Съвет на
Европейския съюз

Брюксел, 17 май 2016 г.
(OR. en)

5581/1/16
REV 1

Междуинституционално досие:
2013/0027 (COD)

TELECOM 7
DATAPROTECT 6
CYBER 4
MI 37
CSC 15
CODEC 84
PARLNAT 154

ЗАКОНОДАТЕЛНИ АКТОВЕ И ДРУГИ ПРАВНИ ИНСТРУМЕНТИ

Относно:	Позиция на Съвета на първо четене с оглед приемането на ДИРЕКТИВА НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза - Приета от Съвета на 17 май 2016 г.

ДИРЕКТИВА (ЕС) 2016/…
НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ И НА СЪВЕТА

от ...

относно мерки за високо общо ниво на сигурност на мрежите и информационните системи в Съюза

ЕВРОПЕЙСКИЯТ ПАРЛАМЕНТ И СЪВЕТЪТ НА ЕВРОПЕЙСКИЯ СЪЮЗ,

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

като взеха предвид предложението на Европейската комисия,

след предаване на проекта на законодателния акт на националните парламенти,

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

в съответствие с обикновената законодателна процедура[2],

[1] ОВ С 271, 19.9.2013 г., стр. 133.

[2] Позиция на Европейския парламент от 13 март 2014 г. (все още непубликувана в Официален вестник) и позиция на Съвета на първо четене от 17 май 2016 г. (все още непубликувана в Официален вестник). Позиция на Европейския парламент от … (все още непубликувана в Официален вестник).

като имат предвид, че:

(1) Мрежите и информационните системи и услуги имат изключително важна роля в обществото. Тяхната надеждност и сигурност са от основно значение за стопанските и обществените дейности и особено за функционирането на вътрешния пазар.

(2) Мащабите, честотата и въздействието на свързаните със сигурността инциденти се увеличават и представляват крупна заплаха за функционирането на мрежите и информационните системи. Тези системи могат също така да се превърнат в мишена за преднамерени злонамерени действия, имащи за цел да повредят системите или да прекъснат тяхната работа. Подобни инциденти могат да попречат на извършването на стопански дейности, да причинят значителни финансови загуби, да подкопаят доверието на потребителите и да причинят големи вреди на икономиката на Съюза.

(3) Мрежите и информационните системи, и най-вече интернет, са от основно значение за улесняването на трансграничното движение на стоки, услуги и хора. Поради транснационалния им характер всяко съществено нарушение на тези системи, било то умишлено или неволно и без значение на кое място се извършва, може да засегне отделни държави членки, а и целия Съюз. Ето защо сигурността на мрежите и информационните системи е от основно значение за гладкото функциониране на вътрешния пазар.

(4) Като се използва значителният напредък, постигнат в рамките на Европейския форум за държавите членки, при насърчаването на дискусиите и обмена на добри практики в политиките, включително разработването на принципи на европейското сътрудничество при киберкризи, следва да бъде създадена група за сътрудничество, състояща се от представители на държавите членки, Комисията и Агенцията на Европейския съюз за мрежова и информационна сигурност (ENISA), която да улеснява и подкрепя стратегическото сътрудничество между държавите членки по отношение на сигурността на мрежите и информационни системи. За да бъде ефективна и приобщаваща тази група, е от основно значение всички държави членки да разполагат с минимален капацитет и със стратегия, гарантираща високо ниво на сигурност на мрежите и информационни системи на тяхна територия. Освен това към операторите на основни услуги и доставчиците на цифрови услуги следва да се прилагат изисквания за сигурност и уведомяване, с цел да се насърчи култура на управление на риска и да се гарантира докладването на най-сериозните инциденти.

(5) Съществуващите способности не са достатъчни, за да се гарантира високо ниво на сигурност на мрежите и информационни системи в Съюза. Нивото на подготвеност на различните държави членки е твърде различно, което води до разпокъсани действия в различните части на Съюза. Това от своя страна е причина нивото на защита на потребителите и предприятията да не е еднакво и подкопава общото ниво на сигурност на мрежите и информационни системи в Съюза. Липсата на общи изисквания за операторите на основни услуги и доставчиците на цифрови услуги на свой ред прави невъзможно създаването на глобален и ефективен механизъм за сътрудничество на равнището на Съюза. Университетите и изследователските центрове имат основно значение за насърчаване на научноизследователската и развойна дейност и иновациите в тези области.

(6) Поради това ефективният отговор на предизвикателствата пред сигурността на мрежите и информационните системи изисква глобален подход на равнището на Съюза, който да включва общи минимални изисквания за изграждане на капацитет и планиране, обмен на информация, сътрудничество и общи изисквания по отношение на сигурността за операторите на основни услуги и доставчиците на цифрови услуги. Допуска се обаче операторите на основни услуги и доставчиците на цифрови услуги да прилагат мерки за сигурност, които са по-строги от предвидените в настоящата директива.

(7) За да бъдат обхванати всички съответни инциденти и рискове, настоящата директива следва да се прилага както по отношение на операторите на основни услуги, така и на доставчиците на цифрови услуги. Въпреки това задълженията за операторите на основни услуги и доставчиците на цифрови услуги следва да не се прилагат по отношение на предприятия, предоставящи обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги по смисъла на Директива 2002/21/ЕО на Европейския парламент и на Съвета[1], към които се прилагат специалните изисквания за сигурност и цялост от същата директива, нито следва да се прилагат по отношение на доставчиците на удостоверителни услуги по смисъла на Регламент (ЕС) № 910/2014 на Европейския парламент и на Съвета[2], към които се прилагат изискванията за сигурност, предвидени в същия регламент.

---

1 Директива 2002/21/ЕО на Европейския парламент и на Съвета от 7 март 2002 г. относно общата регулаторна рамка за електронните съобщителни мрежи и услуги (Рамкова директива), (ОВ L 108, 24.4.2002 г., стр. 33).

2 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).

(8) Настоящата директива следва да не засяга възможността всяка държава членка да предприема необходимите мерки, с които да гарантира защитата на основните интереси на своята сигурност, да опазва обществения ред и обществената сигурност и да създава условия за разследването, разкриването и преследването на престъпления. В съответствие с член 346 от Договора за функционирането на Европейския съюз (ДФЕС) нито една държава членка не може да бъде задължавана да предоставя информация, чието разкриване тя счита за противоречащо на основните интереси на нейната сигурност. В този контекст имат значение Решение 2013/488/ЕС на Съвета[1] и споразуменията за неразкриване на информация или неформалните споразумения за неразкриване на информация, като протокола за обмен на информация с цветен код за поверителност (Traffic Light Protocol).

(9) Някои стопански сектори са вече регулирани или е възможно да бъдат регулирани в бъдеще посредством правни актове на Съюза, които са специални за конкретния сектор и които включват правила, свързани със сигурността на мрежите и информационните системи. Когато в тези правни актове на Съюза се съдържат разпоредби, налагащи изисквания за сигурност на мрежите и информационните системи или за уведомяването за инциденти, тези разпоредби следва да се прилагат, ако съдържат изисквания, които са най-малкото равностойни по действие на задълженията, съдържащи се в настоящата директива. В такъв случай държавите членки следва да прилагат разпоредбите на тези специални за конкретен сектор правни актове на Съюза, включително онези от тях, които се отнасят за юрисдикцията, и следва да не изпълняват процеса по определяне на операторите на основни услуги, определен в настоящата директива. В този контекст държавите членки следва да представят информация на Комисията относно прилагането на разпоредбите, имащи характера на *lex specialis*. При определяне дали изискванията за сигурност на мрежите и информационните системи и за уведомяване за инциденти, съдържащи се в специални за конкретен сектор правни актове на Съюза, са равностойни на изискванията по настоящата директива следва да се имат предвид единствено разпоредбите на приложимите правни актове на Съюза и тяхното приложение в държавите членки.

---

[1] Решение 2013/488/ЕС на Съвета от 23 септември 2013 г. относно правилата за сигурност за защита на класифицирана информация на ЕС (ОВ L 274, 15.10.2013 г., стр. 1).

(10) В сектора на водния транспорт изискванията за сигурност на дружества, кораби, пристанищни съоръжения, пристанища и услуги за корабния трафик, съобразени с правните актове на Съюза, обхващат всички операции, включително радио- и телекомуникационните системи, компютърните системи и мрежите. В част от задължителните процедури, които трябва да бъдат следвани, се включва докладването за всички инциденти, поради което тази част следва да се разглежда като *lex specialis*, доколкото посочените изисквания са най-малкото равностойни на съответните разпоредби на настоящата директива.

(11) При определянето на оператори в сектора на водния транспорт държавите членки следва да вземат предвид съществуващи и бъдещи международни кодекси и насоки, изготвени по-специално от Международната морска организация, с оглед осигуряване на съгласуван подход за отделните морски оператори.

(12) Регулирането и надзорът в секторите на банковото дело и инфраструктурите на финансовите пазари е с висока степен на хармонизация на равнището на Съюза, постигната чрез използването на първичното и вторичното право на Съюза и стандартите, разработени заедно с европейските надзорни органи. В рамките на банковия съюз прилагането и надзорът във връзка с тези изисквания се осигурява чрез единния надзорен механизъм. За държавите членки, които не са част от банковия съюз, това се осигурява от съответните банкови регулатори на държавите членки. В други области на регулиране на финансовия сектор Европейската система за финансов надзор също осигурява висока степен на уеднаквяване и сближаване на надзорните практики. Европейският орган за ценни книжа и пазари също изпълнява функции на пряк надзор за някои субекти, а именно агенциите за кредитен рейтинг и регистрите на транзакции.

(13) Операционният риск е важна част от пруденциалното регулиране и надзор в областта на банковото дело и инфраструктурите на финансовите пазари. Той обхваща всички операции, включително сигурността, целостта и устойчивостта на мрежите и информационните системи. Изискванията във връзка с тези системи, които често надхвърлят изискванията, предвидени в настоящата директива, са установени в редица правни актове на Съюза, включително: правилата относно достъпа до дейността на кредитните институции и относно пруденциалния надзор върху кредитните институции и инвестиционните посредници и правилата относно пруденциалните изисквания за кредитните институции и инвестиционните посредници, които включват изисквания относно операционния риск; правилата относно пазарите на финансови инструменти, които включват изисквания относно оценката на риска във връзка с инвестиционните посредници и регулираните пазари; правилата относно извънборсовите деривати, централните контрагенти и регистрите на транзакции, които включват изисквания за операционния риск във връзка с централните контрагенти и регистрите на транзакции; и правилата относно подобряването на сетълмента на ценни книжа в Съюза и относно централните депозитари на ценни книжа, които включват изисквания за операционен риск. Освен това изискванията за уведомяване за инциденти са част от нормалните надзорните практики във финансовия сектор и често са включени в наръчници за надзор. Държавите членки следва да вземат предвид посочените правила и изисквания при прилагането на *lex specialis*.

(14) Както отбелязва Европейската централна банка в своето становище от 25 юли 2014 г.[1], настоящата директива не засяга възприетия съгласно правото на Съюза режим за надзор от страна на Евросистемата върху платежните системи и системите за сетълмент. За органите, отговарящи за този надзор, би било подходящо да обменят знания и опит по въпросите, свързани със сигурността на мрежите и информационните системи, с компетентните по настоящата директива органи. Същото съображение важи и за държавите, които са извън еврозоната, но са част от Европейската система на централните банки, които упражнява такъв надзор върху платежните системи и системите за сетълмент въз основа на националните им законови и подзаконови разпоредби.

[1] ОВ C 352, 7.10.2014 г., стр. 4.

(15) Онлайн местата за търговия дават възможност на потребители и търговци да сключват онлайн договори за продажба или услуги с търговци и са крайното място за сключването на тези договори. Те следва да не обхващат онлайн услугите, които служат единствено като посредник към услуги на трети лица, чрез които в крайна сметка може да бъде сключен договор. Ето защо те следва да не обхващат онлайн услуги, които сравняват цената на определени продукти или услуги от различни търговци, а после препращат ползвателя към предпочитания търговец за закупуване на продукта. Изчислителните услуги, предоставяни от онлайн мястото за търговия, биха могли да включват обработването на сделки, агрегирането на данни или изготвянето на профил на ползвателите. Магазините за приложения, които работят като онлайн магазини, позволяващи цифровото разпространение на приложения или софтуерни програми от трети лица, следва да бъдат разглеждани като вид онлайн място за търговия.

(16) Онлайн търсачките позволяват на ползвателя да извършва търсене по принцип във всички уебсайтове въз основа на запитване, независимо от темата. Алтернативно те може да са насочени към уебсайтовете на определен език. Определението за онлайн търсачка, предвидено в настоящата директива, следва да не обхваща функциите за търсене, които са ограничени до съдържанието на конкретен уебсайт, независимо дали тази функция за търсене се предоставя от външна онлайн търсачка. То следва да не обхваща и онлайн услуги, които сравняват цената на определени продукти или услуги от различни търговци, а после препращат ползвателя към предпочитания търговец за закупуване на продукта.

(17) Компютърните услуги „в облак“ обхващат широк спектър от дейности, които могат да бъдат предоставяни съгласно различни модели. За целите на настоящата директива понятието „компютърни услуги „в облак“ включва услуги, които позволяват достъп до променлив по мащаб и еластичен набор от компютърни ресурси, които могат да бъдат ползвани съвместно. Тези „компютърни ресурси“ включват ресурси като мрежи, сървъри или друга инфраструктура, средства за съхранение, приложения и услуги. 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.

(18) Функцията на точките за обмен в интернет (ТОИ) е да свързват мрежи. ТОИ не осигуряват достъп до мрежа, нито служат като транзитен доставчик или превозвач. ТОИ също така не предоставят други услуги, които не са свързани с междумрежови връзки, въпреки че това не изключва възможността операторите на ТОИ да предоставят други услуги, които не са свързани с междумрежови връзки. ТОИ съществуват, за да свързват мрежи, които са технически и организационно разделени. Понятието „автономна система“ се използва за описанието на технически независима мрежа.

(19) Държавите членки следва да отговарят за определянето на това кои субекти отговарят на критериите от определението за оператор на основни услуги. За да се осигури последователен подход, определението за оператор на основни услуги следва да се прилага съгласувано от всички държави членки. За тази цел в настоящата директива е предвидена оценка на субектите, които извършват дейност в конкретните сектори и подсектори, изготвяне на списък на основните услуги, разглеждане на възможността за въвеждане на общ списък на междусекторните фактори за определяне дали потенциален инцидент би имал значително увреждащо въздействие, процес на консултиране, включващ съответните държави членки, в случай на субекти, които предоставят услуги в повече от една държава членка, и подкрепа за групата за сътрудничество в процеса на идентификация. За да се гарантира точното отражение на евентуалните промени на пазара, списъкът с определени оператори следва да подлежи на редовен преглед от държавите членки и при необходимост да бъде актуализиран. На последно място, държавите членки следва да представят на Комисията необходимата информация, за да може тя да прецени до каква степен тази обща методология е позволила на държавите членки да прилагат единно определение.

(20) В процеса на определяне на операторите на основни услуги държавите членки следва да направят оценка най-малко за всеки подсектор, посочен в настоящата директива, кои услуги трябва да се считат за основни за поддържането на особено важни обществени и стопански дейности, а също и дали субектите, изброени в секторите и подсекторите, посочени в настоящата директива и предоставящи въпросните услуги, отговарят на критериите за определяне на операторите. При изготвянето на оценката дали даден субект предоставя услуга, която е основна за поддържането на особено важни обществени или стопански дейности, е достатъчно да бъде проверено дали този субект предоставя услуга, която е включена в списъка на основни услуги. Освен това следва да се докаже, че предоставянето на основната услуга зависи от мрежи и информационни системи. На последно място, при изготвянето на оценката дали даден инцидент би имал значително увреждащо въздействие върху предоставянето на услугата държавите членки следва да имат предвид редица междусекторни фактори, както и факторите, които са характерни за конкретния сектор, когато е подходящо.

(21) За целите на определянето на операторите на основни услуги установяването в държава членка предполага ефективно и действително упражняване на дейност въз основа на стабилни правила. Правната форма на тези правила, независимо дали става въпрос за клон или дъщерно дружество с правосубектност, не е определящ фактор в това отношение.

(22) Възможно е субектите, работещи в секторите и подсекторите, посочени в настоящата директива, да предоставят както основни, така и неосновни услуги. Например, в сектора на въздушния транспорт летищата предоставят услуги, които дадена държава членка би могла да счете за основни, като управление на пистите, но и редица услуги, които може да бъдат счетени за неосновни, като предоставяне на търговски площи. Операторите на основни услуги следва да спазват специалните изисквания за сигурност единствено по отношение на услугите, които се считат за основни. Ето защо за целите на определянето на операторите държавите членки следва да съставят списък на услугите, които се считат за основни.

(23) Списъкът на услугите следва да съдържа всички услуги, предоставяни на територията на дадена държава членка, които отговарят на изискванията на настоящата директива. Държавите членки следва да могат да допълват съществуващия списък, като включват нови услуги. Списъкът на услугите следва да служи за справка на държавите членки и да им позволява да определят операторите на основни услуги. Неговото предназначение е да бъдат набелязани видовете основни услуги във всеки сектор, посочен в настоящата директива, като по този начин бъдат разграничени от неосновните дейности, за които даден субект, извършващ дейност в даден сектор, може да отговаря. Списъкът на услугите, съставен от всяка държава членка, ще служи за допълнителна информация при оценката на регулаторните практики на всяка държава членка с оглед на гарантирането на цялостна последователност на процеса на идентификация между държавите членки.

(24) За целите на процеса на идентификация, когато даден субект предоставя основна услуга в две или повече държави членки, тези държави членки следва да провеждат двустранни или многостранни обсъждания помежду си. Целта на този консултативен процес е да подпомогне оценката на влиянието на оператора предвид трансграничното му въздействие, като така се даде възможност на всяка участваща държава членка да изрази своето мнение относно рисковете, свързани с предоставяните услуги. В този процес участващите държави членки следва да отчетат взаимно мненията си и следва да могат да се обърнат за съдействие към групата за сътрудничество.

(25) В резултат на процеса на идентификация държавите членки следва да приемат национални мерки, за да определят за кои субекти се прилагат задълженията, свързани със сигурността на мрежите и информационните системи. Този резултат би могъл да се постигне чрез приемането на списък на всички оператори на основни услуги или чрез приемането на национални мерки, включително обективни количествени критерии, като например продукция на оператора или брой ползватели, които да позволяват да се определи за кои субекти се прилагат задълженията, свързани със сигурността на мрежите и информационните системи. Националните мерки, независимо дали са съществуващи или се приемат във връзка с настоящата директива, следва да включват всички правни мерки, административни мерки и политики, които позволяват определянето на операторите на основни услуги съгласно настоящата директива.

(26) За да се укаже значението на определените оператори на основни услуги във връзка със съответния сектор, държавите членки следва да вземат предвид броя и мащаба на операторите, например по отношение на пазарен дял или на произведено или превозено количество, без да са длъжни да разпространяват информация, която би разкрила кои са определените оператори.

(27) За да определят дали даден инцидент би имал значително увреждащо въздействие върху предоставянето на основна услуга, държавите членки следва да вземат предвид различни фактори, като броя на ползвателите, които разчитат на услугата за лични или професионални цели. Използването на услугата може да бъде пряко, непряко или чрез посредник. При оценяване на възможното въздействие на даден инцидент в зависимост от неговия мащаб и продължителност върху стопанските и обществените дейности или върху обществената безопасност, държавите членки следва да правят оценка и на времето, което вероятно ще измине, преди прекъсването да започне да оказва отрицателно въздействие.

(28) В допълнение към междусекторните фактори следва да бъдат взети предвид и характерните за конкретния сектор фактори, за да се определи дали даден инцидент би оказал значително увреждащо въздействие върху предоставянето на основна услуга. По отношение на доставчиците на енергия такива фактори биха могли да включват обема на произведената енергия или нейния дял в национален план; за доставчиците на нефт — дневния обем; за въздушния транспорт, включително летищата и въздушните превозвачи, железопътния транспорт и морските пристанища — дела от националния обем на трафика и броя на пътниците или товарните операции за година; за банковите инфраструктури или инфраструктурите на финансовите пазари — тяхното системно значение въз основа на общите им активи или съотношението между тези активи и БВП; за сектора на здравеопазването — броя на пациентите, обслужени от доставчика на здравни услуги за година; за добива, обработката и доставката на вода — обема и броя на ползвателите, за които е доставена водата, и техния вид, включително например болници, учреждения за обществени услуги, организации или физически лица, както и наличието на алтернативни източници на вода, които да покриват същата географска територия.

(29) С цел постигане и поддържане на високо ниво на сигурност на мрежите и информационните системи всяка държава членка следва да има национална стратегия относно сигурността на мрежите и информационните системи, в която да са определени стратегическите цели и конкретните действия на политиката, които ще бъдат изпълнявани.

(30) С оглед на различията в националните структури на управление и с цел да се защитят вече съществуващи секторни правила или надзорните и регулаторни органи на Съюза, както и да се избегне дублирането, 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 операторите на основни услуги и доставчиците на цифрови услуги съгласно настоящата директива.

(31) За да се улесни трансграничното сътрудничество и комуникация и да се осигури възможност за ефективно изпълнение на настоящата директива, е необходимо всяка държава членка, без да се засягат секторните регулаторни правила, да определи национално единно звено за контакт, което да отговаря координацията на въпросите, свързани със сигурността на мрежите и информационните системи, и за трансграничното сътрудничество на равнището на Съюза. Компетентните органи и единните звена за контакт следва да разполагат с достатъчно технически, финансови и човешки ресурси, за да се гарантира, че са в състояние да изпълняват ефективно и ефикасно възложените им задачи и по този начин да постигат целите на настоящата директива. Тъй като настоящата директива има за цел да подобри функционирането на вътрешния пазар чрез изграждането на доверие, органите на държавите членки трябва да могат да си сътрудничат ефективно със стопанските субекти и да бъдат подходящо структурирани.

(32) Уведомленията за инцидентите следва да се подават до компетентните органи или до екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС). Единните звена за контакт следва да не получават директно уведомления за инциденти, освен ако не изпълняват и функциите на компетентен орган или ЕРИКС. Даден компетентен орган или ЕРИКС следва обаче да може да възложи на единното звено за контакт задачата да предава уведомленията за инциденти на единните звена за контакт на други засегнати държави членки.

(33) За да се осигури ефективното предоставяне на информация на държавите членки и Комисията, единното звено за контакт следва да представи на групата за сътрудничество обобщителен доклад, който следва да съдържа информация на анонимна основа, така че да се запази поверителността на уведомленията и самоличността на операторите на основни услуги и доставчиците на цифрови услуги, тъй като информацията относно идентификационните данни на уведомяващия субект не се изисква за обмена на най-добри практики в групата за сътрудничество. Обобщителният доклад следва да съдържа информация относно броя на получените уведомления, както и данни относно характера на инцидентите, за които са подадени уведомления, като например типа на нарушенията на сигурността, тяхната сериозност или продължителност.

(34) Държавите членки следва да бъдат достатъчно добре подготвени и като технически, и като организационен капацитет да предотвратяват, установяват, 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, които да отговарят на основните изисквания за гарантиране на ефективни и съвместими способности за справяне с инциденти и рискове и за осигуряване на ефективно сътрудничество на равнището на Съюза. За да се ползват всички видове оператори на основни услуги и доставчици на цифрови услуги от тези способности и това сътрудничество, държавите членки следва да гарантират, че за всички тези видове има определен ЕРИКС. 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.

(35) Тъй като повечето мрежи и информационни системи се експлоатират от частни субекти, сътрудничеството между публичния и частния сектор е от основно значение. Операторите на основни услуги и доставчиците на цифрови услуги следва да бъдат насърчавани да развиват свои собствени механизми за неформално сътрудничество за гарантиране на сигурността на мрежите и информационните системи. Групата за сътрудничество следва да може да покани съответните конституенти на обсъжданията, когато това е целесъобразно. За ефективното насърчаване на споделянето на информация и най-добри практики е от основно значение да се гарантира, че операторите на основни услуги и доставчиците на цифрови услуги, които се включват в такъв обмен, няма да бъдат ощетени в резултат на сътрудничеството си.

(36) ENISA следва да оказва подкрепа на държавите членки и Комисията, като предоставя на разположение своите експертни познания и консултации и улеснява обмена на най-добри практики. По-специално Комисията следва, а държавите членки следва да могат да се консултират с ENISA при прилагането на настоящата директива. За изграждането на капацитет и знания сред държавите членки групата за сътрудничество следва да служи и като инструмент за обмен на най-добри практики, за обсъждане на способностите и на подготвеността на държавите членки, за подпомагане на доброволна основа на нейните членове при оценката на националните стратегии относно сигурността на мрежите и информационните системи, изграждането на капацитет и оценката на учения в областта на сигурността на мрежите и информационните системи.

(37) Когато е целесъобразно, държавите членки следва да могат да използват или да адаптират съществуващите организационни структури или стратегии при прилагането на настоящата директива.

(38) Съответните задачи на групата за сътрудничество и на ENISA са взаимозависими и се допълват. Като цяло ENISA следва да подпомага групата за сътрудничество в изпълнението на нейните задачи в съответствие с целта на ENISA, установена в Регламент (ЕС) № 526/2013 на Европейския парламент и на Съвета[1], а именно да подпомага институциите, органите, службите и агенциите на Съюза и държавите членки при изпълнението на политиките, необходими за спазването на правните и регулаторните изисквания за сигурност на мрежите и информационните системи съгласно действащите и бъдещите правни актове на Съюза. По-специално ENISA следва да предоставя помощ в онези области, които съответстват на нейните собствени задачи, установени в Регламент (ЕС) № 526/2013, а именно анализиране на стратегии относно сигурността на мрежите и информационните системи, подкрепа за организирането и провеждането на учения на Съюза в областта на сигурността на мрежите и информационните системи и обмен на информация и на най-добри практики в повишаването на осведомеността. ENISA следва също така да участва в разработването на насоки за характерни за конкретния сектор критерии за определяне на значимостта на въздействието на инцидентите.

(39) С цел да способства за усъвършенствана сигурност на мрежите и информационните системи групата за сътрудничество следва, когато е целесъобразно, да си сътрудничи със съответните институции, органи, служби и агенции на Съюза, за да обменя знания и най-добри практики с тях и да им дава консултации по свързани със сигурността въпроси на мрежите и информационните системи, които биха могли да окажат въздействие върху тяхната работа, като спазва съществуващите правила за обмен на класифицирана информация. При сътрудничеството си с правоприлагащите органи по въпроси, свързани със сигурността на мрежите и информационните системи, които биха могли да окажат въздействие върху тяхната работа, групата за сътрудничество следва да се придържа към съществуващите информационни канали и изградените мрежи.

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

(40) Информацията относно инцидентите е все по-ценна за широката общественост и предприятията, особено за малките и средните предприятия. В някои случаи тази информация вече се предоставя посредством уебсайтове на национално равнище, на езика на дадена държава, и е насочена главно към инциденти и случаи с национално измерение. Предвид факта, че предприятията работят все по-често на трансгранична основа и гражданите използват онлайн услуги, информацията за инцидентите следва да се предоставя обобщено на равнището на Съюза. Секретариатът на мрежата на ЕРИКС се насърчава да поддържа уебсайт или да създаде специална страница в съществуващ уебсайт, където на широката общественост да се предоставя обща, насочена специално към интересите и нуждите на предприятията информация за големи свързани със сигурността инциденти, засягащи мрежите и информационните системи, които са възникнали на територията на целия Съюз. Участващите в мрежата на ЕРИКС се насърчават да предоставят на доброволна основа информацията, която да бъде публикувана на този уебсайт, без да се включва поверителна информация или информация с чувствителен характер.

(41) Когато информация се счита за поверителна в съответствие с националните правила и правилата на Съюза относно търговската тайна, следва да се гарантира поверителност при провеждането на дейностите и изпълнението на целите, определени в настоящата директива.

(42) Ученията, при които в реално време се симулират сценарии на инциденти, са от основно значение за проверка на подготвеността и сътрудничеството на държавите членки във връзка със сигурността на мрежите и информационните системи. Цикълът от учения CyberEurope, координиран от ENISA, с участието на държавите членки, е полезен инструмент за проверка и изготвяне на препоръки за подобряване в бъдеще на действията при инциденти на равнището на Съюза. Като се има предвид, че понастоящем държавите членки не са задължени нито да планират, нито да участват в учения, създаването на мрежата на ЕРИКС съгласно настоящата директива следва да даде възможност на държавите членки да участват в учения въз основа на точно планиране и стратегически решения. Групата за сътрудничество, създадена съгласно настоящата директива, следва да обсъжда стратегическите решения във връзка с ученията, по-специално, но не само, по отношение на тяхната честота и подготовката на сценариите. В съответствие с мандата си ENISA следва да подкрепя организирането и провеждането на учения в целия Съюз, като предоставя своите експертни познания и консултации на групата за сътрудничество и на мрежата на ЕРИКС.

(43) С оглед на глобалния характер на свързаните със сигурността проблеми, засягащи мрежите и информационните системи, е необходимо по-тясно международно сътрудничество за повишаване на стандартите за сигурност, за подобряване на обмена на информация и за насърчаване на единен глобален подход по въпросите на сигурността.

(44) Отговорността по гарантиране на сигурността на мрежите и информационните системи е в голяма степен на операторите на основни услуги и на доставчиците на цифрови услуги. Следва да се насърчава култура на управление на риска, част от която са оценката на риска и изпълнението на мерки за сигурност, съобразени със съществуващите рискове, и тази култура следва да се развива чрез подходящи регулаторни изисквания и доброволни практики от страна на съответните сектори. Постигането на надеждни условия на равнопоставеност също е от основно значение за ефективното функциониране на групата за сътрудничество и мрежата на ЕРИКС при гарантирането на ефективно сътрудничество от страна на всички държави членки.

(45) Настоящата директива се прилага единствено по отношение на публичните администрации, които са определени за оператори на основни услуги. Следователно държавите членки отговарят за гарантирането на сигурността на мрежите и информационните системи на публичните администрации, които не попадат в обхвата на настоящата директива.

(46) Мерките за управление на риска включват мерки за набелязване на всякакви рискове от инциденти с цел предотвратяване, разкриване и предприемане на действия при инциденти, както и за тяхното ограничаване. Сигурността на мрежите и информационните системи включва сигурността на данните, които се съхраняват, предават и обработват.

(47) Компетентните органи следва да запазят способността си да приемат национални насоки за обстоятелствата, при които от операторите на основни услуги се изисква да уведомяват за инциденти.

(48) Много предприятия в Съюза разчитат на доставчици на цифрови услуги за предоставянето на своите услуги. Тъй като някои цифрови услуги биха могли да бъдат важен ресурс за техните ползватели, включително за операторите на основни услуги, и тъй като е възможно тези ползватели не винаги да разполагат с алтернативи, настоящата директива следва да се прилага и по отношение на доставчиците на такива услуги. Сигурността, непрекъснатостта и надеждността на видовете цифрови услуги, посочени в настоящата директива, е от основно значение за гладкото функциониране на много предприятия. Нарушаването на такава цифрова услуга може да попречи на предоставянето на други услуги, които зависят от нея и по този начин може да окаже въздействие върху основни стопански и обществени дейности в Съюза. Ето защо такива цифрови услуги може да бъдат от основно значение за гладкото функциониране на предприятията, които зависят от тях, и не само това, но и за участието на тези предприятия във вътрешния пазар, както и в трансграничната търговия в Съюза. Доставчиците на цифрови услуги, за които се прилага настоящата директива, са тези, които се счита, че предлагат цифрови услуги, от които все повече зависят много предприятия в Съюза.

(49) Доставчиците на цифрови услуги следва да гарантират такова ниво на сигурност, което да отговаря на степента на риска за сигурността на цифровите услуги, които предоставят, като се има предвид значението на техните услуги за дейността на други предприятия в Съюза. На практика степента на риска за операторите на основни услуги, които често са от основно значение за поддържането на особено важни обществени и стопански дейности, е по-висока от тази за доставчиците на цифрови услуги. Поради това изискванията по отношение на сигурността за доставчиците на цифрови услуги следва да бъдат по-облекчени. Доставчиците на цифрови услуги следва да запазят правото да вземат мерки по своя преценка за управление на рисковете, които застрашават сигурността на техните мрежи и информационни системи. Поради трансграничния им характер към доставчиците на цифрови услуги следва да се прилага по-хармонизиран подход на равнището на Съюза. Конкретизирането и прилагането на тези мерки следва да бъде улеснено с актове за изпълнение.

(50) Въпреки че производителите на хардуер и разработчиците на софтуер не са оператори на основни услуги, нито доставчици на цифрови услуги, техните продукти повишават сигурността на мрежите и информационните системи. Поради това те са от важно значение за създаването на условия, позволяващи на операторите на основни услуги и доставчиците на цифрови услуги да обезопасят своите мрежи и информационни системи. За хардуерните и софтуерните продукти вече се прилагат съществуващи правила относно отговорността за продукта.

(51) Техническите и организационните мерки, наложени на операторите на основни услуги и на доставчиците на цифрови услуги, следва да не изискват проектирането, разработването или производство по определен начин на конкретен търговски продукт на информационните и комуникационните технологии.

(52) Операторите на основни услуги и доставчиците на цифрови услуги следва да гарантират сигурността на мрежите и информационните системи, които използват. Това са предимно частни мрежи и информационни системи, управлявани или от вътрешен ИТ персонал, или чиято сигурност е възложена на външни изпълнители. Изискванията за сигурност и уведомяване следва да се прилагат за съответните оператори на основни услуги и доставчици на цифрови услуги без оглед на това дали те извършват вътрешно поддръжката на своите мрежи и информационни системи или я възлагат на външни изпълнители.

(53) С цел да се избегне налагането на несъразмерна финансова и административна тежест върху операторите на основни услуги и доставчиците на цифрови услуги изискванията следва да бъдат съразмерни с риска, който съществува по отношение на съответната мрежа и информационна система, като се отчитат последните постижения в областта на тези мерки. По отношение на доставчици на цифрови услуги тези изисквания следва да не се прилагат за микро- и малките предприятия.

(54) Когато публичните администрации в държавите членки използват услуги, предлагани от доставчик на цифрови услуги, по-специално компютърни услуги „в облак“, те може да пожелаят да изискат от доставчиците на тези услуги допълнителни мерки за сигурност, които да надхвърлят обичайно предлаганите от доставчиците на цифрови услуги мерки за сигурност в съответствие с изискванията на настоящата директива. Те следва да могат да направят това чрез налагането на договорни задължения.

(55) Съдържащите се в настоящата директива определения за онлайн места за търговия, онлайн търсачки и компютърни услуги „в облак“ са предназначени за конкретните цели на настоящата директива и не засягат никакви други актове.

(56) Настоящата директива не следва да възпрепятства държавите членки да приемат национални мерки, с които да се задължават органите от публичния сектор да осигурят изпълнението на специални изисквания за сигурност, когато възлагат поръчки за компютърни услуги „в облак“. Тези национални мерки следва да се прилагат спрямо съответния орган от публичния сектор, а не спрямо доставчика на компютърни услуги „в облак“.

(57) Предвид фундаменталните различия между операторите на основни услуги, по-специално тяхната пряка връзка с физическата инфраструктура, и доставчиците на цифрови услуги, по-специално трансграничния им характер, настоящата директива следва да възприеме различен подход по отношение на нивото на хармонизация във връзка с тези две групи субекти. По отношение на операторите на основни услуги държавите членки следва да могат да определят съответните оператори и да налагат по-строги изисквания от предвидените в настоящата директива. Държавите членки не следва да определят доставчици на цифрови услуги, тъй като настоящата директива следва да се прилага за всички доставчици на цифрови услуги, попадащи в нейния обхват. Освен това настоящата директива и приетите съгласно нея актове за изпълнение следва да осигурят висока степен на хармонизация за доставчиците на цифрови услуги по отношение на изискванията за сигурност и уведомяване. Това следва да позволи еднаквото третиране на доставчиците на цифрови услуги в целия Съюз по начин, който е съразмерен с техния характер и със степента на риск, на която може да са изложени.

(58) Настоящата директива не следва да възпрепятства държавите членки да налагат изисквания за сигурност и уведомяване на субекти, които не са доставчици на цифрови услуги, попадащи в обхвата на настоящата директива, без да се засягат задълженията на държавите членки съгласно правото на Съюза.

(59) Компетентните органи следва да обръщат необходимото внимание на запазването на неофициалните и ползващи се с доверие канали за обмен на информация. При даването на публичност на докладваните на компетентните органи инциденти следва да се постига нужният баланс между интереса на обществеността да бъде информирана за заплахите и възможните вреди за търговската дейност и репутацията на операторите на основни услуги и доставчиците на цифрови услуги, които докладват за инцидентите. При изпълнението на задълженията за уведомяване компетентните органи и ЕРИКС следва да обръщат особено внимание на необходимостта информацията за уязвимостите на продуктите да остане строго поверителна преди публикуването на съответните корекции по отношение на сигурността.

(60) Доставчиците на цифрови услуги следва да подлежат на облекчена и ответна последваща надзорна дейност, обоснована от естеството на извършваните от тях услуги и операции. Поради това съответният компетентен орган следва да предприема действия само когато разполага с доказателства, например от самия доставчик на цифрови услуги, от друг компетентен орган, включително от компетентен орган на друга държава членка, или от ползвател на услугата, че доставчик на цифрови услуги не отговаря на изискванията на настоящата директива, по-специално вследствие настъпването на инцидент. Ето защо компетентният орган следва да няма общо задължение да упражнява надзор над доставчиците на цифрови услуги.

(61) Компетентните органи следва да разполагат с необходимите средства за изпълнение на своите задължения, включително правомощия за получаване на достатъчно информация за оценяване на нивото на сигурност на мрежите и информационните системи.

(62) Инцидентите може да са резултат от престъпления, предотвратяването, разследването и наказателното преследване на които се подпомага чрез координацията и сътрудничеството между операторите на основни услуги, доставчиците на цифрови услуги, компетентните органи и правоприлагащите органи. Когато съществуват подозрения, че даден инцидент е свързан с тежки престъпления — съобразно правото на Съюза или националното право, държавите членки следва да насърчават операторите на основни услуги и доставчиците на цифрови услуги да докладват инциденти, чийто характер може да бъде свързан с тежки престъпления, на съответните правоприлагащи органи. Когато е целесъобразно, е желателно координацията между компетентните органи и правоприлагащите органи на различни държави членки да бъде улеснявана от Европейския център за борба с киберпрестъпността (EC3) и ENISA.

(63) В много случаи вследствие на инциденти се засягат лични данни. В този контекст компетентните органи и органите за защита на данните следва да си сътрудничат и да обменят информация относно всички съответни въпроси с цел справяне с нарушенията на сигурността на лични данни, предизвикани от инциденти.

(64) Юрисдикцията по отношение на доставчиците на цифрови услуги следва да бъде предоставена на държавата членка, в която съответният доставчик на цифрови услуги има основно място на установяване в Съюза, която по принцип съответства на мястото, където се намира главното управление на доставчика в Съюза. Установяването предполага ефективното и действителното упражняване на дейност съгласно стабилни правила. Правната форма на тези правила, независимо дали става въпрос за клон или дъщерно дружество с правосубектност, не е определящ фактор в това отношение. 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 критерии за определяне на основното място на установяване.

(65) Когато доставчик на цифрови услуги, който не е установен в Съюза, предлага услуги в Съюза, той следва да определи свой представител. За да се установи дали този доставчик на цифрови услуги предлага услуги в Съюза, следва да се установи дали е видно, че този доставчик на цифрови услуги възнамерява да предлага услуги на лица на територията на една или повече държави членки. Сама по себе си достъпността в Съюза на уебсайт на доставчика на цифрови услуги 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 доставчикът на цифрови услуги, са недостатъчни, за да бъде установено 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 доставчикът на цифрови услуги възнамерява да предлага услуги в Съюза. Представителят следва да действа от името на доставчика на цифрови услуги, а компетентните органи или ЕРИКС следва да могат да се свържат с представителя. Представителят следва да е определен изрично чрез упълномощаване в писмена форма от доставчика на цифрови услуги да действа от негово име във връзка със задълженията му съгласно настоящата директива, включително за докладването на инциденти.

(66) Стандартизацията на изискванията за сигурност е процес, движен от пазарни сили. С цел да гарантират еднообразното прилагане на стандартите за сигурност държавите членки следва да насърчават съответствието или спазването на посочените стандарти с оглед осигуряването на високо ниво на сигурност на мрежите и информационните системи на равнището на Съюза. ENISA следва да подпомага държавите членки чрез консултации и насоки. За тази цел може да се окаже полезно изготвянето на хармонизирани стандарти, като това следва да е в съответствие с Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета[1].

(67) Субекти, които попадат извън обхвата на настоящата директива, може да претърпят инциденти, оказващи съществено въздействие върху предоставяните от тях услуги. Когато тези субекти считат, че би било от обществен интерес да уведомят за настъпването на такива инциденти, те следва да могат да го направят на доброволна основа. Подобни сигнали следва да бъдат обработвани от компетентните органи или от ЕРИКС, когато това не представлява несъразмерна или неоправдана тежест за съответните държави членки.

[1] 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).

(68) За да се гарантират еднакви условия за изпълнение на настоящата директива следва да се предоставят изпълнителни правомощия на Комисията, за да се предвидят процедурните правила, необходими за работата на групата за сътрудничество, и изискванията за сигурност и уведомяване, приложими за доставчиците на цифрови услуги. Тези правомощия следва да се упражняват в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета[1]. При приемането на актове за изпълнение във връзка с процедурните правила, необходими за работата на групата за сътрудничество, Комисията следва да отчита в максимална степен становището на ENISA.

(69) При приемането на актове за изпълнение относно изискванията за сигурност към доставчиците на цифрови услуги Комисията следва да отчита в максимална степен становището на ENISA и да се консултира с конституентите. Освен това Комисията се насърчава да вземе под внимание следните примери: във връзка със сигурността на системите и съоръженията: физическа и екологична сигурност, сигурност на доставките, контрол на достъпа до мрежите и информационните системи и целостта на мрежите и информационните системи; във връзка с действията при инциденти: процедури за предприемане на действия при инциденти, способности за установяване на инциденти, докладване на инциденти и комуникация; във връзка с управлението на непрекъснатостта на дейностите: стратегия и планове за действие при извънредни ситуации за осигуряване непрекъснатостта на услугата, способности за възстановяване при бедствия; и във връзка с наблюдението, одита и изпитванията: политики за наблюдението и регистрирането, планове за действие при извънредни ситуации, изпитвания на мрежите и информационните системи, оценки на сигурността и наблюдение на съответствието.

[1] 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).

(70) При изпълнението на настоящата директива Комисията следва да поддържа, когато е целесъобразно,връзка със съответните секторни комитети и органи, създадени на равнището на Съюза в областите, обхванати от настоящата директива.

(71) Комисията следва периодично да прави преглед на настоящата директива, като се консултира с конституентите, по-специално с оглед определянето на необходимостта от изменения с оглед на промените в обществените, политически, технологични или пазарни условия.

(72) При обмена на информация относно рисковете и инцидентите в рамките на групата за сътрудничество и мрежата на ЕРИКС и спазването на изискванията за уведомяване на националните компетентни органи или ЕРИКС за инциденти може да възникне необходимост от обработването на лични данни. Това обработване следва да се извършва в съответствие с Директива 95/46/ЕО на Европейския парламент и на Съвета[1] и Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета[2]. При прилагането на настоящата директива следва да се прилага Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета[3], в зависимост от случая.

(73) Беше проведена консултация с Европейския надзорен орган по защита на данните в съответствие с член 28, параграф 2 от Регламент (ЕО) № 45/2001, като той прие своето становище на 14 юни 2013 г.[4].

---

1 Директива 95/46/ЕО на Европейския парламент и на Съвета от 24 октомври 1995 г. за защита на физическите лица при обработването на лични данни и за свободното движение на тези данни (ОВ L 281, 23.11.1995 г., стр. 31).

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

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

4 ОВ C 32, 4.2.2014 г., стр. 19

(74) Тъй като целта на настоящата директива, и именно постигане на високо общо ниво на сигурност на мрежите и информационните системи в Съюза, не може да бъде постигната в достатъчна степен единствено 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.

(75) 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 и обхват

1. С настоящата директива се установяват мерки с цел постигане на високо общо ниво на сигурност на мрежите и информационните системи в Съюза, така че да се подобри функционирането на вътрешния пазар.

2. За тази цел с настоящата директива:

   а) се предвиждат задължения за всички държави членки да приемат национална стратегия относно сигурността на мрежите и информационните системи;

   б) се създава група за сътрудничество с цел подкрепа и улесняване на стратегическото сътрудничество и обмен на информация между държавите членки и изграждане на доверие сред тях;

   в) се създава мрежа на екипите за реагиране при инциденти с компютърната сигурност (наричана по-долу „мрежата на ЕРИКС“) с цел да се способства за изграждане на доверие между държавите членки и да се насърчи бързото и ефективно оперативно сътрудничество;

   г) се установяват изискванията за сигурност и уведомяване за операторите на основни услуги и за доставчиците на цифрови услуги;

д) се предвиждат задълженията на държавите членки да определят националните компетентни органи, единните звена за контакт и ЕРИКС със задачи, свързани със сигурността на мрежите и информационните системи.

3. Изискванията за сигурност и уведомяване, предвидени в настоящата директива, не се прилагат нито за предприятията, за които се прилагат изискванията по членове 13а и 13б от Директива 2002/21/ЕО, нито за доставчиците на удостоверителни услуги, за които се прилагат изискванията по член 19 от Регламент (ЕС) № 910/2014.

4. Настоящата директива се прилага, без да се засягат Директива 2008/114/ЕО на Съвета[1] и директиви 2011/93/ЕС[2] и 2013/40/ЕС[3] на Европейския парламент и на Съвета.

5. Без да се засяга член 346 ДФЕС, информацията, която е поверителна съгласно правилата на Съюза и националните правила, например правилата за търговската тайна, се обменят с Комисията и други съответни органи само когато този обмен е необходим за прилагането на настоящата директива. Обменяната информация е ограничена до информацията, която има значение целите на този обмен и която е пропорционална на тези цели. При този обмен на информация се запазва поверителността на информацията, както и сигурността и търговските интереси на операторите на основни услуги и доставчиците на цифрови услуги.

---

1 Директива 2008/114/ЕО на Съвета от 8 декември 2008 г. относно установяването и означаването на европейски критични инфраструктури и оценката на необходимостта от подобряване на тяхната защита (ОВ L 345, 23.12.2008 г., стр. 75).

2 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).

3 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).

6. Настоящата директива не засяга действията, предприети от държавите членки за защита на техните основни държавнически функции, по-специално за защита на националната сигурност, включително действия за защита на информацията, разкриването на която държавите членки считат за противоречащо на основните интереси на своята сигурност, и за поддържане на законността и реда, по-специално да се осигури възможност за разследване, разкриване и наказателно преследване на престъпления.

7. Когато в правен акт на Съюза, който е специален за конкретен сектор, е предвидено операторите на основни услуги или доставчиците на цифрови услуги да гарантират сигурността на своите мрежи и информационни системи или да уведомяват за инциденти, се прилагат разпоредбите на специалния за сектора правен акт на Съюза, при условие че изискванията са най-малкото равностойни като резултат на задълженията, предвидени в настоящата директива.

Член 2

Обработване на личните данни

1. Съгласно настоящата директива личните данни се обработват в съответствие с Директива 95/46/ЕО.

2. Обработването на лични данни от институции и органи на Съюза съгласно настоящата директива се извършва в съответствие с Регламент (ЕО) № 45/2001.

Член 3

Минимална хармонизация

Без да се засягат член 16, параграф 10 и задълженията на държавите членки съгласно правото на Съюза, държавите членки могат да приемат или запазват разпоредби с оглед постигането на по-високо ниво на сигурност на мрежите и информационните системи.

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, буква а) от Директива 2002/21/ЕО,

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

   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 действия, засягащи 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;

3) „национална стратегия относно сигурността на мрежите и информационните системи“ означава рамка, включваща стратегически цели и приоритети в областта на сигурността на мрежите и информационните системи на национално равнище;

4) „оператор на основни услуги“ означава публичен или частен субект от посочените в приложение II категории, който отговаря на критериите, определени в член 5, параграф 2;

5) „цифрова услуга“ означава услуга по смисъла на член 1, параграф 1, буква б) от Директива (ЕС) № 2015/1535 на Европейския парламент и на Съвета[1] от категориите, изброени в приложение III;

6) „доставчик на цифрови услуги“ означава юридическо лице, предоставящо цифрова услуга;

7) „инцидент“ означава събитие, което има реално неблагоприятно въздействие върху сигурността на мрежите и информационните системи;

8) „действия при инцидент“ означава всички процедури, подпомагащи установяването, анализа и ограничаването на инцидент и реагирането на такъв инцидент;

[1] 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).

9) „риск“ означава разумно установимо обстоятелство или събитие, което може да има неблагоприятно въздействие върху сигурността на мрежите и информационните системи;

10) „представител“ означава физическо или юридическо лице, установено в Съюза, което е изрично определено да действа от името на доставчик на цифрови услуги, който не е установен в Съюза, и към което националните компетентен орган или ЕРИКС може да се обърне вместо към доставчика на цифрови услуги във връзка със задълженията на доставчика на цифрови услуги по настоящата директива;

11) „стандарт“ означава стандарт по смисъла на член 2, точка 1 от Регламент (ЕС) № 1025/2012;

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

13) „точка за обмен в интернет (ТОИ)“ означава мрежово средство, което дава възможност за свързване на повече от две независими 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;

14) „система за имена на домейни (Domain Name System - DNS)“ означава йерархично разпределена и мрежова система за именуване на домейни, която разпределя заявки за имена на домейни;

15) „доставчик на DNS услуги“ означава субект, предоставящ DNS услуги по интернет;

16) „регистър на имена на домейни от първо ниво“ означава субект, който извършва и управлява регистрацията на имената на интернет домейни в специален домейн от първо ниво (top-level domain — TLD);

17) „онлайн място за търговия“ означава цифрова услуга, която дава на потребители и/или търговци — по смисъла на определенията, съдържащи се съответно в член 4, параграф 1, букви а) и б) от Директива 2013/11/ЕС на Европейския парламент и на Съвета[1] — възможността да сключват договори за онлайн продажби или услуги с търговци или на уебсайта на онлайн мястото за търговия, или на уебсайт на търговеца, използващ електронни услуги, предоставяни от онлайн мястото за търговия;

18) „онлайн търсачка“ означава цифрова услуга, която дава възможност на ползвателите на интернет да извършват търсене по правило на всички уебсайтове или уебсайтове на даден език въз основа на запитване по всякакви теми под формата на ключова дума, израз или друг вид въведени данни, в отговор на което тя подава интернет връзки, съдържащи информация, свързана с искането съдържание;

19) „компютърна услуга „в облак“ означава цифрова услуга, която дава възможност за достъп до променлив по мащаб и еластичен набор от компютърни ресурси, които могат да бъдат ползвани съвместно;

Член 5

Определяне на операторите на основни услуги

1. До ... [27 месеца след датата на влизане в сила на настоящата директива] за всеки сектор и подсектор, посочен в приложение II, държавите членки определят операторите на основни услуги с място на установяване на тяхна територия.

[1] Директива 2013/11/ЕС на Европейския парламент и на Съвета от 21 май 2013 г. за алтернативно решаване на потребителски спорове и за изменение на Регламент (ЕО) № 2006/2004 и Директива 2009/22/ЕО (Директива за АРС за потребители) (ОВ L 165, 18.6.2013 г., стр. 63).

2. Критериите за определянето на операторите на основни услуги, посочени в член 4, точка 4, са, както следва:

а) субектът предоставя услуга, която е от основно значение за поддържането на особено важни обществени и/или стопански дейности;

б) предоставянето на тази услуга зависи от мрежи и информационни системи; и

в) евентуален инцидент би имал значително увреждащо въздействие върху предоставянето на тази услуга.

3. За целите на параграф 1 всяка държава членка изготвя списък на услугите, посочени в параграф 2, буква а).

4. За целите на параграф 1, когато даден субект предоставя услуга, посочена в параграф 2, буква а), в две или повече държави членки, тези държави членки провеждат консултации помежду си. Тези консултации се провеждат преди вземането на решение относно определянето.

5. Държавите членки преразглеждат списъка на определените оператори на основни услуги редовно и най-малкото на всеки две години след … [21 месеца след датата на влизане в сила на настоящата директива], като при необходимост го актуализират.

6. Ролята на групата за сътрудничество е, в съответствие с посочените в член 11 задачи, да подкрепя държавите членки при възприемането на последователен подход в процеса на определяне на операторите на основни услуги.

7. За целите на прегледа, посочен в член 23, в срок от … [27 месеца след датата на влизане в сила на настоящата директива], както и на всеки две години след това, държавите членки предоставят на Комисията информацията, която ѝ е необходима, за да може тя да извърши оценка на изпълнението на настоящата директива, по-специално на последователността на подходите на държавите членки по отношение на определянето на операторите на основни услуги. Тази информация включва най-малкото:

а) националните мерки, които дават възможност за определяне на операторите на основни услуги;

б) списъка на услугите, посочен в параграф 3;

в) броят на операторите на основни услуги, определени за всеки сектор, посочен в приложение II, и посочване на тяхното значение във връзка с този сектор;

г) прагове, когато има такива, за определяне на съответното равнище на доставките спрямо броя на ползвателите, разчитащи на тази услуга, в съответствие с посоченото в член 6, параграф 1, буква а), или значението на конкретния оператор на основни услуги в съответствие с посоченото в член 6, параграф 1, буква е).

С цел да способства за предоставянето на съпоставима информация Комисията, като отчита в максимална степен становището на ENISA, може да приеме подходящи технически насоки относно параметрите на информацията, посочена в настоящия параграф.

Член 6

Значително увреждащо въздействие

1. При определяне на значимостта на увреждащото въздействие в съответствие с посоченото в член 5, параграф 2, буква в) държавите членки вземат предвид най-малко следните фактори, валидни за всички сектори:

   а) броят на ползвателите, разчитащи на услугите, предоставяни от субекта;

   б) зависимостта на други сектори, посочени в приложение II, от услугата, предоставяна от субекта;

   в) въздействието, което инцидентите биха могли да имат от гледна точка на мащаб и продължителност върху стопанските и обществените дейности или обществената безопасност;

   г) пазарния дял на субекта;

   д) географският обхват, що се отнася до областта, която би била засегната от даден инцидент;

   е) значението на субекта за поддържането на достатъчно ниво на услугата, като се взема предвид наличието на други средства за предоставянето на тази услуга.

2. За да се определи дали даден инцидент би имал значително увреждащо въздействие, държавите членки вземат предвид и характерните за сектора фактори, когато е целесъобразно.

ГЛАВА II
НАЦИОНАЛНИ РАМКИ ОТНОСНО СИГУРНОСТТА НА МРЕЖИТЕ И ИНФОРМАЦИОННИТЕ СИСТЕМИ

Член 7

Национална стратегия относно сигурността на мрежите и информационните системи

1. Всяка държава членка приема национална стратегия относно сигурността на мрежите и информационните системи, в която са определени стратегическите цели и подходящи мерки на политиката, както и подходящи регулаторни мерки за постигане и поддържане на високо ниво на сигурност на мрежите и информационните системи и която обхваща най-малко секторите, посочени в приложение II, и услугите, посочени в приложение III. В националната стратегия относно сигурността на мрежите и информационните системи се разглеждат по-специално следните въпроси:

   а) целите и приоритетите на националната стратегия относно сигурността на мрежите и информационните системи;

   б) управленска рамка за постигане на целите и приоритетите на националната стратегия относно сигурността на мрежите и информационните системи, включително ролите и отговорностите на държавните органи и на съответните други участници;

   в) набелязване на мерки във връзка с подготвеността, реагирането и възстановяването, включително сътрудничеството между публичния и частния сектор;

г) основна информация за образователните и обучителните програми и програмите за повишаване на осведомеността във връзка с националната стратегия относно сигурността на мрежите и информационните системи;

д) посочване на плановете за научноизследователска и развойна дейност във връзка с националната стратегия относно сигурността на мрежите и информационните системи;

е) план за оценка на риска с цел набелязване на рисковете;

ж) списък на различните участници в изпълнението на националната стратегия относно сигурността на мрежите и информационните системи;

2. Държавите членки може да поискат съдействие от ENISA при изготвянето на националните стратегии относно сигурността на мрежите и информационните системи.

3. Държавите членки съобщават своите национални стратегии относно сигурността на мрежите и информационните системи на Комисията в тримесечен срок след приемането им. При това държавите членки могат да изключат някои елементи на стратегията, свързани с националната сигурност.

Член 8

Национални компетентни органи и единни звена за контакт

1. Всяка държава членка определя един или повече национални компетентни органи по сигурността на мрежите и информационните системи (наричани по-долу „компетентният орган“), който обхваща най-малко секторите, посочени в приложение II, и услугите, посочени в приложение III. Държавите членки могат да възложат тези функции на съществуващ орган или органи.

2. Компетентните органи наблюдават прилагането на настоящата директива на национално равнище.

3. Всяка държава членка определя единно национално звено за контакт по сигурността на мрежите и информационните системи (наричано по-долу „единното звено за контакт“). Държавите членки могат да възложат тези функции на съществуващ орган. Когато държава членка определи само един компетентен орган, този компетентен орган изпълнява функцията и на единно звено за контакт.

4. Единното звено за контакт изпълнява функция за връзка, така че да се осигури трансграничното сътрудничество между органите на държавите членки и със съответните органи в други държави членки и с групата за сътрудничество, посочена в член 11, и с мрежата на ЕРИКС, посочена в член 12.

5. Държавите членки гарантират, че компетентните органи 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 гарантират ефективно, ефикасно и сигурно сътрудничество на определените представители в групата за сътрудничество.

6. Когато е целесъобразно и в съответствие с националното право компетентните органи и единните звена за контакт провеждат консултации и осъществяват сътрудничество със съответните национални правоприлагащи органи и национални органи за защита на данните.

7. Всяка държава членка уведомява незабавно Комисията за определянето на компетентен орган и единно звено за контакт, за техните задачи и за всякакви последващи промени във връзка с това. Всяка държава членка оповестява публично обстоятелството, че е определен компетентен орган и единно звено за контакт. 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 точка 1 от приложение I, които обхващат най-малко секторите, посочени в приложение II, и услугите, посочени в приложение III, които отговарят за предприемането на действия при инциденти и рискове в съответствие с подробно определена процедура,. ЕРИКС може да бъде създаден в рамките на компетентен орган.

2. Държавите членки гарантират, че ЕРИКС разполагат с достатъчни ресурси, за да изпълняват ефективно задачите си, установени в точка 2 от приложение I.

   Държавите членки гарантират, че чрез мрежата на ЕРИКС, посочена в член 12, техните ЕРИКС си сътрудничат ефективно, ефикасно и сигурно.

3. Държавите членки гарантират, че ЕРИКС имат достъп до подходяща, сигурна и устойчива комуникационна и информационна инфраструктура на национално равнище.

4. Държавите членки информират Комисията за обхвата на задачите на ЕРИКС, както и за основните елементи от тяхната процедура за предприемане на действия при инциденти.

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

Член 10

Сътрудничество на национално равнище

1. Ако са отделени, компетентният орган, 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 компетентните органи или ЕРИКС получават уведомления за инциденти, подадени съгласно настоящата директива. Ако държава членка реши, че ЕРИКС няма да получават уведомления, на ЕРИКС — до степента, необходима за изпълнението на техните задачи — се предоставя достъп до данните за инцидентите, за които са постъпили уведомления от операторите на основни услуги съгласно член 14, параграфи 3 и 5 или от доставчиците на цифрови услуги съгласно член 16, параграфи 3 и 6.

3. Държавите членки гарантират, че компетентните органи или ЕРИКС информират единните звена за контакт за уведомленията за инциденти, подадени съгласно настоящата директива.

   До ... [24 месеца след датата на влизане в сила на настоящата директива], а след това — веднъж годишно, единното звено за контакт представя обобщен доклад до групата за сътрудничество относно получените уведомления, включително броя уведомления и естеството на инцидентите, за които са подадени уведомленията, и относно действията, предприети в съответствие с член 14, параграфи 3 и 5 и член 16, параграфи 3 и 6.

ГЛАВА III
СЪТРУДНИЧЕСТВО

Член 11

Група за сътрудничество

1. Създава се група за сътрудничество с цел да се подпомага и улеснява стратегическото сътрудничество и обмена на информация между държавите членки и да се изгражда доверие и с оглед постигането на високо общо ниво на сигурност на мрежите и информационните системи в Съюза.

   Групата за сътрудничество изпълнява задачите си въз основа на двугодишните работни програми, посочени в параграф 3, втора алинея.

2. Групата за сътрудничество се състои от представители на държавите членки, Комисията и ENISA.

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

   Комисията осигурява административното обслужване.

3. Групата за сътрудничество изпълнява следните задачи:

   а) осигуряване на стратегически насоки за дейностите на мрежата на ЕРИКС, създадена съгласно член 12;

б) обмен на най-добри практики относно обмена на информация, свързана с уведомяването за инциденти, посочено в член 14, параграфи 3 и 5 и член 16, параграфи 3 и 6;

в) обмен на най-добри практики между държавите членки и, в сътрудничество с ENISA, подпомагане на държавите членки при изграждането на капацитет в областта на сигурността на мрежите и информационните системи;

г) обсъждане на капацитета и подготвеността на държавите членки и, на доброволна основа, оценка на националните стратегии относно сигурността на мрежите и информационните системи и ефективността на ЕРИКС, и набелязване на най-добри практики;

д) обмен на информация и най-добри практики в областта на повишаването на осведомеността и обучението;

е) обмен на информация и най-добри практики в областта на научноизследователската и развойната дейност относно сигурността на мрежите и информационните системи;

ж) когато е приложимо, обмен на опит по въпроси, свързани със сигурността на мрежите и информационните системи, със съответните институции, органи, служби и агенции на Съюза;

з) обсъждане на стандартите и спецификациите, посочени в член 19, с представители от съответните европейски организации по стандартизация;

и) събиране на информация за най-добри практики относно рисковете и инцидентите;

й) преглед на годишна основа на обобщените доклади, посочени в член 10, параграф 3, втора алинея;

к) обсъждане на работата, предприета във връзка с ученията в областта на сигурността на мрежите и информационните системи, образователните програми и обучението, включително работата на ENISA;

л) с помощта на ENISA, обмен на най-добри практики относно определянето на операторите на основни услуги от държавите членки, включително по отношение на трансграничната зависимост, свързана с рисковете и инцидентите;

м) обсъждане на правилата за докладване на уведомленията за инциденти, посочени в членове 14 и 16.

До ... [18 месеца след влизането 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 осъществяване на нейните цели и задачи, която е съобразена с целите на настоящата директива

4. За целите на прегледа, посочен в член 23, до … [24 месеца след датата на влизане в сила на настоящата директива] и на всяка година и половина след това групата за сътрудничество подготвя доклад за оценка на опита, придобит чрез стратегическото сътрудничество, осъществявано съгласно настоящия член.

5. Комисията установява 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 22, параграф 2.

За целите на първа алинея Комисията представя първия проект на акт за изпълнение на комитета, посочен в член 22, параграф 1, до ... [6 месеца след влизането в сила на настоящата директива].

Член 12

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.

2. Мрежата на ЕРИКС се състои от представители на ЕРИКС на държавите членки 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 услугите, операциите и способностите за сътрудничество на ЕРИКС;

   б) по искане на представител на ЕРИКС на държава членка, която е възможно да е засегната от инцидент — обмен и обсъждане на нетърговски чувствителна информация, свързана с този инцидент, и съпътстващите го рискове; въпреки това всеки ЕРИКС на държава членка може да откаже да участва в това обсъждане, ако съществува риск да бъде засегнато разследването на инцидента;

в) обмен и предоставяне на доброволна основа на неповерителна информация относно отделни инциденти;

г) по искане на представител на ЕРИКС на държава членка — обсъждане и, при възможност, набелязване на координирана реакция на инцидент, констатиран в рамките на юрисдикцията на същата държава членка;

д) оказване на подкрепа на държавите членки за справяне с трансгранични инциденти въз основа на доброволната им взаимопомощ;

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

i) категории рискове и инциденти;

ii) ранни предупреждения;

iii) взаимопомощ;

iv) принципи и условия за координация, когато държавите членки реагират на трансгранични рискове и инциденти;

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

з) обсъждане на поуките, извлечени от ученията в областта на сигурността на мрежите и информационните системи, включително от организираните от ENISA;

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

й) отправяне 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 прегледа, посочен в член 23, до … [24 месеца след датата на влизане в сила на настоящата директива] и на всяка година и половина след това мрежата на ЕРИКС изготвя доклад за оценка на опита, придобит чрез осъществяваното съгласно настоящия член оперативно сътрудничество, включително заключения и препоръки. Този доклад се представя и на групата за сътрудничество.

5. Мрежата на ЕРИКС установява своя процедурен правилник.

Член 13

Международно сътрудничество

Съюзът може да сключва международни споразумения в съответствие с член 218 ДФЕС с трети държави или международни организации, които допускат и уреждат участието им в някои дейности на групата за сътрудничество. Подобни споразумения са съобразени с необходимостта да се гарантира надеждна защита на данните.

ГЛАВА IV
СИГУРНОСТ НА МРЕЖИТЕ И ИНФОРМАЦИОННИТЕ СИСТЕМИ НА ОПЕРАТОРИТЕ НА ОСНОВНИ УСЛУГИ

Член 14

Изисквания за сигурност и уведомяване за инциденти

1. Държавите членки гарантират, че операторите на основни услуги предприемат подходящи и пропорционални технически и организационни мерки за управление на рисковете за сигурността на мрежите и информационните системи, използвани от операторите за дейността им. Тези мерки осигуряват ниво на сигурност на мрежите и информационните системи, съответстващо на съществуващия риск, съобразно последните постижения в тази област.

2. Държавите членки гарантират, че операторите на основни услуги предприемат подходящи мерки за предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи сигурността на мрежите и информационните системи, които се използват за предоставянето на тези основни услуги, с цел осигуряване на непрекъснатост на тези услуги.

3. Държавите членки гарантират, че операторите на основни услуги уведомяват без неоправдано забавяне компетентния орган или ЕРИКС за инцидентите, които имат значително въздействие върху непрекъснатостта на предоставяните от тях основни услуги. Уведомленията включват информация, която дава възможност на компетентния орган или на ЕРИКС да определи евентуалното трансгранично въздействие на инцидента. Уведомлението не води до повишена отговорност за уведомяващия.

4. С цел да се определи значимостта на въздействието на даден инцидент се вземат по-специално предвид следните показатели:

а) броят потребители, засегнати от нарушаването на основната услуга;

б) продължителността на инцидента;

в) географският обхват по отношение на областта, засегната от инцидента.

5. Въз основа на информацията, предоставена в уведомлението от оператора на основни услуги, компетентният орган или ЕРИКС информира другата (другите) засегната (засегнати) държава(и) членка(и), ако инцидентът има значително въздействие върху непрекъснатостта на основните услуги в тази държава членка. При това компетентният орган или ЕРИКС запазва сигурността и търговските интереси на оператора на основните услуги, както и поверителността на информацията, съдържаща се в уведомлението му, в съответствие с правото на Съюза или с националното законодателство, което е в съответствие с правото на Съюза.

Когато обстоятелствата го позволяват, компетентният орган или ЕРИКС предоставя на подалия уведомлението оператор на основни услуги съответната информация във връзка с последващите действия по уведомлението за инцидент, като например информация, която би спомогнала за предприемането на ефективни действия при инцидента.

По искане на компетентния орган или ЕРИКС единното звено за контакт предава посочените в първа алинея уведомления на единните звена за контакт на други засегнати държави членки.

6. След консултация с уведомяващия оператор на основни услуги уведоменият компетентен орган или ЕРИКС може да информира обществеността за отделни инциденти, когато е необходима обществена осведоменост с цел предотвратяване на инцидент или справяне с текущ инцидент.

7. Компетентните органи, като действат съвместно в рамките на групата за сътрудничество, могат да разработят и приемат насоки относно обстоятелствата, при които от операторите на основни услуги се изисква да уведомяват за инциденти, включително показателите за определяне значимостта на въздействието на даден инцидент, посочени в параграф 4.

Член 15

Прилагане и изпълнение

1. Държавите членки гарантират, че компетентните органи разполагат с всички необходими правомощия и средства за оценяване на това дали операторите на основни услуги изпълняват задълженията си по член 14 и на въздействието от това изпълнение върху сигурността на мрежите и информационните системи.

2. Държавите членки гарантират, че компетентните органи разполагат с правомощия и средства, за да изискват от операторите на основни услуги да предоставят:

   а) информацията, необходима за оценка на сигурността на техните мрежи и информационни системи, включително съществуващи политики за сигурност;

б) доказателства за ефективното изпълнение на политиките за сигурност, като например резултатите от одит на сигурността, извършван от компетентния орган или от квалифициран одитор, а във втория случай — да предоставят на компетентния орган резултатите от одита, включително доказателствата, на които той се основава.

В искането за подобна информация или доказателства компетентните органи посочват целта на искането и уточняват каква информация се изисква.

3. След оценяването на информацията или на резултатите от одитите на сигурността, посочени в параграф 2, компетентният орган може да даде задължителни указания на операторите на основни услуги с цел отстраняване на установените пропуски.

4. Компетентният орган работи в тясно сътрудничество с органите за защита на данните при работа по инцидентите, които водят до нарушаване на сигурността на лични данни.

ГЛАВА V
СИГУРНОСТ НА МРЕЖИТЕ И ИНФОРМАЦИОННИТЕ СИСТЕМИ НА ДОСТАВЧИЦИТЕ НА ЦИФРОВИ УСЛУГИ

Член 16

Изисквания за сигурност и уведомяване за инциденти

1. Държавите членки гарантират, че доставчиците на цифрови услуги установяват и предприемат подходящи и пропорционални технически и организационни мерки за управление на рисковете за сигурността на мрежите и информационните системи, използвани от тези доставчици в контекста на предоставянето на услугите, посочени в приложение III, в Съюза. Тези мерки осигуряват ниво на сигурност на мрежите и информационните системи, съответстващо на съществуващия риск, съобразно последните постижения в тази област и са съобразени със следните елементи:

   а) сигурност на системите и съоръженията;

   б) действия при инциденти;

   в) управление на непрекъснатостта на дейностите;

   г) наблюдение, одит и изпитване;

   д) спазване на международни стандарти.

2. Държавите членки гарантират, че доставчиците на цифрови услуги предприемат мерки с цел предотвратяване и намаляване до минимум на въздействието на инцидентите, засягащи сигурността на техните мрежи и информационни системи, върху услугите, посочени в приложение III и предлагани в Съюза, с цел осигуряване на непрекъснатост на тези услуги.

3. Държавите членки гарантират, че доставчиците на цифрови услуги уведомяват без неоправдано забавяне компетентния орган или ЕРИКС за всеки инцидент, който има съществено въздействие върху предоставянето от тях на услуга, посочена в приложение III, която те предлагат в Съюза. Уведомленията включват информация, която дава възможност на компетентния орган или на ЕРИКС да определи значимостта на евентуалното трансгранично въздействие на инцидента. Уведомлението не води до повишена отговорност за уведомяващия.

4. За да се определи дали въздействието на даден инцидент е съществено, се вземат по-специално предвид следните показатели:

   а) броят ползватели, засегнати от инцидента, и по-специално ползвателите, които разчитат на услугата за предоставяне на собствените си услуги;

   б) продължителността на инцидента;

   в) географският обхват по отношение на областта, засегната от инцидента;

   г) степента на нарушаване на функционирането на услугата;

   д) степента на въздействие върху стопанските и обществени дейности.

Задължението за уведомяване за инцидент се прилага само когато доставчикът на цифрови услуги има достъп до информацията, която е необходима, за да се оцени въздействието на инцидента спрямо показателите по първа алинея.

5. Когато даден оператор на основни услуги разчита на доставчик на цифрови услуги, който е трето лице, за да предоставя услуга от основно значение за поддържането на особено важни обществени и стопански дейности, този оператор уведомява за всяко значително въздействие върху непрекъснатостта на основните услуги, дължащо се на инцидент, засягащ доставчика на цифрови услуги.

6. Когато е целесъобразно и особено ако инцидентът, посочен в параграф 3, засяга две или повече държави членки, компетентният орган или ЕРИКС информира другите засегнати държави членки. При това компетентните органи, ЕРИКС и единните звена за контакт запазват сигурността и търговските интереси на доставчика на цифрови услуги, 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. След консултация със засегнатия доставчик на цифрови услуги компетентният орган или ЕРИКС и, когато е приложимо, органите или ЕРИКС на други засегнати държави членки може да информират обществеността за отделни инциденти или да изискат от доставчика на цифрови услуги да направи това, когато е необходима обществена осведоменост с цел предотвратяване на инцидент или справяне с текущ инцидент или когато разкриването на инцидента е в интерес на обществеността поради други причини.

8. На Комисията се предоставя правомощието да приема актове за изпълнение за допълнително конкретизиране на елементите, посочени в параграф 1, и на показателите, посочени в параграф 4 от настоящия член. Тези актове за изпълнение се приемат до ... [1 година след влизането в сила на настоящата директива] в съответствие с процедурата по разглеждане, посочена член 22, параграф 2.

9. Комисията може да приеме актове за изпълнение за установяване на форматите и процедурите, приложими към изискванията за уведомяване. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 22, параграф 2.

10. Без да се засяга член 1, параграф 6, държавите членки не налагат на доставчиците на цифрови услуги никакви други изисквания за сигурност или уведомяване.

11. Глава V не се прилага за микро- и малките предприятия съгласно определението в Препоръка 2003/361/ЕО[1] на Комисията.

Член 17

Прилагане и изпълнение

1. Държавите членки гарантират, че компетентните органи предприемат действия, ако е необходимо, посредством последващи надзорни мерки, когато получат доказателства, че даден доставчик на цифрови услуги не отговаря на изискванията, установени в член 16. Тези доказателства могат да се предоставят от компетентен орган на друга държава членка, в която се предоставя услугата.

[1] 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).

2. За целите на параграф 1 компетентните органи разполагат с необходимите правомощия и средства да изискват от доставчиците на цифрови услуги:

а) да предоставят информацията, необходима за оценка на сигурността на техните мрежи и информационни системи, включително съществуващи политики за сигурност;

б) да отстраняват всеки пропуск в изпълнението на изискванията, предвидени в член 16.

3. Ако даден доставчик на цифрови услуги има основно място на установяване или представител в държава членка, но неговите мрежи и информационни системи са разположени в една или повече други държави членки, компетентният орган на държавата членка на основното място на установяване или на представителя и компетентните органи на тези други държави членки си сътрудничат и се подпомагат взаимно, ако е необходимо. Тази помощ и сътрудничество може да обхващат обмена на информация между съответните компетентни органи и исканията за предприемане на надзорните мерки, посочени в параграф 2.

Член 18

Юрисдикция и териториалност

1. За целите на настоящата директива се приема, че даден доставчик на цифрови услуги е под юрисдикцията на държавата членка, в която е основното му място на установяване. Приема се, че основното място на установяване на доставчик на цифрови услуги е в дадена държава членка, ако главното му управление е в тази държава членка.

2. Доставчик на цифрови услуги, който не е установен в Съюза, но предлага в Съюза услугите, посочени в приложение III, определя представител в Съюза. Представителят трябва да е установен в една от държавите членки, в които се предлагат услугите. Приема се, че доставчикът на цифрови услуги е под юрисдикцията на държавата членка, в която е установен представителят.

3. Определянето на представител от доставчика на цифрови услуги не засяга съдебните производства, които биха могли да бъдат започнати срещу самия доставчик на цифрови услуги.

ГЛАВА VI
СТАНДАРТИЗАЦИЯ И ДОБРОВОЛНО УВЕДОМЯВАНЕ

Член 19

Стандартизация

1. С цел насърчаване на еднообразното прилагане на член 14, параграфи 1 и 2 и на член 16, 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 20

Доброволно уведомяване

1. Без да се засяга член 3, субекти, които не са били определени като оператори на основни услуги и не са доставчици на цифрови услуги, може да уведомяват на доброволна основа за инциденти, които имат значително въздействие върху непрекъснатостта на предоставяните от тях услуги.

2. При обработването на уведомленията държавите членки действат в съответствие с процедурата по член 14. Държавите членки могат да обработват задължителните уведомления с предимство пред доброволните уведомления. Доброволните уведомления се обработват само когато обработването им не представлява несъразмерна или неоправдана тежест за съответните държави членки.

   Доброволното уведомяване не трябва да води до налагане на задължения за уведомяващия субект, каквито не биха му били наложени, ако не беше подал уведомлението.

ГЛАВА VII
ЗАКЛЮЧИТЕЛНИ РАЗПОРЕДБИ

Член 21

Санкции

Държавите членки установяват система от санкции, приложими при нарушение на националните разпоредби, приети съгласно настоящата директива, и вземат всички необходими мерки за осигуряване на тяхното прилагане. Предвидените санкции са ефективни, пропорционални и възпиращи. До … [21 месеца след датата на влизане в сила на настоящата директива] държавите членки уведомяват Комисията за тази система и мерки и я уведомяват незабавно за всяко последващо изменение, което ги засяга.

Член 22

Процедура на комитет

1. Комисията се подпомага от Комитета по сигурност на мрежите и информационните системи. 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.

Член 23

Преглед

1. До … [33 месеца след датата на влизане в сила на настоящата директива] Комисията представя на Европейския парламент и на Съвета доклад за оценка на последователността на подхода, възприет от държавите членки при определянето на операторите на основни услуги.

2. Комисията периодично прави преглед на действието на настоящата директива и докладва на Европейския парламент и Съвета. За тази цел и с оглед на допълнителното засилване на стратегическото и оперативното сътрудничество Комисията взема предвид докладите на групата за сътрудничество и мрежата на ЕРИКС за натрупания опит на стратегическо и оперативно равнище. В своя преглед Комисията прави също така оценка на списъците, съдържащи се в приложения II и III, и на последователността при определянето на операторите на основни услуги и на услугите в секторите, посочени в приложение II. Първият доклад се предава до… [57 месеца след датата на влизане в сила на настоящата директива].

Член 24

Преходни мерки

1. Без да се засяга член 25 и с цел на държавите членки да се осигурят допълнителни възможности за подходящо сътрудничество по време на периода на транспониране, групата за сътрудничество и мрежата на ЕРИКС започват да изпълняват задачите си, установени съответно в член 11, параграф 3 и член 12, параграф 3, до … [6 месеца след датата на влизане в сила на настоящата директива].

2. В периода от … [6 месеца след датата на влизане в сила на настоящата директива] до … [27 месеца след датата на влизане в сила на настоящата директива] и с цел оказването на подкрепа на държавите членки при възприемането на последователен подход в процеса на определяне на операторите на основни услуги, групата за сътрудничество обсъжда процеса, същността и вида на националните мерки, даващи възможност за определяне на операторите на основни услуги в конкретен сектор в съответствие с критериите, посочени в членове 5 и 6. По искане на държава членка групата за сътрудничество обсъжда също така конкретни проекти на национални мерки на тази държава членка, даващи възможност за определяне на операторите на основни услуги в конкретен сектор в съответствие с критериите, посочени в членове 5 и 6.

3. До … [6 месеца след датата на влизане в сила на настоящата директива] и за целите на настоящия член държавите членки осигуряват подходящо представителство в групата за сътрудничество и в мрежата на ЕРИКС.

Член 25

Транспониране

1. Държавите членки приемат и публикуват до ... [21 месеца след датата на влизане в сила на настоящата директива] законовите, подзаконовите и административните разпоредби, необходими, за да се съобразят с директивата. Те незабавно информират Комисията за това.

   Те прилагат тези разпоредби, считано от … [един ден след датата, посочена в първа алинея].

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.

2. Държавите членки съобщават на Комисията текста на основните разпоредби от националното право, които те приемат в областта, уредена с настоящата директива.

Член 26

Влизане в сила

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

Член 27

Адресати

Адресати на настоящата директива са държавите членки.

Съставено в

За Европейския парламент	*За Съвета*
Председател	*Председател*

ПРИЛОЖЕНИЕ I

Изисквания към и задачи на екипите за реагиране при инциденти с компютърната сигурност (ЕРИКС)

Изискванията към ЕРИКС и техните задачи се определят по подходящ и ясен начин, като в тяхна подкрепа има национални политики и/или нормативна уредба. Те включват следното:

1) Изисквания към ЕРИКС

   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. Комуникационните канали трябва да бъдат също така ясно посочени и добре известни на конституентите и на партньорите от сътрудничеството.

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

   в) Непрекъснатост на дейността:

      i) ЕРИКС разполагат с подходяща система за управление и разпределяне на заявките с цел да се улесни предаването на задачите от един на друг изпълнител;

      ii) ЕРИКС разполагат с достатъчен персонал, който да гарантира, че са постоянно на разположение;

      iii) ЕРИКС разчитат на инфраструктура с гарантирана непрекъснатост на дейността. За тази цел има на разположение резервни системи и резервно работно пространство;

г) ЕРИКС имат възможността да участват в международни мрежи за сътрудничество, когато желаят това.

2) Задачи на ЕРИКС

а) Задачите на ЕРИКС включват най-малко следните елементи:

i) наблюдение на инциденти на национално равнище;

ii) подаване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за инциденти и рискове сред съответните конституенти;

iii) реагиране на инциденти;

iv) осигуряване на динамичен анализ на рисковете и инцидентите и информация за текущата ситуация;

v) участие в мрежата на ЕРИКС;

б) ЕРИКС изграждат отношения на сътрудничество с частния сектор;

в) с цел улесняване на сътрудничеството ЕРИКС насърчават възприемането и използването на общи практики за стандартизация за:

i) процедури за предприемане на действия при инциденти и рискове;

ii) схеми за класификация на инциденти, рискове и информация.

ПРИЛОЖЕНИЕ II

Категории субекти за целите на член 4, точка 4

Сектор:	Подсектор:	Категория субект
1. Енергетика	а) Електроенергия	– електроенергийни предприятия по смисъла на член 2, точка 35 от Директива 2009/72/ЕО на Европейския парламент и на Съвета[1], което изпълнява функцията „доставка“ по смисъла на член 2, точка 19 от посочената директива
		– оператори на разпределителна система по смисъла на член 2, точка 6 от Директива 2009/72/ЕО
		– оператори на преносна система по смисъла на член 2, точка 4 от Директива 2009/72/ЕО
	б) Нефт	– оператори на нефтопроводи
		– оператори на съоръжения за добив, рафиниране и преработка, съхранение и пренос на нефт

[1] Директива 2009/72/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. относно общите правила за вътрешния пазар на електроенергия и за отмяна на Директива 2003/54/ЕО (ОВ L 211, 14.8.2009 г., стр. 55).

Сектор:	Подсектор:	Категория субект
	в) Природен газ	– предприятия за доставка по смисъла на член 2, точка 8 от Директива 2009/73/ЕО на Европейския парламент и на Съвета[1]
		– оператори на газоразпределителна система по смисъла на член 2, точка 6 от Директива 2009/73/ЕО
		– оператори на газопреносна система по смисъла на член 2, точка 4 от Директива 2009/73/ЕО
		– оператори на система за съхранение по смисъла на член 2, точка 10 от Директива 2009/73/ЕО
		– оператори на система за ВПГ по смисъла на член 2, точка 12 от Директива 2009/73/ЕО
		– предприятия за природен газ по смисъла на член 2, точка 1 от Директива 2009/73/ЕО
		– оператори на съоръжения за рафиниране и преработка на природен газ

[1] Директива 2009/73/ЕО на Европейския парламент и на Съвета от 13 юли 2009 г. 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).

Сектор:	Подсектор:	Категория субект
2. Транспорт	а) Въздушен транспорт	– въздушни превозвачи по смисъла на член 3, точка 4 от Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета[1]
		– управляващи летищата органи по смисъла на член 2, точка 2 от Директива 2009/12/ЕО на Европейския парламент и на Съвета[2], летища по смисъла на член 2, точка 1 от посочената директива, включително летища, изброени в раздел 2 от приложение II към Регламент (ЕС) № 1315/2013 на Европейския парламент и на Съвета[3]; както и субекти, които експлоатират помощни инсталации, намиращи се в рамките на летището.
		– оператори по контрола на управлението на движението, осъществяващи обслужване по контрол на въздушното движение (КВД) по смисъла на член 2, точка 1 от Регламент (ЕО) № 549/2004 на Европейския парламент и на Съвета[4]

[1] Регламент (ЕО) № 300/2008 на Европейския парламент и на Съвета от 11 март 2008 г. 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).

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

[3] Регламент (ЕС) № 1315/2013 на Европейския парламент и на Съвета от 11 декември 2013 г. 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).

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

Сектор:	Подсектор:	Категория субект
	б) Железопътен транспорт	– управители на инфраструктура по смисъла на член 3, точка 2 от Директива 2012/34/ЕС на Европейския парламент и на Съвета[1]
		– железопътни предприятия по смисъла на член 3, точка 1 от Директива 2012/34/ЕС, включително оператори на обслужващи съоръжения по смисъла на член 3, точка 12 от Директива 2012/34/ЕС
	в) Воден транспорт	– предприятия за вътрешноводен, морски и крайбрежен транспорт на пътници и товари съгласно определението за морски транспорт в приложение I към Регламент (ЕО) № 725/2004 на Европейския парламент и на Съвета[2], с изключение на отделните кораби, експлоатирани от тези предприятия
		– управителните органи на пристанища по смисъла на член 3, точка 1 от Директива 2005/65/ЕО на Европейския парламент и на Съвета[3], включително техните пристанищни съоръжения по смисъла на член 2, точка 11 от Регламент (ЕО) № 725/2004; както и субекти, експлоатиращи инсталации и оборудване, разположено в рамките на пристанището

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

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

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

Сектор:	Подсектор:	Категория субект
		– операторите на службата по морския трафик по смисъла на член 3, буква о) от Директива 2002/59/ЕО на Европейския парламент и на Съвета[1]
	г) Автомобилен транспорт	– пътни органи по смисъла на член 2, точка 12 от Делегиран регламент (ЕС) № 2015/962 на Комисията[2], които отговарят за контрола на управлението на движението
		– операторите на интелигентни транспортни системи по смисъла на член 4, точка 1 от Директива 2010/40/ЕС на Европейския парламент и на Съвета[3]
3. Банково дело		– кредитни институции по смисъла на член 4, параграф 1, точка 1 от Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета[4]

[1] Директива 2002/59/ЕО на Европейския парламент и на Съвета от 27 юни 2002 г. 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).

[2] Делегиран регламент (ЕС) № 2015/962 на Комисията от 18 декември 2014 г. 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).

[3] Директива 2010/40/ЕС на Европейския парламент и на Съвета от 7 юли 2010 г. 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).

[4] Регламент (ЕС) № 575/2013 на Европейския парламент и на Съвета от 26 юни 2013 г. 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).

Сектор:	Подсектор:	Категория субект
4. Инфраструктури на финансовия пазар		– операторите на местата за търговия по смисъла на член 4, точка 24 от Директива 2014/65/ЕС на Европейския парламент и на Съвета[1]
		– централни контрагенти (ЦК) по смисъла на член 2, точка 1 от Регламент (ЕС) № 648/2012 на Европейския парламент и на Съвета[2]
5. Здравеопазване	Здравни заведения (включително болници и частни клиники)	Доставчици на здравно обслужване по смисъла на член 3, буква ж) Директива 2011/24/ЕС на Европейския парламент и на Съвета[3]
6. Доставка и снабдяване с питейна вода		Доставчици и снабдители с води, предназначени за консумация от човека по смисъла на член 2, параграф 1, буква а) от Директива 98/83/ЕО на Съвета[4], с изключение на снабдителите, за които снабдяването с води, предназначени за консумация от човека, е само част от общата им дейност за снабдяване с блага и стоки, които не се считат за основни услуги.
7. Цифрова инфраструктура		– ТОИ
		– Доставчици на DNS услуги
		– Регистри на имената на домейни от първо ниво

---

[1] 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).

[2] 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).

[3] 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).

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

ПРИЛОЖЕНИЕ III

Видове цифрови услуги за целите на член 4, точка 5

1. Онлайн място за търговия

2. Онлайн търсачка

3. Компютърни услуги „в облак“