоящата директива от страна на субект, определен като доставчик на удостоверителни услуги съгласно Регламент (ЕС) № 910/2014.

Член 30

Надзор и правоприлагане за значимите субекти

1. Когато разполагат с доказателства, индикации **или информация**, че значим субект **вероятно** не изпълнява задълженията по настоящата директива, и по-специално по членове 18 и 20, държавите членки гарантират, че компетентните органи предприемат действия, при необходимост, посредством последващи мерки за надзор.

2. Държавите членки гарантират, че когато изпълняват своите задачи по надзора във връзка със значимите субекти, компетентните органи **следват основан на риска подход и** са упълномощени подлагат тези субекти **най-малко** на:

   а) проверки на място и последващ дистанционен надзор;

   б) целеви одити на сигурността въз основа на оценки на риска или свързана с риска налична информация;

   в) проверки за сигурност, основани на обективни, **недискриминационни**, справедливи и прозрачни критерии за оценка на риска, **когато това е необходимо по технически причини, със съдействието на съответния субект**;

   г) искания за информация, необходима за последваща оценка на мерките за киберсигурност […];

   д) искания за достъп до данни, документи и/или всякаква информация, необходими за изпълнението на задачите по надзор;

   да) искания за доказателства за изпълнение на политиките в областта на киберсигурността, като например резултатите от одитите на сигурността, извършени от квалифициран одитор, и съответните подкрепящи доказателства.

2а. При изпълнението на надзорните си задачи, предвидени в параграф 2 от настоящия член, компетентните органи могат да установят надзорни методологии, които дават възможност за приоритизиране на тези задачи, следвайки основан на риска подход.

3. При упражняване на своите правомощия по параграф 2, букви г) – **да)** компетентните органи заявяват целта на своето искане и пояснят исканата информация.

4. Държавите членки гарантират, че в рамките на своите правомощия по правоприлагане във връзка със значимите субекти компетентните органи са упълномощени **най-малкото**:

а) да издават предупреждения при неизпълнение на задълженията по настоящата директива от субектите;

б) да изискват посредством обвързващи указания или разпореждане от тези субекти да поправят установените пропуски или нарушението на задълженията по настоящата директива;

в) да разпореждат на тези субекти да преустановяват поведение, което не е в съответствие със задълженията по настоящата директива и да се въздържат от повтарянето на такова поведение;

г) да разпореждат на тези субекти да привеждат своите мерки за управление на риска или задължения за докладване в съответствие със задълженията по членове 18 и 20 по конкретизиран начин и в рамките на посочен период;

д) да разпореждат на тези субекти да уведомяват физическото или юридическото лице или лица, на които предоставят услуги или дейности, потенциално засегнати от значителна киберзаплаха, **за естеството на заплахата, както и** за възможните защитни или коригиращи мерки, които могат да бъдат предприети от това физическо или юридическо лице или лица в отговор на тази заплаха;

е) да разпореждат на тези субекти да изпълняват препоръките, предвидени в резултат на одит на сигурността в рамките на разумен срок;

ж) да разпореждат на тези субекти да оповестяват по определен начин аспектите на неспазване от тяхна страна на задълженията, предвидени в настоящата директива, **когато такова публично оповестяване не води до вредна експозиция на съответния субект**;

з) [...]

и) да налагат или изискват налагането от съответните органи или съдилища съгласно националното право на административна глоба по член 31 в допълнение към или вместо мерките по букви а) – з) от настоящия параграф, в зависимост от обстоятелствата по всеки отделен случай.

5. Член 29, параграфи 6—8 се прилагат и за мерките по надзор и правоприлагане, предвидени в настоящия член за значимите субекти […].

Член 31

Общи условия за налагане на административни глоби на съществените и значимите субекти

1. Държавите членки гарантират, че налагането на административни глоби на съществените и значимите субекти съгласно настоящия член по отношение на нарушения на задълженията, предвидени в настоящата директива, за всеки отделен случай е ефективно, пропорционално и възпиращо.

2. В зависимост от обстоятелствата във всеки конкретен случай административните глоби се налагат в допълнение към или вместо мерките, посочени в член 29, параграф 4, букви а)—и), член 29, параграф 5, и член 30, параграф 4, букви а)—з).

3. Когато се взема решение дали да бъде наложена административна глоба и се определя нейният размер, във всеки конкретен случай надлежно се разглеждат най-малко елементите, предвидени в член 29, параграф 7.

4. Държавите членки гарантират, че нарушенията **от страна на съществени субекти** на задълженията по член 18 или член 20, в съответствие с параграфи 2 и 3 от настоящия член, подлежат на максимални административни глоби от поне […] **4** 000 000 EUR или – **за физически лица** – на 2% от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи съществения […] субект, която от двете стойности е по-висока.

4а. Държавите членки гарантират, че нарушенията от страна на значими субекти на задълженията по член 18 или член 20, в съответствие с параграфи 2 и 3 от настоящия член, подлежат на максимални административни глоби от поне 2 000 000 EUR или – за физически лица – на 1% от общия световен годишен оборот за предходната финансова година на предприятието, към което принадлежи значимият субект, която от двете стойности е по-висока.

5. Държавите членки може да предвидят правомощие за налагане на периодични наказателни плащания с цел принуждаване на съществен или значим субект да преустанови нарушение в съответствие с предходно решение на компетентния орган.

6. Без да се засягат правомощията на компетентните органи по членове 29 и 30, всяка държава членка може да установи правилата за това дали и в каква степен административните глоби могат да бъдат налагани на органи на публичната администрация по член 4, параграф 23, които са обект на задълженията, предвидени в настоящата директива.

(6а) Когато в правната система на държавата членка не са предвидени административни наказания „глоба“, държавите членки гарантират, че настоящият член може да се прилага по такъв начин, че глобата да се инициира от компетентния орган и да се налага от компетентните национални съдилища, като в същото време се гарантира, че тези правни средства за защита са ефективни и имат ефект, равностоен на административните наказания „глоба“, налагани от компетентните органи. Във всички случаи наложените глоби са ефективни, пропорционални и възпиращи. Въпросните държави членки уведомяват Комисията за разпоредбите в своето право, които приемат съгласно настоящия параграф, до […], и я информират незабавно за всеки последващ закон за изменение или за всяко изменение, които ги засягат.

Член 32

Нарушения, водещи до нарушаване на сигурността на лични данни

1. Когато **в хода на надзора или правоприлагането** компетентните органи […] **разберат**, че нарушението на задълженията по членове 18 и 20 **от настоящата директива** от страна на съществен или значим субект води до нарушаване на сигурността на лични данни съгласно определеното в член 4, параграф 12 от Регламент (ЕС) 2016/679, за което трябва да се изпрати уведомление съгласно член 33 от посочения регламент, те **без излишно забавяне** уведомяват надзорните органи, компетентни съгласно членове 55 и 56 от същия регламент […].

2. Когато надзорните орани, компетентни съгласно членове 55 и 56 от Регламент (ЕС) 2016/679, решат да упражнят правомощията си по член 58, **параграф 2,** буква и) от същия регламент и да наложат административна глоба, компетентните органи, **посочени в член 8 от настоящата директива,** не налагат административна глоба за […] **същото нарушение** съгласно член 31 от настоящата директива. Компетентните органи могат обаче да предприемат правоприлагащи действия или да упражнят правомощията по санкциониране, предвидени в член 29, параграф 4, букви а)—и), член 29, параграф 5, и член 30, параграф 4, букви а)—з) от настоящата директива.

3. Когато надзорният орган, компетентен съгласно Регламент (ЕС) 2016/679, е установен в държава членка, различна от тази на компетентния орган, компетентният орган може да уведоми надзорния орган, установен в същата държава членка.

Член 33

Санкции

1. Държавите членки установяват правилата за налагане на санкции, приложими при нарушение на националните разпоредби, приети съгласно настоящата директива, и вземат всички необходими мерки за осигуряване на тяхното прилагане. Предвидените наказания трябва да бъдат ефективни, пропорционални и възпиращи.

2. Най-късно до [две] години от влизането в сила на настоящата директива държавите членки съобщават на Комисията тези правила и мерки и ѝ съобщават незабавно всички последващи техни изменения.

Член 34

Взаимопомощ

1. Когато съществен или значим субект предоставя услуги в повече от една държава членка или […] **предоставя услуги** в **една или повече** държави членки, но неговите мрежи и информационни системи са разположени в една или повече други държави членки, компетентните органи на **въпросните** държав**и** членк**и** […]си сътрудничат и се подпомагат взаимно, ако е необходимо. Това сътрудничество включва най-малко следното:

а) компетентните органи, прилагащи мерки по надзор или правоприлагане в държава членка, посредством единното звено за контакт, уведомяват и се консултират с компетентните органи в останалите засегнати държави членки относно взетите мерки за надзор и правоприлагане;

б) компетентен орган може да поиска от друг компетентен орган да предприеме мерки за надзор или правоприлагане;

в) когато компетентен орган получи обосновано искане от друг компетентен орган, той оказва на искащия орган помощ, която е **пропорционална на ресурсите, с които разполага**, така че действията по надзор или правоприлагане […] да могат да бъдат приложени по ефективен, ефикасен и последователен начин. Тази взаимопомощ може да обхваща искания за информация и мерки по надзор, включително искания за провеждане на проверки на място или дистанционен надзор, или целеви одити на сигурността. Компетентен орган, към който е отправено искане за помощ, не може да откаже това искане, освен ако след обмен на информация с останалите засегнати органи […] не бъде установено, че […] органът не е компетентен да предостави исканата помощ **или няма необходимите ресурси**, или поисканата помощ не е пропорционална на изпълняваните […] от компетентния орган задачи за надзор, **или искането засяга информация или предполага дейности, които противоречат на националната сигурност, обществения ред или отбраната на въпросната държава членка**.

2. Когато е подходящо и при общо съгласие компетентните органи от различни държави членки може да извършват общите действия по надзор.

ГЛАВА VII

Преходни и заключителни разпоредби

Член 35

Преглед

Комисията периодично прави преглед на действието на настоящата директива и докладва на Европейския парламент и на Съвета. В доклада по-специално се прави оценка на относимостта на секторите, подсекторите, размера и вида на субектите, посочени в приложения I и II, за функционирането на икономиката и обществото във връзка с киберсигурността. За […] целите на **прегледа** […]Комисията взема предвид докладите на […]мрежата на ЕРИКС за натрупания опит на […] оперативно равнище. Първият доклад се представя до …[54 месеца след датата на влизане в сила на настоящата директива].

Член 36

[...]

[...]

[...]

Член 37

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 от Регламент (ЕС) № 182/2011.

3. Когато становището на комитета трябва да бъде получено по писмена процедура, тази процедура се прекратява без резултат, ако в рамките на срока за даване на становище председателят на комитета вземе такова решение или член на комитета отправи такова искане.

Член 38

Транспониране

1. Държавите членки приемат и публикуват до […] **24** месеца след влизане в сила на настоящата директива законовите, подзаконовите и административните разпоредби, необходими за да се съобразят с настоящата директива. Те незабавно информират Комисията за това. Те прилагат тези мерки, считано от … [един ден след датата, посочена в първа алинея].

2. Когато държавите членки приемат тези разпоредби, в тях се съдържа позоваване на настоящата директива или то се извършва при официалното им публикуване. Условията и редът на позоваване се определят от държавите членки.

Член 39

Изменение на Регламент (ЕС) № 910/2014

В Регламент (ЕС) № 910/2014 член 19 се заличава, считано от ... [датата на крайния срок за транспониране на настоящата директива].

Член 40

Изменение на Директива (ЕС) 2018/1972

В Директива (ЕС) 2018/1972 членове 40 и 41 […] се заличават, **считано от ... [датата на крайния срок за транспониране на настоящата директива]**.

Член 41

Отмяна

Директива (ЕС) 2016/1148 се отменя, считано от ... [датата на крайния срок за транспониране на настоящата директива].

Позоваванията на Директива (ЕС) 2016/1148 се считат за позовавания на настоящата директива и се четат в съответствие с таблицата на съответствието в приложение II.

Член 42

Влизане в сила

Настоящата директива влиза в сила на двадесетия ден след публикуването ѝ в *Официален вестник на Европейския съюз*.

Член 43

Адресати

Адресати на настоящата директива са държавите членки.

Съставено в Брюксел на […] година.

За Европейския парламент	*За Съвета*
Председател	*Председател*

ПРИЛОЖЕНИЕ I

СЕКТОРИ, ПОДСЕКТОРИ И ВИДОВЕ СУБЕКТИ

Сектор	Подсектор	Вид субект
1. Енергетика	а) Електроенергия	— Електроенергийни предприятия, посочени в член 2, точка 57 от Директива (ЕС) 2019/944, които осъществяват „доставките“, посочени в член 2, точка 12 от същата директива ([39])
		— Оператори на разпределителни системи, посочени в член 2, точка 29 от Директива (ЕС) 2019/944
		— Оператори на преносни системи, посочени в член 2, точка 35 от Директива (ЕС) 2019/944
		— Производители, посочени в член 2, точка 38 от Директива (ЕС) 2019/944
		— Номинирани оператори на пазара на електроенергия, посочени в член 2, точка 8 от Регламент (ЕС) 2019/943 ([40])
		— Участници на пазара на електроенергия, посочени в член 2, точка 25 от Регламент (ЕС) 2019/943, предоставящи услуги за агрегиране, оптимизация на потреблението или съхраняване на енергия, посочени в член 2, точки 18, 20 и 59 от Директива (ЕС) 2019/944
	б) Районно отопление и	— Районни отоплителни системи или районни охладителни

[39] Директива (ЕС) 2019/944 на Европейския парламент и на Съвета от 5 юни 2019 година относно общите правила за вътрешния пазар на електроенергия и за изменение на Директива 2012/27/ЕС (ОВ L 158, 14.6.2019 г., стр. 125).

[40] Регламент (ЕС) 2019/943 на Европейския парламент и на Съвета от 5 юни 2019 година относно вътрешния пазар на електроенергия (ОВ L 158, 14.6.2019 г., стр. 54).

	охлаждане	системи, посочени в член 2, точка 19 от Директива (ЕС) 2018/2001 ([41]) за насърчаване използването на енергия от възобновяеми източници
	в) Нефт	— Оператори на нефтопроводи
		— Оператори на съоръжения за добив, рафиниране и преработка, съхранение и пренос на нефт
		— Централни структури за управление на запасите от нефт, посочени в член 2, буква е) от Директива 2009/119/ЕО на Съвета ([42])
	г) Природен газ	— Предприятия за доставка, посочени в член 2, точка 8 от Директива 2009/73/ЕО ([43])
		— Оператори на газоразпределителни системи, посочени в член 2, точка 6 от Директива 2009/73/ЕО
		— Оператори на газопреносни системи, посочени в член 2, точка 4 от Директива 2009/73/ЕО
		— Оператори на системи за съхранение, посочени в член 2, точка 10 от Директива 2009/73/ЕО
		— Оператори на системи за ВПГ, посочени в член 2, точка 12 от Директива 2009/73/ЕО

41 Директива (ЕС) 2018/2001 на Европейския парламент и на Съвета от 11 декември 2018 година за насърчаване използването на енергия от възобновяеми източници (ОВ L 328, 21.12.2018 г., стр. 82).

42 Директива на Съвета 2009/119/ЕО от 14 септември 2009 година за налагане на задължение на държавите-членки да поддържат минимални запаси от суров нефт и/или нефтопродукти (ОВ L 265, 9.10.2009 г., стр. 9).

43 Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 година относно общите правила за вътрешния пазар на природен газ и за отмяна на Директива 2003/55/ЕО (ОВ L 211, 14.8.2009 г., стр. 94).

		— Предприятия за природен газ, посочени в член 2, точка 1 от Директива 2009/73/ЕО
		— Оператори на съоръжения за рафиниране и преработка на природен газ
	в) Водород	Оператори в областта на производството, съхранението и преноса на водород
2. Транспорт	а) Въздушен	— Въздушни превозвачи, посочени в член 3, точка 4 от Регламент (ЕО) № 300/2008 ([44]), **използвани за търговски цели**
		— Управляващи летища органи, посочени в член 2, точка 2 от Директива № 2009/12/ЕО ([45]), летища, посочени в член 2, точка 1 от същата директива, включително основните летища, изброени в раздел 2 от приложение II към Регламент (ЕС) № 1315/2013 ([46]), и субекти, експлоатиращи спомагателни инсталации, намиращи се на летищата
		— Оператори по управление на въздушното движение, предоставящи обслужване по контрол на въздушното движение

[44] Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета от 11 март 2008 година относно общите правила в областта на сигурността на гражданското въздухоплаване и за отмяна на Регламент (ЕО) № 2320/2002 (ОВ L 97, 9.4.2008 г., стр. 72).

[45] Директива 2009/12/ЕО на Европейския парламент и на Съвета от 11 март 2009 година относно летищните такси (ОВ L 70, 14.3.2009 г., стр. 11).

[46] Регламент (ЕО) № 1315/2013 на Европейския парламент и на Съвета от 11 декември 2013 година относно насоките на Съюза за развитието на трансевропейската транспортна мрежа и за отмяна на Решение № 661/2010/ЕС (ОВ L 348, 20.12.2013 г., стр. 1).

		(КВД), посочено в член 2, точка 1 от Регламент (ЕО) № 549/2004 ([47])
	б) Железопътен	— Управители на инфраструктура, посочени в член 3, точка 2 от Директива 2012/34/ЕС ([48])
		— Железопътни предприятия, посочени в член 3, точка 1 от Директива 2012/34/ЕС, включително оператори на обслужващи съоръжения, посочени в член 3, точка 12 от Директива 2012/34/ЕС
	в) Воден	— Дружества за вътрешен, морски и крайбрежен пътнически и товарен воден транспорт, посочени за морския транспорт в приложение I към Регламент (ЕО) № 725/2004 ([49]), с изключение на отделните плавателни съдове, експлоатирани от тези дружества
		— Управителни органи на пристанищата, посочени в член 3, точка 1 от Директива 2005/65/ЕО ([50]), включително техните пристанищни съоръжения, посочени в член 2, точка 11 от Регламент (ЕО) № 725/2004, и субекти, извършващи строителни работи и експлоатиращи оборудване на територията на пристанищата

[47] Регламент (ЕО) № 549/2004 на Европейския парламент и на Съвета от 10 март 2004 година за определяне на рамката за създаването на Единно европейско небе (рамков регламент) (ОВ L 96, 31.3.2004 г., стр. 1).

[48] Директива 2012/34/ЕС на Европейския парламент и на Съвета от 21 ноември 2012 година за създаване на единно европейско железопътно пространство (ОВ L 343, 14.12.2012 г., стр. 32).

[49] Регламент (ЕО) № 725/2004 на Европейския парламент и на Съвета от 31 март 2004 година относно подобряване на сигурността на корабите и на пристанищните съоръжения (ОВ L 129, 29.4.2004 г., стр. 6).

[50] Директива 2005/65/ЕО на Европейския парламент и на Съвета от 26 октомври 2005 година за повишаване на сигурността на пристанищата (ОВ L 310, 25.11.2005 г., стр. 28).

		— Оператори на служби по морския трафик, посочени в член 3, буква о) от Директива 2002/59/ЕО ([51])
	г) Автомобилен	— Пътните органи, посочени в член 2, точка 12 от Делегиран регламент (ЕС) 2015/962 на Комисията ([52]), отговарящи за контрола на управлението на трафика, **с изключение на публичните субекти, за които управлението на трафика или операторите на интелигентни транспортни системи са само несъществена част от общата им дейност**
		— Оператори на интелигентни транспортни системи, посочени в член 4, точка 1 от Директива 2010/40/ЕС ([53])
3. Банков сектор		— Кредитни институции, посочени в член 4, точка 1 от Регламент (ЕС) № 575/2013([54]) **[с изключение на посочените в член 2, параграф 5, точка 8 от Директива 2013/36/ЕС, които са освободени в съответствие с член 2, параграф 4 от Регламент XX [DORA]]**

[51] Директива 2002/59/ЕО на Европейския парламент и на Съвета от 27 юни 2002 година за създаване на система на Общността за контрол на движението на корабите и за информация и отменяща Директива 93/75/ЕИО на Съвета (ОВ L 208, 5.8.2002 г., стр. 10)

[52] Делегиран регламент (ЕС) 2015/962 на Комисията от 18 декември 2014 година за допълване на Директива 2010/40/ЕС на Европейския парламент и на Съвета по отношение на предоставянето в целия ЕС на информационни услуги в реално време за движението по пътищата (ОВ L 157, 23.6.2015 г., стр. 21).

[53] Директива 2010/40/ЕС на Европейския парламент и на Съвета от 7 юли 2010 година относно рамката за внедряване на интелигентните транспортни системи в областта на автомобилния транспорт и за интерфейси с останалите видове транспорт (ОВ L 207, 6.8.2010 г., стр. 1).

[54] Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета от 26 юни 2013 година относно пруденциалните изисквания за кредитните институции и инвестиционните посредници и за изменение на Регламент (ЕС) № 648/2012 (ОВ L 176, 27.6.2013 г., стр. 1).

4. Инфраструктури на финансовия пазар		— Оператори на места на търговия, посочени в член 4, точка 24 от Директива 2014/65/ЕС ([55])
		— Централни контрагенти (ЦК), посочени в член 2, точка 1 от Регламент (ЕС) № 648/2012 ([56])
5. Здравеопазване		— Доставчици на здравно обслужване, посочени в член 3, буква ж) от Директива 2011/24/ЕС ([57])
		— Референтни лаборатории на ЕС, посочени в член 15 от Регламент XXXX/XXXX относно сериозните трансгранични здравни заплахи[58]
		— Субекти, извършващи научноизследователска и развойна дейност в областта на лекарствените продукти, посочени в член 1, точка 2 от Директива 2001/83/ЕО ([59]) — Субекти, произвеждащи основни фармацевтични продукти и препарати, посочени в раздел B, разделение 21 на NACE Rev. 2 — Субекти, произвеждащи медицински изделия, които се

[55] Директива 2014/65/ЕС на Европейския парламент и на Съвета от 15 май 2014 г. относно пазарите на финансови инструменти и за изменение на Директива 2002/92/ЕО и на Директива 2011/61/ЕС (ОВ L 173, 12.6.2014 г., стр. 349).

[56] Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета от 4 юли 2012 г. относно извънборсовите деривати, централните контрагенти и регистрите на транзакции (ОВ L 201, 27.7.2012 г., стр. 1).

[57] Директива 2011/24/ЕС на Европейския парламент и на Съвета от 9 март 2011 г. за упражняване на правата на пациентите при трансгранично здравно обслужване (ОВ L 88, 4.4.2011 г., стр. 45).

[58] [Регламент на Европейския парламент и на Съвета относно сериозните трансгранични здравни заплахи и за отмяна на Решение 1082/2013/ЕС; да се актуализира позоваването, след като предложението COM (2020)727 final бъде прието].

[59] Директива 2001/83/ЕО на Европейския парламент и на Съвета от 6 ноември 2001 г. за утвърждаване на кодекс на Общността относно лекарствени продукти за хуманна употреба (ОВ L 311, 28.11.2001 г., стр. 67).

		считат за критично важни при извънредни ситуации в областта на общественото здраве („списък на критично важните медицински изделия при извънредни ситуации в областта на общественото здраве“), посочени в член 20 от Регламент XXXX[60]
6. Питейна вода		Доставчици и дистрибутори на води, предназначени за консумация от човека, посочени в член 2, точка (1), буква а) от Директива 98/83/ЕО на Съвета([61]), с изключение на дистрибуторите, за които дистрибуцията на вода за консумация от човека е само **несъществена** част от общата им дейност по дистрибуция на други стоки и стоки [...]
7. Отпадъчни води		Предприятия, които събират, обезвреждат или пречистват градски, битови и промишлени отпадъчни води, посочени в член 2, точки 1—3 от Директива 91/271/ЕИО на Съвета ([62]), **но с изключение на предприятията, за които събирането, обезвреждането или пречистването на градски, битови и промишлени отпадъчни води е само несъществена част от тяхната обща дейност** [...]
8. Цифрова инфраструктура		— Доставчици на точки за обмен в интернет
		— Доставчици на DNS услуги, **с изключение на оператори на**

60 [Регламент на Европейския парламент и на Съвета относно засилена роля на Европейската агенция по лекарствата в готовността за действия при кризи и управлението на кризи по отношение на лекарствените продукти и медицинските изделия; да се актуализира позоваването, след като предложението COM (2020)725 final бъде прието].

61 Директива 98/83/ЕО на Съвета от 3 ноември 1998 година относно качеството на водите, предназначени за консумация от човека (ОВ L 330, 5.12.1998 г., стр. 32).

62 Директива 91/271/ЕИО на Съвета от 21 май 1991 г. относно пречистването на градските отпадъчни води (ОВ L 135, 30.5.1991 г., стр. 40).

		коренови сървъри за имена
		— Регистри на имената на домейни от първо ниво
		Доставчици на услуги за изчисления в облак
		Доставчици на услуги на центрове за данни
		Доставчици на мрежи за доставка на съдържание
		— Доставчици на удостоверителни услуги, посочени в член 3, точка 19 от Регламент (ЕС) № 910/2014 ([63])
		— Доставчици на обществени електронни съобщителни мрежи, посочени в член 2, точка 8 от Директива (ЕС) 2018/1972 ([64]) или доставчици на електронни съобщителни услуги, посочени в член 2, точка 4 от Директива (ЕС) 2018/1972, когато техните услуги са обществено достъпни
8.a Управление на ИКТ услуги **(B2B)**		— **Доставчици на управлявани услуги (ДУУ)** — **Доставчици на услуги по управление на сигурността (MSSP)**

[63] Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета от 23 юли 2014 г. относно електронната идентификация и удостоверителните услуги при електронни трансакции на вътрешния пазар и за отмяна на Директива 1999/93/ЕО (ОВ L 257, 28.8.2014 г., стр. 73).

[64] Директива (ЕС) 2018/1972 на Европейския парламент и на Съвета от 11 декември 2018 г. за установяване на Европейски кодекс за електронни съобщения (ОВ L 321, 17.12.2018 г., стр. 36).

9. Реформа на **субектите на** публичната администрация		— Субекти на публичната администрация на централни правителства , **определени от държава членка в съответствие с националното право** — [...][65][...] — [...]
10. Космическо пространство		— Оператори на наземна инфраструктура, притежавани, управлявани и експлоатирани от държавите членки или от частни лица, които подпомагат предоставянето на космически услуги, с изключение на доставчиците на обществени електронни съобщителни мрежи, посочени в член 2, точка 8 от Директива (ЕС) 2018/1972

[65] [...]

ПРИЛОЖЕНИЕ II

СЕКТОРИ, ПОДСЕКТОРИ И ВИДОВЕ СУБЕКТИ

Сектор	Подсектор	Вид субект
1. Пощенски и куриерски услуги		Доставчици на пощенски услуги, посочени в член 2, точка 1 от Директива 97/67/ЕО ([66]), **включително** [...] доставчици на куриерски услуги
2. Управление на отпадъците		Предприятия, извършващи управление на отпадъците, посочени в член 3, точка 9 от Директива 2008/98/ЕО ([67]), с изключение на предприятия, за които управлението на отпадъците не е основна икономическа дейност

[66] Директива 97/67/ЕО на Европейския парламент и на Съвета от 15 декември 1997 г. относно общите правила за развитието на вътрешния пазар на пощенските услуги в Общността и за подобряването на качеството на услугата (ОВ L 15, 21.1.1998 г., стр. 14), **изменена с Директива 2008/6/ЕО на Европейския парламент и на Съвета от 20 февруари 2008 г. за изменение на Директива 97/67/ЕО относно по-нататъшното отваряне на пощенските услуги в Общността за конкуренция (ОВ L 52, 27.2.2008 г., стр. 3)**

[67] Директива 2008/98/ЕО на Европейския парламент и на Съвета от 19 ноември 2008 г. относно отпадъците и за отмяна на някои директиви (ОВ L 312, 22.11.2008 г., стр. 3).

3. Производство на изделия, производство и дистрибуция на химикали		Предприятия, извършващи производство [...] на вещества и [...] **смеси**, посочени в член 3, точки [...] 9 и 14 от Регламент (ЕО) № 1907/2006 ([68]), **и предприятия, извършващи производство на изделия, посочени в член 3, точка 3 от същия регламент, от вещества или смеси.**
4. Производство, преработка и разпространение на храни		Предприятия за храни, посочени в член 3, точка 2 от Регламент (ЕО) № 178/2002 ([69]), **които се занимават с дистрибуция на едро и промишлено производство и преработка**
5. Производство	а) Производство на медицински изделия и медицински изделия за инвитро диагностика	Субекти, произвеждащи медицински изделия, посочени в член 2, точка 1 от Регламент (ЕС) 2017/745([70]), и субекти, произвеждащи медицински изделия за инвитро диагностика, посочени в член 2, точка 2 от Регламент (ЕС) 2017/746([71]), с

68 Регламент (ЕО) № 1907/2006 на Европейския парламент и на Съвета от 18 декември 2006 г. относно регистрацията, оценката, разрешаването и ограничаването на химикали (REACH), за създаване на Европейска агенция по химикали, за изменение на Директива 1999/45/ЕО и за отмяна на Регламент (ЕИО) № 793/93 на Съвета и Регламент (ЕО) № 1488/94 на Комисията, както и на Директива 76/769/ЕИО на Съвета и директиви 91/155/ЕИО, 93/67/ЕИО, 93/105/ЕО и 2000/21/ЕО на Комисията (ОВ L 396, 30.12.2006 г., стр. 1).

69 Регламент (ЕО) № 178/2002 на Европейския парламент и на Съвета от 28 януари 2002 г. за установяване на общите принципи и изисквания на законодателството в областта на храните, за създаване на Европейски орган за безопасност на храните и за определяне на процедури относно безопасността на храните (ОВ L 31, 1.2.2002 г., стр. 1.)

70 Регламент (ЕС) 2017/745 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия, за изменение на Директива 2001/83/ЕО, Регламент (ЕО) № 178/2002 и Регламент (ЕО) № 1223/2009 и за отмяна на директиви 90/385/ЕИО и 93/42/ЕИО на Съвета (ОВ L 117, 5.5.2017 г., стр. 1).

71 Регламент (ЕС) 2017/746 на Европейския парламент и на Съвета от 5 април 2017 г. за медицинските изделия за инвитро диагностика и за отмяна на Директива 98/79/ЕО и Решение 2010/227/ЕС на Комисията (ОВ L 117, 5.5.2017 г., стр. 176).

		изключение на субектите, произвеждащи медицински изделия, посочени в приложение 1, точка 5.
	б) Производство на компютри, електронни и оптични продукти	Предприятия, извършващи някоя от икономическите дейности, посочени в раздел B, разделение 26 на NACE Rev. 2
	в) Производство на електрически съоръжения	Предприятия, извършващи някоя от икономическите дейности, посочени в раздел B, разделение 27 на NACE Rev. 2
	г) Производство на машини и оборудване, некласифицирани другаде	Предприятия, извършващи някоя от икономическите дейности, посочени в раздел B, разделение 28 на NACE Rev. 2
	д) Производство на моторни превозни средства, ремаркета и полуремаркета	Предприятия, извършващи някоя от икономическите дейности, посочени в раздел B, разделение 29 на NACE Rev. 2
	е) Производство на друго транспортно оборудване	Предприятия, извършващи някоя от икономическите дейности, посочени в раздел B, разделение 30 на NACE Rev. 2
6. Доставчици на цифрови услуги		— Доставчици на онлайн места за търговия
		— Доставчици на онлайн търсачки
		— Доставчици на платформи за услуги на социални мрежи