ЕВРОПЕЙСКИ ПАРЛАМЕНТ 2009 - 2014

Консолидиран законодателен документ

13.3.2014 EP-PE_TC1-COD(2013)0027

***I

ПОЗИЦИЯ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ

приета на първо четене на 13 март 2014 г. с оглед приемането на Директива 2014/.../ЕС на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност в Съюза
(EP-PE_TC1-COD(2013)0027)

PE 505.562

ПОЗИЦИЯ НА ЕВРОПЕЙСКИЯ ПАРЛАМЕНТ

приета на първо четене на 13 март 2014 г.

с оглед приемането на Директива 2014/.../ЕС на Европейския парламент и на Съвета относно мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност 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 C 271, 19.9.2013 г., стр. 133.

2 Позиция на Европейския парламент от 13 март 2014 г.

като имат предвид, че:

(1) Мрежовите и информационните системи и услуги имат изключително важна роля в обществото. Тяхната надеждност и сигурност са от основно значение за ***свободата и цялостната сигурност на гражданите на Съюза, както и за*** стопанските дейности и общественото благополучие и особено за функционирането на вътрешния пазар. **[Изм. 1]**

(2) Мащабите***, честотата и въздействието*** на ~~нарочно предизвиканите или случайно настъпили инциденти~~ ***инцидентите*** в сигурността ~~и честотата, с която~~ се ~~появяват те,~~ се увеличават и представляват крупна заплаха пред функционирането на мрежите и информационните системи. ***Тези системи могат също да се превърнат в лесна мишена за нарочно предизвикани злонамерени действия, имащи за цел да навредят на функционирането на системите или да го прекъснат.*** Подобни инциденти могат да попречат на осъществяването на стопански дейности, да причинят значителни финансови загуби, да подкопаят доверието на потребителите и ***инвеститорите,*** да причинят големи вреди на икономиката на Съюза ***и в крайна сметка да поставят под заплаха благосъстоянието на гражданите на Съюза и способността на държавите членки да се защитават и да гарантират сигурността на критичните инфраструктури***. **[Изм. 2]**

(3) Като комуникационен инструмент без граници цифровите информационни системи и най-вече интернет играят основна роля за улесняването на трансграничното движение на стоки, услуги и хора. Поради транснационалния характер на тези системи значителните нарушения в дейността им в една държава членка могат да засегнат и други държави членки, както и Съюза като цяло. Устойчивостта и стабилността на мрежите и информационните системи е поради това от основно значение за безпроблемното функциониране на вътрешния пазар.

(3a) Тъй като често причините за повреди в системата продължават да са неумишлени, като природни бедствия или човешка грешка, инфраструктурата следва да е устойчива както на умишлени, така и на неумишлени нарушения, а операторите на критичната инфраструктура следва да създадат основани на устойчивост системи. **[Изм. 3]**

(4) На равнището на Съюза следва да бъде изграден механизъм за сътрудничество, който да дава възможност за обмен на информация и ~~координирано~~ ***координирана превенция,*** откриване и отговор във връзка с мрежовата и информационна сигурност („МИС“). За да бъде ефективен и приобщаващ този механизъм, е от основно значение всички държави членки да разполагат с минимален капацитет и със стратегия, гарантираща високо равнище на МИС на тяхна територия. ***Поне*** към ~~публичните администрации и операторите на критична информационна~~ ***определени участници на пазара в областта на информационната*** инфраструктура следва да се прилагат и минимални изисквания по отношение на сигурността с цел да се насърчава култура на управление на риска и да се гарантира докладването на най-сериозните инциденти. ***Дружествата, регистрирани за борсова търговия, следва да бъдат насърчавани да оповестяват инцидентите в своите финансови доклади на доброволна основа. Правната рамка следва да се основава на необходимостта от защита на неприкосновеността на личния живот и неприкосновеността на гражданите. Предупредителната информационна мрежа за критичната инфраструктура (ПИМКИ) следва да бъде разширена и да обхване участниците на пазара, обхванати от настоящата директива.*** **[Изм. 4]**

(4а) ***Докато поради своята обществена мисия публичните администрации следва да полагат дължима грижа в управлението и защитата на собствените си мрежи и информационни системи, настоящата директива следва да се съсредоточи върху критичната инфраструктура, която е от основно значение за поддържането на особено важни икономически и обществени дейности в сферата на енергетиката, транспорта, банковото дело, инфраструктурите на финансовия пазар и здравеопазването. Разработващите софтуер и производителите на хардуер следва да бъдат изключени от приложното поле на настоящата директива.*** **[Изм. 5]**

(4б) ***Сътрудничеството и координацията между съответните органи на Съюза с върховния представител на Съюза по въпросите на външните работи и политиката на сигурност и заместник-председател на Комисията, натоварен с отговорността за общата външна политика и политика на сигурност и общата политика за сигурност и отбрана, както и с координатора на ЕС за борба с тероризма следва да бъдат гарантирани, когато се счита, че инцидентите със значително въздействие имат външен или терористичен характер.*** **[Изм. 6]**

(5) С цел да бъдат обхванати всички имащи отношение инциденти и рискове настоящата директива следва да се прилага за всички мрежови и информационни системи. Задълженията за публичните администрации и участниците на пазара обаче не следва да се прилагат за предприятията, предоставящи обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги по смисъла на Директива 2002/21/ЕО на Европейския парламент и на Съвета[1], които са обект на конкретните изисквания за сигурност и цялост, определени в член 13а от посочената Директива, нито към доставчиците на удостоверителни услуги.

[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).

(6) Съществуващият капацитет не е достатъчен, за да гарантира високо равнище на МИС в Съюза. Равнището на готовност на различните държави членки е твърде различно, което води до фрагментираност на подходите в различните части на Съюза. Това от своя страна е причина за нееднаква степен на защита на потребителите и стопанските субекти и подкопава общото ниво на МИС в Съюза. Отсъствието на общи минимални изисквания за ~~публичните администрации и~~ участниците на пазара от своя страна прави невъзможно изграждането на глобален и ефективен механизъм за сътрудничество на равнище Съюза. ***Университетите и изследователските центрове играят решаваща роля за стимулиране на научноизследователската и развойна дейност и новаторството в тези области и следва да им се предостави достатъчно финансиране.*** **[Изм. 7]**

(7) Поради това ефективният отговор на предизвикателствата пред сигурността на мрежовите и информационните системи изисква глобален подход на равнище Съюза, който да включва общи минимални изисквания за изграждане на капацитет и планиране, ***развиване на необходимите умения в областта на киберсигурността,*** обмен на информация и координиране на действията и общи минимални изисквания по отношение на сигурността ~~за всички имащи отношение участници на пазара и публични администрации~~. ***Минимални общи стандарти следва да се прилагат в съответствие с подходящи препоръки от страна на групите за координация по отношение на киберсигурността.*** **[Изм. 8]**

(8) Разпоредбите на настоящата директива следва да не засягат възможността всяка държава членка да предприема необходимите мерки, с които да гарантира сигурността на защитата на своите основни интереси в сферата на сигурността, да опазва публичната политика и публичната сигурност и да дава възможност 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. ***Нито една държава членка не е задължена да разкрива класифицирана информация на ЕС съгласно предвиденото в Решение 2011/292/ЕС[1], информация, която е предмет на споразумения за неразкриване на информация или неформални споразумения за неразкриване на информация, като например Протокола „Светофар“ (Traffic Light Protocol).*** **[Изм. 9]**

---

1 ***Решение 2011/292/ЕС[1] на Съвета от 31 март 2011 г. относно правилата за сигурност за защита на класифицирана информация на ЕС (ОВ L 141, 27.5.2011 г., стр. 17).***

(9) С цел постигане и поддържане на общо високо равнище на сигурност на мрежовите и информационните системи всяка държава членка следва да има национална стратегия за МИС, в която да са определени стратегическите цели и конкретните действия на политиката, които ще бъдат изпълнявани. На национално ниво ***въз основа на минималните изисквания, посочени в настоящата директива,*** следва да бъдат разработени планове за сътрудничество за МИС, които да отговарят на основните изисквания, с цел да бъдат постигнати нива на капацитет на отговора, даващи възможност в случай на инциденти за ефективно и ефикасно сътрудничество на национално равнище и на равнище Съюза***, като се зачита и защитава неприкосновеността на личния живот и личните данни***. ***Следователно всяка държава членка следва да бъде задължена да отговаря на общите стандарти относно формата на данните и заменяемостта на данните, които се споделят и оценяват. Държавите членки следва да могат да поискат помощ от Европейската агенция за мрежова и информационна сигурност (ENISA) при разработване на своите национални стратегии за МИС въз основа на общ план с минимални изисквания по отношение на стратегията за МИС***. **[Изм. 10]**

(10) С цел да се осигури възможност за ефективно изпълнение на разпоредбите, приети в съответствие с настоящата директива, във всяка държава членка следва да бъде създаден или определен орган, който да отговоря за координацията на въпросите във връзка с МИС и да бъде център за трансгранично сътрудничество. Тези органи следва да получат достатъчно технически, финансови и човешки ресурси, за да се гарантира, че са в състояние да изпълняват ефективно и ефикасно определените им задачи и по този начин да постигат целите на настоящата директива.

(10a) ***С оглед на различията в националните структури на управление и с цел да се защитят вече съществуващи секторни споразумения или надзорни и регулаторни органи на Съюза и за да се избегне дублиране, 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 участниците на пазара съгласно настоящата директива. За да се гарантира обаче гладко трансграничено сътрудничество и комуникация, е необходимо всяка държава членка, без да засяга секторните регулаторни споразумения, да определи само едно национално звено за контакт, което да отговаря за трансграничното сътрудничество на равнището на Съюза. Когато това се налага от конституционния ред или от други договорености, дадена държава членка следва да може да определи само един орган, който да изпълнява задачите на компетентния орган и на единичното звено за контакт. Компетентните органи и единичните звена за контакт следва да бъдат граждански органи, които подлежат на пълен демократичен надзор, и не следва да изпълняват никакви задачи в областта на разузнаването, правоприлагането или отбраната или под някаква форма да са организационно свързани с органи, действащи в тези области.*** **[Изм. 11]**

(11) Всички държави членки ***и участници на пазара*** следва да бъдат достатъчно добре подготвени и като технически, и като организационен капацитет да предотвратяват, реагират на и ограничават инциденти и рискове в мрежовите и информационните системи ***по всяко време***. ***Системите*** за ***сигурност на публичните администрации следва да бъдат безопасни и да подлежат на демократичен контрол и проверка. Общото необходимо оборудване и капацитет следва да бъдат в съответствие със съвместно договорените технически стандарти, както и със стандартните процедури за работа (СПО). За*** целта във всички държави членки следва да бъдат създадени добре функциониращи екипи за незабавно реагиране при компютърни инциденти ***(CERT)***, отговарящи на основни изисквания, които да гарантират наличието на ефективен и съвместим капацитет за справяне с инциденти и рискове и да осигуряват ефикасно сътрудничество на равнище Съюза. ***Тези CERT следва да могат да си взаимодействат въз основа на общите технически стандарти и СПО. С оглед на различните характеристики на съществуващите CERT, които отговарят на различни субективни нужди и участници, държавите членки следва да гарантират, че за всеки един от секторите, включени в списъка на участниците на пазара, посочен в настоящата директива, се предоставят услуги от поне един CERT. По отношение на трансграничното сътрудничество между CERT държавите членки следва да гарантират, че CERT разполагат с достатъчно средства, за да участват в съществуващите вече действащи международни и европейски мрежи за сътрудничество.*** **[Изм. 12]**

(12) Като използват значителния напредък, постигнат в рамките на Европейския форум за държавите членки (ЕФДЧ) при насърчаването на дискусиите и обмена на добри практики в политиките, включително разработването на принципи на европейското сътрудничество при киберкризи, държавите членки и Комисията следва да създадат мрежа, която да им осигурява постоянна комуникация и да оказва подкрепа на тяхното сътрудничество. Този сигурен и ефикасен механизъм за сътрудничество**,** ***включващ по целесъобразност участието на участниците на пазара,*** следва да дава възможност за структуриран и координиран обмен на информация, откриване и отговор на ~~равнище~~ ***равнището на*** Съюза. **[Изм. 13]**

(13) ~~Европейската агенция за мрежова и информационна сигурност („~~ENISA~~“)~~ следва да оказва подкрепа на държавите членки и на Комисията, като предоставя на разположение своите експертни познания и консултации и улеснява обмена на най-добри практики. Комисията ***и държавите членки*** по-специално следва да се ~~консултира~~ ***консултират*** с ENISA при прилагането на настоящата директива. За да се осигури навременна и ефикасна информация за държавите членки и Комисията, в рамките на мрежата за сътрудничество следва да се подават ранни предупреждения за инциденти и рискове. С цел у държавите членки да бъдат натрупани познания и изграден капацитет мрежата за сътрудничество следва да служи и като инструмент за обмен на най-добри практики, които да подпомагат нейните членове в изграждането на капацитет и да направляват организирането на партньорски проверки и учения за МИС. **[Изм. 14]**

(13а) По целесъобразност държавите членки следва да могат да използват или да адаптират съществуващите организационни структури или стратегии при прилагането на разпоредбите на настоящата директива. **[Изм. 15]**

(14) Следва да се създаде сигурна инфраструктура за обмен на информация, която да дава възможност за предаване на чувствителна и поверителна информация в мрежата за сътрудничество. ***Съществуващите структури в рамките на Съюза следва да бъдат изцяло използвани за тази цел.*** Без да се засяга задължението на държавите членки да уведомяват в мрежата за сътрудничество за инциденти и рискове, чието измерение е от мащабите на Съюза, достъпът до поверителна информация от други държави членки следва да се предоставя само на държави членки, които са доказали, че техните технически, финансови и човешки ресурси и процедури, както и тяхната комуникационна инфраструктура гарантират тяхното ефикасно, ефективно и сигурно участие в мрежата***, като използват прозрачни методи***. **[Изм. 16]**

(15) Тъй като повечето мрежови и информационни системи се експлоатират от частни субекти, сътрудничеството между публичния и частния сектор е от основно значение. Участниците на пазара следва да бъдат насърчавани да развиват свои собствени механизми за неофициално сътрудничество за гарантиране на МИС. Те следва също така да си сътрудничат с публичния сектор и ***взаимно*** да обменят информация и най-добри практики***, включително реципрочност*** в ~~размяна~~ ***размяната*** на ***относима информация и*** оперативна подкрепа***, както и анализирана от стратегическа гледна точка информация*** в случай на инциденти. ***С цел ефективно насърчаване на споделянето на информация и най-добри практики от основно значение е да се гарантира, че участниците на пазара, които се включват в такава размяна, не са ощетени в резултат на сътрудничеството си. Необходими са достатъчно защитни мерки, за да се гарантира, че подобно сътрудничество няма да изложи тези участници на по-висок риск, свързан със спазването на изискванията, или да доведе до нови задължения съгласно, inter alia, правото в областта на конкуренцията, интелектуалната собственост, защитата на данни или киберпрестъпността, нито ще ги изложи на по-големи рискове във връзка с тяхното функциониране или сигурност.*** **[Изм. 17]**

(16) С цел да се гарантира прозрачност и надлежно информиране на гражданите на ~~ЕС~~ ***Съюза*** и участниците на пазара ~~компетентните органи~~ ***единичните звена за контакт*** следва да създадат общ уебсайт ***за целия Съюз***, на който да публикуват неповерителна информация относно инциденти ~~рискове~~***, рискове*** и ***начини за смекчаване на рисковете и при необходимост да предоставят препоръки за подходящите мерки по поддръжка***. ***Информацията на уебсайта следва да бъде достъпна независимо от използваното устройство. Всички лични данни, публикувани на този уебсайт, следва да се ограничават само до необходимото и да са възможно най-анонимни.*** **[Изм. 18]**

(17) В случаите, когато информация се счита за поверителна в съответствие с националните разпоредби и тези на Съюза относно търговската тайна, се гарантира поверителност при провеждането на дейностите и изпълнението на целите, определени в настоящата директива.

(18) Въз основа по-специално на националния опит в управлението на кризи и в сътрудничество с ENISA Комисията и държавите членки следва да разработят план на Съюза за сътрудничество за МИС, в който да бъдат определени механизми за сътрудничество***, най-добри практики и модели на работа*** за ***предотвратяване, откриване, докладване и*** противопоставяне на рискове и инциденти. Този план следва да бъде надлежно отчитан при работата с ранни предупреждения в мрежата за сътрудничество. **[Изм. 19]**

(19) Подаването на ранно предупреждение в мрежата следва да се изисква единствено когато мащабът и тежестта на инцидента или риска са или могат да бъдат от такова значение, че е необходима информация или координация на отговора на равнище Съюза. Ранните предупреждения следва поради това да бъдат ограничени до ~~действителни или потенциални~~ инциденти и рискове, които се разрастват бързо, превишават националния капацитет за отговор или засягат повече от една държава членка. С цел да се осигури възможност за добра оценка в мрежата за сътрудничество следва да се предава всичката информация, имаща отношение към оценката на риска или инцидента. **[Изм. 20]**

(20) При получаване на ранно предупреждение и след оценката му ~~компетентните органи~~ ***единичните звена за контакт*** следва да постигат съгласие за координиран отговор съгласно плана на Съюза за сътрудничество за МИС. ~~Компетентните органи~~ ***Единичните звена за контакт, ENISA*** и Комисията следва да бъдат информирани за мерките, предприети на национално ниво вследствие на координирания отговор. **[Изм. 21]**

(21) С оглед на глобалния характер на проблемите в МИС е необходимо по-тясно международно сътрудничество за повишаване на стандартите за сигурност и обмен на информация и насърчаване на общ глобален подход към въпросите на МИС. ***Всяка рамка за такова международно сътрудничество следва да бъде 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].*** **[Изм. 22]**

---

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).***

(22) Отговорностите за гарантиране на МИС до голяма степен се носят от ~~публичните администрации и~~ участниците на пазара. Следва да се насърчава културата на управление на риска, ***на тясно сътрудничество и на доверие,*** част от която са оценката на риска и изпълнението на мерки за сигурност, отговарящи на ~~срещаните рискове~~ ***рисковете и инцидентите, независимо дали те са предизвикани или случайно настъпили***, и тази култура да се развива чрез подходящи регулаторни изисквания и доброволни практики от страна на сектора. Постигането на ***надеждни*** еднакви условия също е от основно значение за ефективното функциониране на мрежата за сътрудничество при гарантирането на ефективно сътрудничество от страна на всички държави членки. **[Изм. 23]**

(23) В Директива 2002/21/ЕО се изисква предприятията, предоставящи обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги, да предприемат подходящи мерки за опазване на своята цялост и сигурност и се въвеждат изисквания за уведомяване в случай на нарушаване на сигурността или компрометиране на целостта. В Директива 2002/58/ЕО на Европейския парламент и на Съвета[1] се изисква доставчиците на обществено достъпни електронни съобщителни услуги да предприемат подходящи технически и организационни мерки за опазване на сигурността на своите услуги.

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

(24) Обхватът на тези задължения следва да бъде разширен извън сектора на електронните съобщения и да обхване ~~Нарушеното предоставяне на тези основни услуги на информационното общество прави невъзможно предоставянето на други услуги на информационното общество, за които те са основен фактор. Разработващите софтуер и производителите на хардуер не са доставчици на услуги на информационното общество и поради това са изключени. Тези задължения трябва да обхванат и публичните администрации,~~ и ***операторите на инфраструктура, които разчитат в голяма степен на информационни и комуникационни технологии и са от съществено значение за поддържането на основни икономически или обществени функции, като електро- и газоснабдяване, транспорт, кредитни институции, ~~фондови борси~~ инфраструктури на финансовия пазар и здравеопазване. Нарушаването на дейността на тези мрежови и информационни системи би засегнало вътрешния пазар. Въпреки че обхватът на задълженията, предвидени в настоящата директива, не следва да бъде разширен,*** за да обхване ключовите доставчици на услуги на информационното общество, определени в Директива 98/34/ЕО на Европейския Парламент и на Съвета[1]***,*** които са в основата на услуги на информационното общество надолу по веригата или на онлайн дейности, като платформи за електронна търговия, портали за плащания в интернет, социални мрежи, машини за търсене, услуги за изчисления в облак ***като цяло или*** магазини за приложни програми, ***тези доставчици биха могли да информират на доброволна основа компетентния орган или единичното звено за контакт за тези инциденти, свързани с мрежовата сигурност, когато считат това за целесъобразно. Компетентният орган или единичното звено за контакт следва при възможност да представи на участниците на пазара, които са го уведомили за инцидента, анализирана от стратегическа гледна точка информация, която ще спомогне за преодоляване на заплахата за сигурността***. **[Изм. 24]**

[1] ***Директива 98/34/ЕО на Европейския Парламент и на Съвета от 22 юни 1998 г. за определяне на процедура за предоставяне на информация в областта на техническите стандарти и регламенти (***ОВ L 204, 21.7.1998 г., стр. 37***).***

(24a) Въпреки че хардуерните и софтуерните доставчици не са участници на пазара, сравними с тези, обхванати от настоящата директива, техните продукти улесняват сигурността на мрежовите и информационните системи. Поради това те имат важна роля за насърчаването на участниците на пазара да обезопасят своите мрежови и информационни инфраструктури. Като се има предвид, че хардуерните и софтуерните продукти вече са предмет на съществуващите правила относно отговорността за продукта, държавите членки следва да гарантират, че тези правила се прилагат. **[Изм. 25]**

(25) Техническите и организационните мерки, наложени ~~публичните администрации и участниците~~ на пазара, следва да не изискват проектирането, разработването или производство по определен начин на конкретен търговски продукт на информационните и комуникационните технологии. **[Изм. 26]**

(26) ~~Публичните администрации и~~ Участниците на пазара следва да гарантират сигурността на мрежите и системите, които контролират. Това са предимно частни мрежи и системи, управлявани или от вътрешен ИТ персонал, или чиято сигурност е възложена на външни изпълнители. Задълженията във връзка със сигурността и уведомяването следва да се прилагат за съответния участник на пазара ~~и за съответната публична администрация~~ без оглед на това дали те извършват вътрешно поддръжката на своите мрежови и информационни системи или я възлагат на външни изпълнители. **[Изм. 27]**

(27) С цел да се избегне налагането на несъразмерна финансова и административна тежест върху малките участници и потребители изискванията следва да бъдат съразмерни с риска, който съществува по отношение на съответната мрежова или информационна система, като се отчитат последните постижения по отношение на подобни мерки. Тези изисквания следва да не се прилагат за микропредприятията.

(28) Компетентните органи ***и единичните звена за контакт*** следва да обръщат необходимото внимание на запазването на неофициалните и ползващи се с доверие канали за споделяне на информация между участниците на пазара и между публичния и частния сектор. ***Компетентните органи и единичните звена за контакт следва да информират производителите и доставчиците на засегнатите ИКТ продукти и услуги за инциденти със значително въздействие, за които са били уведомени.*** При даването на публичност на докладваните инциденти компетентните органи ***и единичните звена за контакт*** следва да постигат нужния баланс между интереса на обществеността да бъде информирана за заплахите и възможните търговски щети и накърняването на репутацията на ~~публичните администрации и~~ участниците на пазара, които докладват за инцидентите. При изпълнението на задълженията за уведомяване компетентните органи ***и единичните звена за контакт*** следва да обръщат особено внимание на необходимостта информацията за уязвимите аспекти на продуктите да бъде запазвана строго поверителна до ~~извършването~~ ***въвеждането*** на съответните корекции по отношение на сигурността. ***Като общо правило единичните звена за контакт не следва да разкриват личните данни на лицата, участващи в инциденти. Единичните звена за контакт следва да разкриват лични данни само когато разкриването на тези данни е необходимо и пропорционално с оглед на преследваната цел.*** **[Изм. 28]**

(29) Компетентните органи следва да разполагат с необходимите средства за изпълнението на своите задължения, включително с правомощия да получават достатъчно информация от участниците на пазара ~~и публичните администрации~~ с цел оценка на нивото на сигурност на мрежовите и информационните системи, ***измерване на броя, мащаба и обхвата на инцидентите,*** както и надеждни и комплексни данни за действителните инциденти, които са имали отражение върху работата на мрежовите и информационните системи. **[Изм. 29]**

(30) В много случаи инцидентите са предизвикани от престъпни деяния. Престъпният характер на инцидентите може да бъде обект на подозрение, дори ако доказателствата в подкрепа на подобно твърдение не са достатъчно убедителни в самото начало. В подобни случаи съответното сътрудничество между компетентните органи***, единичните звена за контакт*** и правоприлагащите органи***, както и сътрудничеството с Европейския център за борба с киберпрестъпността и ENISA*** следва да бъде част от един ефикасен и комплексен отговор на заплахата от инциденти в сигурността. Утвърждаването на безопасна, сигурна и по-устойчива среда изисква по-специално системно докладване на правоприлагащите органи на инцидентите с предполагаем сериозен престъпен характер. Сериозният престъпен характер на инцидентите следва да се оценява в светлината на законодателството на Съюза относно киберпрестъпността. **[Изм. 30]**

(31) В много случаи вследствие на инциденти се компрометират лични данни. ***Държавите членки и участниците на пазара следва да защитават личните данни, които съхраняват, обработват или изпращат, от случайно или незаконно унищожаване, случайна загуба или промяна и неразрешено или незаконно съхранение, достъп, разкриване или разпространение, както и да гарантират осъществяването на политика за сигурност по отношение на обработката на лични данни.*** В този контекст компетентните органи***, единичните звена за контакт*** и органите за защита на данните следва да си сътрудничат и да обменят информация ~~относно всички имащи отношение въпроси~~***, включително по целесъобразност*** с ***участниците на пазара, с*** цел справяне с нарушенията на сигурността на лични данни, предизвикани от инциденти***, в съответствие с приложимите правила за защита на данните***. ~~Държавите членки изпълняват~~ Задължението да уведомяват за инциденти по отношение на сигурността ***следва да се изпълнява*** по начин, при който се намалява до минимум административната тежест, в случай че инцидентът във връзка със сигурността представлява и нарушение на сигурността на лични данни ~~съгласно Регламента на Европейския парламент и на Съвета относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни[1]. Като поддържа връзка с компетентните органи и органите за защита на данните~~, ***което изисква уведомяване в съответствие със законодателство на Съюза за защита на личните данни.*** ENISA ~~би могла~~ ***следва*** да оказва съдействие, като разработва механизми за обмен на информация и ~~образци, чрез които се избягва необходимостта от два образеца за уведомленията. Единният~~ ***единен*** образец за уведомленията ~~ще улесни~~ ***с цел улесняване на*** докладването на инцидентите, при които са компрометирани лични данни, ~~и~~ ***като*** по този начин ще облекчи административната тежест върху бизнеса и публичните администрации. **[Изм. 31]**

~~[1] SEC(2012) 72 final.~~

(32) Стандартизацията на изискванията относно сигурността е процес, движен от пазарни сили***, с доброволен характер, който следва да даде възможност на участниците на пазара да използват алтернативни начини за постигане най-малкото на подобни резултати***. С цел да гарантират последователно прилагане на стандартите за сигурност държавите членки следва да насърчават съответствието или спазването на посочените ***оперативно съвместими*** стандарти с оглед осигуряването на високо ниво на сигурност на равнището на Съюза. За тази цел ***е необходимо да бъде обмислено прилагането на открити международни стандарти за мрежова информационна сигурност или проектирането на такива инструменти. Друга необходима стъпка напред*** може да бъде ~~необходимо да бъдат изготвени~~ ***изготвянето на*** хармонизирани стандарти, чиято разработка следва да бъде в съответствие с Регламент (ЕС) № 1025/2012 на Европейския парламент и на Съвета[1]. ***По-специално може да бъде възложено на Европейския институт за стандарти в далекосъобщенията, Европейския комитет за стандартизация и Европейския комитет за електротехническа стандартизация да предложат ефективни и ефикасни отворени стандарти за сигурност на Съюза, при които технологичните предпочитания да бъдат избегнати максимално и които следва да станат по-достъпни за малките и средните участници на пазара. Международните стандарти за киберсигурността следва да бъдат проучени внимателно с цел да се гарантира, че ефективността им не е нарушена и че предоставят необходимата степен на сигурност, като по този начин се гарантира, че съответствието със стандартите за киберсигурността повишава общото ниво на киберсигурност на Съюза, а не обратното.*** **[Изм. 32]**

(33) Комисията следва периодично да прави преглед на настоящата директива ***след консултации с всички заинтересовани лица***, по-специално с оглед да определя необходимостта от изменения в светлината на променящите се ***обществени, политически,*** технологични или пазарни условия. **[Изм. 33]**

---

[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).

(34) С цел да се даде възможност за правилното функциониране на мрежата за сътрудничество на Комисията следва да бъде делегирано правомощието да приема актове в съответствие с член 290 ДФЕС във връзка с~~определянето на критериите, на които трябва да отговорят държавите членки, за да им бъде разрешено да участват в~~ ***общия набор от стандарти за взаимосвързаност и сигурност за*** сигурната ~~система~~ ***инфраструктура*** за обмен на информация~~, относно~~ по-подробното специфициране на началните събития, водещи до ранни предупреждения~~, и относно определянето на обстоятелствата, при които се изисква участниците на пазара и публичните администрации да изпращат уведомления за инцидентите~~. **[Изм. 34]**

(35) От особена важност е по време на своята подготвителна си работа Комисията да проведе подходящи консултации, включително на експертно равнище. При подготовката и изготвянето на делегираните актове Комисията следва да осгури едновременното и своевременно предаване на съответните документи по подходящ начин на Европейския парламент и на Съвета.

(36) С цел да се осигурят еднакви условия за изпълнението на настоящата директива на Комисията следва да бъдат предоставени правомощия за изпълнение по отношение на сътрудничеството между ~~компетентните органи~~ ***единичните звена за контакт*** и Комисията в рамките на мрежата за сътрудничество, ~~достъпа до сигурната инфраструктура за обмен на информация,~~ ***без да се засягат съществуващите механизми за сътрудничество на национално равнище, по отношение на*** плана на Съюза за сътрудничество~~,~~ ***на МИС и*** форматите и процедурите, приложими при ~~информирането на обществеността за инциденти, и стандартите и/или техническите спецификации, имащи отношение към МИС~~ ***уведомяването за инциденти със значително въздействие***. Тези правомощия следва да се изпълняват в съответствие с Регламент (ЕС) № 182/2011 на Европейския парламент и на Съвета[1]. **[Изм. 35]**

[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).

(37) При прилагането на настоящата директива Комисията следва да поддържа според необходимостта връзка със съответните секторни комитети и със съответните органи, създадени на ~~равнище ЕС~~ ***равнището на Съюза***, по-специално в сферата на ***електронното управление,*** енергетиката, транспорта ~~и здравеопазването~~**,** ***здравеопазването*** и ***отбраната***. **[Изм. 36]**

(38) Информацията, която даден компетентен орган ***или дадено единично звено за контакт*** счита за поверителна, следва да бъде обменяна с Комисията ~~и~~**,** ***съответните ѝ агенции,*** останалите ***единични звена за контакт и/или други национални*** компетентни органи в съответствие с националните разпоредби и тези на Съюза относно търговската тайна само ако подобен обмен е абсолютно необходим за прилагането на настоящата директива. Обменената информация следва да се ограничава до имащата отношение информация и да бъде необходима и пропорционална на целите на подобен обмен ***и следва да спазва предварително определените критерии за поверителност и сигурност съгласно Решение 2011/292/ЕС, информация, която е предмет на споразумения за неразкриване на информация или неформални споразумения за неразкриване на информация, като например Протокола „Светофар“ (Traffic Light Protocol)***. **[Изм. 37]**

(39) Обменът на информация относно рисковете и инцидентите в рамките на мрежата за сътрудничество и изпълнението на изискванията за уведомяване на националните компетентни органи ***или единичните звена за контакт*** за инциденти може да изисква обработката на лични данни. Подобна обработка на лични данни е необходима, за да се изпълнят целите на обществения интерес, преследвани от настоящата директива, и следователно е законосъобразна съгласно член 7 от Директива 95/46/ЕО. По отношение на тези законни цели тя не представлява непропорционално и неприемливо вмешателство, нарушаващо в същината му правото на защита на личните данни, гарантирано от член 8 от Хартата на основните права на Европейския Съюз. При прилагането на настоящата директива следва да се прилага Регламент (ЕО) № 1049/2001 на Европейския парламент и на Съвета[1], когато е целесъобразно. Когато институции и органи на Съюза обработват данни, обработката с цел изпълнение на настоящата директива следва да е съобразена с Регламент (ЕО) № 45/2001 на Европейския парламент и на Съвета. **[Изм. 38]**

[1] 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).

(40) Тъй като целта на настоящата директива, а именно да гарантира високо равнище на МИС в Съюза, не може да бъде постигната в достатъчна степен от държавите членки, а поради обхватът или последиците от действието може да бъде по-добре постигната на равнището на Съюза, Съюзът може да приема 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 посочената цел.

(41) 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 личната кореспонденция, защитата на личните данни, свободата на стопанската инициатива, правото на собственост, правото на ефективни правни средства за защита и на съдебен процес. Настоящата директива трябва да бъде изпълнена в съответствие с тези правила и принципи.

(41а) Съгласно Съвместната политическа декларация от 28 септември 2011 г. на държавите членки и на Комисията относно обяснителните документи държавите членки са поели ангажимент в обосновани случаи да прилагат към съобщението за своите мерки за транспониране един или повече документи, обясняващи връзката между елементите на дадена директива и съответстващите им части от националните инструменти за транспониране. Законодателят счита, че по отношение на настоящата директива предаването на такива документи е оправдано. **[Изм. 39]**

(41б) Европейският надзорен орган по защита на данните беше консултиран в съответствие с член 28, параграф 2 от Регламент (ЕО) № 45/2001 и даде своето становище на 14 юни 2013 г.[1],

ПРИЕХА НАСТОЯЩАТА ДИРЕКТИВА:

[1] ОВ C 32, 4.2.2014 г., стр. 19.

ГЛАВА I

Общи разпоредби

Член 1

Предмет и приложно поле

1. С настоящата директива се определят мерки за гарантиране на високо общо ниво на мрежова и информационна сигурност („МИС“) в Съюза.

2. За тази цел с настоящата директива се:

а) определят задължения на всички държави членки относно превенцията, действията и отговора във връзка с рискове и инциденти, засягащи мрежи и информационни системи;

б) създава се механизъм за сътрудничество между държавите членки с цел да се гарантира единното прилагане на настоящата директива в Съюза и, когато е необходимо, координираните***, ефикасни*** и ефективни действия при рискове и инциденти, засягащи мрежи и информационни системи, и отговора на тях ***с участието на съответните заинтересовани лица***; **[Изм. 40]**

в) определят се изисквания за сигурност за участниците на пазара ~~и публичните администрации~~. **[Изм. 41]**

3. Изискванията за сигурност, предвидени в член 14 от настоящата диркетива, не се прилагат за предприятията, предоставящи обществени съобщителни мрежи или обществено достъпни електронни съобщителни услуги по смисъла на Директива 2002/21/ЕО, които отговарят на специфичните изисквания за сигурност и цялост, определени в членове 13а и 13б от посочената директива, нито към доставчиците на удостоверителни услуги.

4. Настоящата директива не засяга законодателството на Съюза относно киберпрестъпността и Директива 2008/114/ЕО на Съвета[1].

[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).

5. Настоящата директива не засяга също така Директива 95/46/ЕО, Директива 2002/58/ЕО и ~~Регламента~~ ***Регламент (ЕО) № 45/2001***. ***Всяко използване на лични данни се ограничава до строго необходимото за целите на настоящата директива и тези данни са възможно най-анонимни, ако не е възможно да са напълно анонимни***. **[Изм. 42]**

6. Обменът на информация в рамките на мрежата за сътрудничество по глава III и уведомленията за инциденти във връзка с МИС съгласно член 14 могат да изискват обработка на лични данни. Подобна обработка, необходима с цел да бъдат изпълнени целите на обществения интерес, които настоящата директива преследва, се разрешава от държавата членка в съответствие с член 7 от Директива 95/46/ЕО и Директива 2002/58/ЕО, така както е въведен в националното законодателство.

Член 1а

Защита и обработване на личните данни

1. *Всяко обработване на лични данни в държавите членки съгласно настоящата директива се извършва в съответствие с Директива 95/46/ЕО и Директива 2002/58/ЕО.*

2. *Всяко обработване на лични данни от Комисията и ENISA съгласно настоящия регламент се извършва в съответствие с Регламент (ЕО) № 45/2001.*

3. *Всяко обработване на лични данни от Европейския център по киберпрестъпността към Европол за целите на настоящата директива се извършва в съответствие с Решение 2009/371/ПВР на Съвета*[1]*.*

4. *Обработването на лични данни е справедливо и законосъобразно и се ограничава стриктно до минималните данни, необходими за целите на обработването. Те се съхраняват във вид, който позволява идентифицирането на субектите на данните за период, не по-дълъг от необходимия за целите, за които се обработват личните данни.*

5. *Посочените в член 14 от настоящата директива уведомления за инциденти не засягат разпоредбите и задълженията относно уведомление за нарушение на разпоредбите относно личните данни, установени в член 4 на Директива 2002/58/ЕО и в Регламент (ЕС) № 611/2013 на Комисията*[2]*.* **[Изм. 43]**

---

[1] *2009/371/ПВР: Решение на Съвета от 6 април 2009 г. за създаване на Европейска полицейска служба (Европол) (ОВ L 121, 15.5.2009 г., стр. 37).*

[2] *Регламент (ЕС) № 611/2013 на Комисията от 24 юни 2013 година относно мерките, приложими за съобщаването на нарушения на сигурността на личните данни съгласно Директива 2002/58/ЕО на Европейския парламент и на Съвета за правото на неприкосновеност на личния живот и електронни комуникации (ОВ L 173, 26.6.2013 г., стр. 2).*

Член 2

Минимална хармонизация

Държавите членки имат право да приемат или запазват разпоредби, които гарантират по-високо ниво на сигурност, без това да засяга техните задължения съгласно законодателството на Съюза.

Член 3

Определения

За целите на настоящата директива се прилагат следните определения:

(1) „мрежова и информационна система“ означава:

а) електронна съобщителна мрежа по смисъла на Директива 2002/21/ЕИО, както и

б) всяко устройство или всяка група взаимосвързани или имащи връзка помежду си устройства, едно или няколко от които, следвайки програма, извършват автоматична обработка на ~~компютърни~~ ***цифрови*** данни, както и **[Изм. 44]**

в) ~~компютърни~~ ***цифрови*** данни, записвани, обработвани, извличани или пренасяни от елементи, обхванати от букви а) и б), с цел обработка, използване, защита и поддръжка; **[Изм. 45]**

(2) „сигурност“ означава способността на мрежа или информационна система да издържа — при дадено равнище на увереност — на инциденти или злонамерени действия, които повлияват на наличността, автентичността, целостта и поверителността на съхранявани или пренасяни данни или на свързаните с тях услуги, предлагани от или достъпни посредством тази мрежова и информационна система; ***„сигурност“ включва подходящи технически устройства, решения и процедури на работа, гарантиращи изискванията във връзка със сигурността, посочени в настоящата директива;*** **[Изм. 46]**

(3) „риск“ означава ***разумно установимо*** обстоятелство или събитие, което има потенциално неблагоприятно отражение върху сигурността; **[Изм. 47]**

(4) „инцидент“ означава ~~обстоятелство или~~ събитие, което има действително неблагоприятно отражение върху сигурността; **[Изм. 48]**

~~(5) „услуга на информационното общество“ означава услуга по смисъла на член 1, точка 2 от Директива 98/34/ЕО;~~ **[Изм. 49]**

(6) „план за сътрудничество за МИС“ означава план, в който се определя рамката на институционалните роли, отговорности и процедури с оглед поддържане или възстановяване на работата на мрежи и информационни системи в случай на риск или инцидент, който ги засяга;

(7) „действия при инцидент“ означава всички процедури в подкрепа на ***откриването, предотвратяването,*** анализа, ограничаването и отговора на инцидента; **[Изм. 50]**

(8) „участник на пазара “ означава:

~~а) доставчик на услуги на информационното общество, които правят възможно предоставянето на други услуги на информационното общество, неизчерпателен списък на които е даден в приложение II;~~ **[Изм. 51]**

б) ~~оператор на критична~~ ***оператори на*** инфраструктура, която е от основно значение за поддържането на особено важни икономически и обществени дейности в сферата на енергетиката, транспорта, банковото дело, ~~фондовите борси~~ ***инфраструктурите на финансовия пазар, точките за обмен в интернет, веригата на доставка на храни*** и здравеопазването ***и чието нарушаване или унищожаване би оказало значително въздействие върху дадена държава членка в резултат на неспособността да се поддържат тези функции, доколкото съответните мрежови и информационни системи са пряко свързани с основните им услуги, като*** неизчерпателен списък на ~~които~~ ***тези оператори*** е даден в приложение II; **[Изм. 52]**

(8а) „инцидент със значително въздействие“ означава инцидент, засягащ сигурността и непрекъснатостта на информационна мрежа или система, който води до сериозно прекъсване на основни икономически или социални функции; **[Изм. 53]**

(9) „стандарт“ означава стандарт, посочен в Регламент (ЕО) № 1025/2012;

(10) „спецификация“ означава спецификация, посочена в Регламент (ЕО) № 1025/2012;

(11) „доставчик на удостоверителни услуги“ означава физическо или юридическо лице, което доставя каквато и да било електронна услуга, състояща се в създаване, проверка, валидиране, обработка и съхраняване на електронни подписи, електронни печати, електронни времеви печати, електронни документи, услуги по електронно доставяне, удостоверяване на автентичността на уебсайтове, електронни удостоверения, включително удостоверения за електронен подпис и електронен печат;

(11а) „регулиран пазар“ означава регулиран пазар съгласно определението в член 4, точка 14 от Директива 2004/39/ЕО на Европейския парламент и на Съвета[1]; **[Изм. 54]**

(11б) „многостранна търговска система“ (МТС) означава многостранна търговска система съгласно определението в член 4, точка 15 от Директива 2004/39/ЕО; **[Изм. 55]**

(11в) „организирана търговска система“ означава многостранна система или механизъм, които не са регулиран пазар, многостранна търговска система или централен контрагент, управлявани от инвестиционен посредник или участник на пазара, в които многобройни интереси на трети лица за покупката и продажбата на облигации, структурирани финансови продукти, квоти за емисии или деривати могат да взаимодействат в системата по начин, който да доведе до сключването на договор за финансови инструменти, в съответствие с дял II от Директива 2004/39/ЕО. **[Изм. 56]**

---

1 ***Директива 2004/39/ЕО на Европейския парламент и на Съвета от 21 април 2004 г. относно пазарите за финансови инструменти (ОВ L 45, 16.2.2005 г., стр. 18).***

ГЛАВА II

Национални рамки за мрежова и информационна сигурност

Член 4

Принцип

Държавите членки гарантират високо ниво на сигурност на мрежовите и информационните системи на тяхна територия в съответствие с настоящата директива.

Член 5

Национална стратегия за МИС и национален план за сътрудничество за МИС

1. Всяка държава членка приема национална стратегия за МИС, в която са определени стратегически цели, конкретни мерки на политиката и регулаторни мерки за постигане и поддържане на високо равнище на мрежова и информационна сигурност. В националната стратегия за МИС се разглеждат по-специално следните въпроси:

   а) определяне на целите и приоритетите на стратегията въз основа на анализ на актуалните рискове и инциденти;

   б) управленска рамка за постигане на стратегическите цели и приоритети, включително ясно определени роли и отговорности на структурите на държавното управление и на останалите имащи отношение действащи лица;

в) набелязване на основните мерки във връзка с готовността, отговора и възстановяването, включително механизми за сътрудничество между публичния и частния сектор;

г) основна информация за образователните и обучителните програми и за програмите за повишаване на осведомеността;

д) планове за научноизследователска и развойна дейност и описание на начина, по който в тях са отразени набелязаните приоритети;

да) държавите членки може да изискат подкрепа от ENISA за разработване на своите национални стратегии за МИС и националните планове за сътрудничество за МИС въз основа на общ план с минимални изисквания във връзка със стратегията за МИС. **[Изм. 57]**

2. Националната стратегия за МИС съдържа национален план за сътрудничество за МИС, който отговаря най-малкото на следните изисквания:

а) ~~план за оценка~~ ***рамка за управление*** на риска с цел ~~установяване~~ ***създаване*** на ***методика за установяването, приоритизирането, оценката и обработката на*** рисковете ~~и оценка~~***, оценката*** на въздействието на потенциалните инциденти***, възможностите за превенция и контрол, както и за определяне на критериите за избор на евентуални мерки за противодействие***; **[Изм. 58]**

б) определяне на ролите и отговорностите на различните ***органи и други*** действащи лица, участващи в изпълнението на ~~плана~~ ***рамката***; **[Изм. 59]**

в) определяне на процесите за сътрудничество и комуникация, чрез които се гарантират превенцията, откриването, отговорът, отстраняването на смущенията и възстановяването, с модификации в тях в зависимост от степента на тревога;

г) пътна карта за учения и обучения във връзка с МИС с цел подсилване, валидиране и тестване на плана. Извлечените поуки се документират и включват при актуализациите на плана.

3. Националната стратегия за МИС и националният план за сътрудничество за МИС се предоставят на Комисията в ~~едномесечен~~ ***тримесечен*** срок след тяхното приемане. **[Изм. 60]**

Член 6

~~Национален компетентен орган~~ ***Национални компетентни органи и единични звена за контакт*** по сигурността на мрежовите и информационните системи **[Изм. 61]**

1. Всяка държава членка определя ~~национален компетентен орган~~ ***един или повече граждански национални компетентни органи*** по сигурността на мрежовите и информационните системи (~~„компетентния орган~~„***компетентният орган/компетентните органи“***). **[Изм. 62]**

2. Компетентните органи следят за прилагането на настоящата директива на национално равнище и спомагат за последователното ѝ прилагане в целия Съюз.

2а. Когато държава членка определи повече от един компетентен орган, тя определя граждански национален орган, например компетентен орган, за национално единично звено за контакт по сигурността на мрежовите и информационните системи („единично звено за контакт“). Когато държава членка определи само един компетентен орган, този компетентен орган изпълнява функцията и на единично звено за контакт. **[Изм. 63]**

2б. Компетентните органи и единичното звено за контакт в една и съща държава членка си сътрудничат тясно по отношение на задълженията, предвидени в настоящата директива. **[Изм. 64]**

2в. Единичното звено за контакт осигурява трансгранично сътрудничество с други единични звена за контакт. **[Изм. 65]**

3. Държавите членки гарантират, че компетентните органи ***и единичните звена за контакт*** разполагат с достатъчно технически, финансови и човешки ресурси, за да изпълняват ефективно и ефикасно определените им задачи и по този начин да постигат целите на настоящата директива. Държавите членки гарантират, че чрез мрежата, посочена в член 8, ~~компетентните органи~~ ***единичните звена за контакт*** си сътрудничат ефективно, ефикасно и сигурно. **[Изм. 66]**

4. Държавите членки гарантират, че компетентните органи ***и единичните звена за контакт, когато е приложимо съгласно параграф 2а от настоящия член,*** получават уведомленията за настъпили инциденти от ~~публичните администрации и~~ участниците на пазара, както е посочено в член 14, параграф 2, и разполагат с правомощията за прилагане и изпълнение, посочени в член 15. **[Изм. 67]**

4a. ***Когато законодателството на Съюза предвижда специфичен за сектора надзорен или регулаторен орган на Съюза, inter alia, по отношение на сигурността на мрежовите и информационните системи, този орган получава уведомления за инциденти в съответствие с член 14, параграф 2, от съответните участници на пазара в този сектор, като му се предоставят правомощията за прилагане и изпълнение, посочени в член 15. Въпросният орган на Съюза си сътрудничи тясно с компетентните органи и единичното звено за контакт в приемащата държава членка по отношение на тези задължения. Единичното звено за контакт в приемащата държава членка представлява органа на Съюза по отношение на задълженията, посочени в глава III.*** **[Изм. 68]**

5. Компетентните органи ***и единичните звена за контакт*** се консултират помежду си и си сътрудничат винаги, когато това е целесъобразно, със съответните национални правоприлагащи органи, включително с органите за защита на данните. **[Изм. 69]**

6. Всяка държава членка уведомява незабавно Комисията за ~~определения~~ ***определените*** от нея ~~компетентен орган, неговите~~ ***компетентни органи и единично звено за контакт, за техните*** задачи и за всякакви последващи промени в тях. Всяка държава членка прави обществено достояние акта, с който определя ~~компетентния орган~~ ***компетентните органи***. **[Изм. 70]**

Член 7

Екипи за незабавно реагиране при компютърни инциденти

1. Всяка държава членка сформира ***най-малко един*** екип за незабавно реагиране при компютърни инциденти („CERT“) ***за всеки от секторите, посочени в приложение II,*** който отговаря за предприемането на действия при инциденти и рискове в съответствие с подробно определена процедура, която отговаря на изискванията, посочени в приложение I, точка 1. CERT може да бъде сформиран в рамките на компетентния орган. **[Изм. 71]**

2. Държавите членки гарантират, че CERT разполагат с достатъчно технически, финансови и човешки ресурси, за да изпълняват ефективно задачите, определени им в приложение I, точка 2.

3. Държавите членки гарантират, че на национално равнище CERT разчитат на сигурна и устойчива комуникационна и информационна инфраструктура, която има обща и оперативна съвместимост със сигурната система за обмен на информация, посочена в член 9.

4. Държавите членки информират Комисията за ресурсите и правомощията на CERT, както и за процедурата за предприемане на действия при инциденти, която CERT следва.

5. Дейността на ***CERT*** е обект на надзор от страна на компетентния орган~~, който~~ ***или на единичното звено за контакт, който/което*** прави редовно преглед на адекватността на ~~неговите~~ ***техните*** ресурси и правомощия и на ефективността на процедурата ***им*** за предприемане на действия при инциденти, която ~~той следва~~ ***те следват***. **[Изм. 72]**

5а. Държавите членки гарантират, че CERT разполагат с достатъчни човешки и финансови ресурси за активно участие в международните мрежи за сътрудничество и по-конкретно в мрежите за сътрудничество на Съюза. **[Изм. 73]**

5б. CERT получават възможност и се насърчават да инициират и да участват в съвместни учения с други CERT, със CERT на всички държави членки и със съответните институции на държави извън ЕС, както и със CERT на многонационални и международни институции като Организацията на Северноатлантическия договор и Обединените нации. **[Изм. 74]**

5в. Държавите членки могат да поискат помощ от ENISA или от други държави членки при създаване на своите национални CERT. **[Изм. 75]**

ГЛАВА III

СЪТРУДНИЧЕСТВО МЕЖДУ КОМПЕТЕНТНИТЕ ОРГАНИ

Член 8

Мрежа за сътрудничество

1. ~~Компетентните органи~~ ***Единичните звена за контакт*** и Комисията ***и ENISA*** изграждат мрежа („мрежа за сътрудничество“) с цел да си сътрудничат в борбата с рисковете и инцидентите, засягащи мрежовите и информационните системи. **[Изм. 76]**

2. Мрежата за сътрудничество осигурява постоянна комуникация между Комисията и ~~компетентните органи~~ ***единичните звена за контакт***. При поискване ~~Европейската агенция за мрежова и информационна сигурност („ENISA“)~~ оказва съдействие на мрежата за сътрудничество, като ѝ предоставя експертни познания и консултации. ***При целесъобразност участниците на пазара и доставчиците на решения за киберсигурност могат също така да бъдат поканени да участват в дейностите на мрежата за сътрудничество, посочени в параграф 3, букви ж) и и).***

При целесъобразност мрежата за сътрудничество си сътрудничи с органите, отговарящи за защита на данните.

Комисията информира редовно мрежата за сътрудничество относно изследвания в областта на сигурността и относно други съответни програми на „Хоризонт 2020“ **[Изм. 77]**

3. В рамките на мрежата за сътрудничество ~~компетентните органи~~ ***единичните звена за контакт***:

а) разпространяват ранни предупреждения за рискове и инциденти в съответствие с член 10;

б) гарантират наличието на координиран отговор в съответствие с член 11;

в) редовно публикуват на общ уебсайт неповерителна информация относно актуални ранни предупреждения и координирани отговори;

г) съвместно обсъждат и оценяват ~~по искане на някоя от държавите членки или на Комисията~~ една или няколко национални стратегии за МИС и национални планове за сътрудничество за МИС, посочени в член 5, в рамките на приложното поле на настоящата директива;

д) съвместно обсъждат и оценяват ~~по искане на някоя от държавите членки или на Комисията~~ ефективността на CERT, по-специално когато на равнище Съюза се провеждат учения за МИС;

е) си сътрудничат и обменят ~~информация по всички~~ ***експертен опит относно*** имащи отношение въпроси ***във връзка*** с ~~Европейския център по киберпрестъпността към Европол и с всички останали имащи отношение европейски органи~~ ***мрежовата и информационната сигурност***, по-специално в сферата на защитата на данни, енергетиката, транспорта, банковото дело, ~~фондовите борси~~ ***финансовите пазари*** и здравеопазването***, с Европейския център по киберпрестъпността към Европол и с други имащи отношение европейски органи***;

еа) когато е целесъобразно, информират координатора на ЕС за борба с тероризма посредством доклад и могат да поискат помощ при извършването на анализ, подготвителна работа и действия на мрежата за сътрудничество;

ж) обменят информация и най-добри практики помежду си и с Комисията и се подпомагат взаимно при изграждането на капацитет за МИС;

~~з) организират редовно партньорски проверки на капацитета и готовността;~~

и) организират учения за МИС на ~~равнище~~ ***равнището на*** Съюза и участват, когато това е целесъобразно, в международни учения за МИС;

иа) включват участниците на пазара, провеждат консултации и където е уместно – обменят информация с участниците на пазара по отношение на рисковете и инцидентите, които засягат техните мрежови и информационни системи;

иб) в сътрудничество с ENISA разработват насоки за специфични за сектора критерии за уведомяването относно значителни инциденти, в допълнение към параметрите, посочени в член 14, параграф 2, за общо тълкуване, последователно прилагане и съгласувано изпълнение в рамките на Съюза.
[Изм. 78]

3a. ***Мрежата за сътрудничество публикува веднъж годишно доклад относно дейността си за предходните 12 месеца въз основа на обобщения доклад, представен в съответствие с член 14, параграф 4 от настоящата директива.*** **[Изм. 79]**

4. Чрез актове за изпълнение Комисията определя необходимата уредба, с която да улесни сътрудничеството между ~~компетентните органи и~~ ***единичните звена за контакт,*** Комисията ***и ENISA***, посочено в параграфи 2 и 3. Тези актове за изпълнение се приемат в съответствие с процедурата по ~~консултиране~~ ***разглеждане,*** посочена в член 19, ~~параграф 2~~ ***параграф 3***. **[Изм. 80]**

Член 9

Сигурна система за обмен на информация

1. Обменът на чувствителна и поверителна информация в рамките на мрежата за сътрудничество се осъществява с помощта на сигурна инфраструктура.

1а. Участниците в сигурната инфраструктура спазват, inter alia, подходящи условия за поверителност и мерки за сигурност в съответствие с Директива 95/46/ЕО и Регламент (ЕО) № 45/2001 във всички етапи на обработката. **[Изм. 81]**

~~2. Комисията е оправомощена да приема делегирани актове в съответствие с член 18 за определяне на критериите, които една държава членка трябва да изпълни, за да получи разрешение да участва в сигурната система за обмен на информация по отношение на:~~

~~а) наличието на сигурна и устойчива комуникационна и информационна инфраструктура на национално равнище, която има общa и оперативна съвместимост със сигурната система за обмен на информация, посочена в член 7, параграф 3, и~~

~~б) наличието на достатъчно технически, финансови и човешки ресурси и адекватни процедури за нейните компетентни органи и CERT, които да дават възможност за ефективно, ефикасно и сигурно участие в сигурната система за обмен на информация по член 6, параграф 3, член 7, параграф 2 и член 7, параграф 3.~~ **[Изм. 82]**

3. Чрез ***делегирани*** актове ~~за изпълнение~~ Комисията приема в съответствие с член 18 ~~решения относно достъпа на държавите-членки до сигурната инфраструктура в съответствие с критериите, посочени в параграфи 2 и 3. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 19, параграф 3.~~ ***общ набор от стандарти за взаимосвързаност и сигурност, които единичните звена за контакт трябва да изпълняват преди да извършват обмен на чувствителна и поверителна информация в мрежата за сътрудничество.***
[Изм. 83]

Член 10

Ранни предупреждения

1. ~~Компетентните органи~~ ***Единичните звена за контакт*** или Комисията изпращат ранни предупреждения в мрежата за сътрудничество относно онези рискове и инциденти, които отговорят поне на едно от следните условия:

~~а) мащабът им се увеличава бързо или може да се увеличи бързо;~~

б) ~~превишават или може да превишат~~ ***единичното звено за контакт преценява дали рискът или инцидентът потенциално превишава*** националния капацитет за отговор;

в) ~~засягат или може да засегнат~~ ***единичното звено за контакт или Комисията преценяват дали рискът или инцидентът засяга*** повече от една държава членка. **[Изм. 84]**

2. В ранните предупреждения ~~компетентните органи~~ ***единичните звена за контакт*** и Комисията съобщават ***без неоправдано забавяне*** всякаква имаща отношение информация, с която разполагат и която може да бъде от полза за оценката на риска или инцидента. **[Изм. 85]**

~~3. По искане на държава членка или по собствена инициатива Комисията може да поиска една държава членка да предостави всякаква имаща отношение информация по конкретен риск или инцидент.~~ **[Изм. 86]**

4. Когато рискът или инцидентът, за който е изпратено ранно предупреждение, е с предполагаем престъпен характер~~, компетентните органи или Комисията уведомяват~~ ***и когато съответният участник на пазара е докладвал за инциденти с предполагаем сериозен престъпен характер, както е посочено в член 15, параграф 4, държавите членки правят необходимото, за да осигурят уведомяването на*** Европейския център по киберпрестъпността към Европол***, когато е уместно***. **[Изм. 87]**

4а. Членовете на мрежата за сътрудничество не оповестяват публично каквато и да е получена информация относно рискове и инциденти, посочени в параграф 1, без да са получили предварителното съгласие на единичното звено за контакт, което изпраща уведомлението.

Освен това преди споделянето на информация в мрежата за сътрудничество единичното звено за контакт, което изпраща уведомлението, уведомява пазарния участник, за когото се отнася информацията, относно намеренията си и ако счете за уместно, прави съответната информация анонимна. **[Изм. 88]**

4б. Когато рискът или инцидентът, за който е изпратено ранно предупреждение, е с предполагаем тежък трансграничен технически характер, единичните звена за контакт или Комисията уведомяват ENISA. **[Изм. 89]**

5. Комисията е оправомощена да приема делегирани актове в съответствие с член 18 за допълнително специфициране на рисковете и инцидентите, които са причина за изпращане на ранното предупреждение, посочено в параграф 1 от настоящия член.

Член 11

Координиран отговор

1. След постъпването на ранното предупреждение, посочено в член 10, ~~компетентните органи~~ ***единичните звена за контакт***, след като направят оценка на имащата отношение информация, се споразумяват ***без неоправдано забавяне*** за координиран отговор в съответствие с плана на Съюза за сътрудничество за МИС, посочен в член 12. **[Изм. 90]**

2. Различните мерки, приети на национално равнище вследствие на координирания отговор, се съобщават на мрежата за сътрудничество.

Член 12

План на Съюза за сътрудничество за МИС

1. Комисията е оправомощена чрез делегирани актове да приема план на Съюза за сътрудничество за МИС. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 19, параграф 3.

2. В плана на Съюза за сътрудничество за МИС се предвиждат:

а) за целите на член 10:

– определение на формата и процедурата за събиране и обмен на съвместима и съпоставима информация относно рискове и инциденти от страна на ~~компетентните органи~~ ***единичните звена за контакт*** **[Изм. 91]**;

– определяне на процедурите и критериите за оценка на рисковете и инцидентите от страна на мрежата за сътрудничество;

б) процедурата, която следва координираният отговор съгласно член 11, включително определяне на ролите и отговорностите и на процедурите за сътрудничество;

в) пътна карта за учения и обучения във връзка с МИС с цел подсилване, валидиране и тестване на плана;

г) програма за трансфер на знания между държавите членки във връзка с изграждането на капацитетите и ученето от партньорите;

д) програма за повишаване на осведомеността и за обучение между държавите членки.

3. Планът на Съюза за МИС се приема не по-късно от една година след влизането в сила на настоящата директива и се преразглежда редовно. ***Резултатите от всяко преразглеждане се докладват на Европейския парламент.*** **[Изм. 92]**

3а. Осигурява се съгласуваност между плана на Съюза за сътрудничество за МИС и националните стратегии за МИС и националните планове за сътрудничество за МИС, както е предвидено в член 5. **[Изм. 93]**

Член 13

Международно сътрудничество

Без да се засяга възможността мрежата за сътрудничество да провежда неофициално международно сътрудничество, Съюзът може да сключва международни споразумения с трети държави или международни организации, които да дават възможност за участие в някои от дейностите на мрежата за сътрудничество и да ги организират. Подобни споразумения отчитат необходимостта да се гарантира надеждна защита на личните данни, които са в обращение в мрежата за сътрудничество ***и посочват процедурата за мониторинг, която трябва да се следва, за да се гарантира защитата на личните данни***. ***Европейският парламент бива информиран относно преговорите във връзка със споразуменията. Всеки трансфер на лични данни към получатели, установени в държави извън ЕС, се извършва в съответствие с членове 25 и 26 от Директива 95/46/ЕО и член 9 от Регламент (ЕО) № 45/2001.*** **[Изм. 94]**

Член 13а

Равнище на критичност на участниците на пазара

Държавите членки могат да определят равнището на критичност на участниците на пазара, като вземат предвид спецификите на секторите, параметри, включващи значението на определен участник на пазара за поддържане на достатъчно равнище на секторната услуга, броя на страните, които участникът на пазара снабдява, и периода от време до момента, в който основните услуги на участника на пазара оказват отрицателно въздействие върху поддържането на жизненоважни икономически и социални дейности. **[Изм. 95]**

ГЛАВА IV

Сигурност на мрежите и информационните системи на публичните администрации и на участниците на пазара

Член 14

Изисквания за сигурност и уведомяване за инциденти

1. Държавите членки гарантират, че ~~публичните администрации и~~ участниците на пазара предприемат подходящи ***и пропорционални*** технически и организационни мерки за ***установяване и ефективно*** управление на рисковете, пред които е изправена сигурността на мрежите и информационните системи, които контролират и използват като част от дейността си. Тези мерки ~~гарантират~~ ***осигуряват*** ниво на сигурност, съответстващо на съществуващия риск с оглед на последните постижения в тази сфера. Предприемат се по-специално мерки с цел предотвратяване и намаляване до минимум на отражението на инциденти, засягащи ***сигурността на*** техните мрежи и информационни системи, върху основните услуги, които те предоставят, и по този начин за гарантиране на непрекъснатостта на услугите, които се поддържат от тези мрежи и информационни системи. **[Изм. 96]**

2. Държавите членки гарантират, че ~~публичните администрации и~~ участниците на пазара уведомяват ***без неоправдано забавяне*** компетентния орган ***или единичното звено за контакт*** за инцидентите~~, които са имали~~ ***със*** значително ~~отражение~~ ***въздействие*** върху ~~сигурността~~ ***непрекъснатостта*** на основните предоставяни от тях услуги. ***Уведомлението не излага уведомяващата страна на повишена отговорност.***

За да се определи значимостта на въздействието на даден инцидент, се вземат предвид, inter alia, следните параметри: **[Изм. 97]**

а) броят на потребителите, чиято основна услуга е засегната; **[Изм. 98]**

б) продължителността на инцидента; **[Изм. 99]**

в) географският обхват по отношение на областта, засегната от инцидента. **[Изм. 100]**

Тези параметри се конкретизират допълнително в съответствие с член 8, параграф 3, буква иб). **[Изм. 101]**

2а. ***Участниците на пазара уведомяват компетентния орган или единичното звено за контакт в държавата членка, в която е засегната основната услуга, за инцидентите, посочени в параграфи 1 и 2. Когато са засегнати основни услуги в повече от една държава членка, единичното звено за контакт, което е било уведомено, предупреждава, въз основа на информацията, предоставена от участника на пазара, другите заинтересовани единични звена за контакт. Участникът на пазара се уведомява във възможно най-кратък срок за това кои други единични звена за контакт са информирани за инцидента, какви стъпки са били предприети и какви резултати са били постигнати и получава всяка друга информация от значение за инцидента.*** **[Изм. 102]**

2б. ***Когато уведомлението съдържа лични данни, то се оповестява само на получатели в рамките на компетентния орган или единично звено за контакт, където е получено уведомлението, които трябва да обработят тези данни, за да изпълнят своите задачи в съответствие с правилата за защита на данните. Оповестяването на данни се ограничава до необходимото за изпълнение на техните задачи.*** **[Изм. 103]**

2в. ***Участници на пазара, които не са обхванати от приложение II, могат да докладват инциденти съгласно посоченото в член 14, параграф 2 на доброволна основа.*** **[Изм. 104]**

3. Параграфи 1 и 2 се прилагат за всички участници на пазара, които предоставят услуги в Европейския съюз.

4. ~~Компетентният~~ ***След консултация с компетентния*** орган***, получил уведомлението, и със съответния участник на пазара единичното звено за контакт*** може да информира обществеността ~~или да изиска това да бъде направено от публичните администрации и участниците на пазара, в случай че прецени, че разкриването на инцидента е в интерес на обществото.~~ ***за отделни инциденти, когато определи, че е необходимо обществеността да е осведомена с цел предотвратяване на инцидент или справяне с текущ инцидент, или когато участникът на пазара, обект на инцидент, е отказал да предприеме незабавно действия по отношение на сериозна структурна уязвимост, свързана с този инцидент***.

Преди публичното оповестяване компетентният орган, получил уведомлението, прави необходимото, за да гарантира, че съответният участник на пазара има възможност да бъде изслушан и че решението за оповестяване на информацията е било подложено на надлежна преценка по отношение на обществения интерес.

Когато информацията за отделни инциденти се прави обществено достояние, компетентният орган или единичното звено за контакт, където е получено уведомлението, прави необходимото, за да гарантира, че това се извършва по възможно най-анонимен начин.

Когато в рамките на разумното е възможно, компетентният орган или единичното звено за контакт предоставя на съответния участник на пазара информация, която подпомага ефективното разглеждане на инцидента, за който е получено уведомление.

Веднъж годишно ~~компетентният орган~~ ***единичното звено за контакт*** предава обобщен доклад до мрежата за сътрудничество относно получените уведомления***, който включва броя на уведомленията*** и ***посочва параметрите на инцидента, изброени в параграф 2 от настоящия член, както и относно*** предприетите действия в съответствие с настоящия параграф. **[Изм. 105]**

4а. Държавите членки насърчават участниците на пазара доброволно да оповестяват инцидентите, отнасящи се до тяхната стопанска дейност, във финансовите си доклади. **[Изм. 106]**

~~5. Комисията е оправомощена да приема делегирани актове в съответствие с член 18 относно определянето на обстоятелства, при които се изисква публичните администрации и участниците на пазара да информират за настъпилите инциденти.~~ **[Изм. 107]**

6. ~~В съответствие с евентуално приетите съгласно параграф 5 делегирани актове~~ Компетентните органи ***или единичното звено за контакт*** могат да приемат насоки ~~и, когато е необходимо, да издават указания~~ относно обстоятелствата, при които се изисква ~~публичните администрации и~~ участниците на пазара да информират за настъпилите инциденти. **[Изм. 108]**

7. Комисията е оправомощена чрез делегирани актове да определя форматите и процедурите, приложими за целите на параграф 2. Тези актове за изпълнение се приемат в съответствие с процедурата по разглеждане, посочена в член 19, параграф 3.

8. Параграфи 1 и 2 не се прилагат за микропредприятия, съгласно определението от Препоръка 2003/361/ЕО на Комисията[1]***, освен ако микропредприятието действа като дъщерно предприятие на участник на пазара по смисъла на член 3, параграф 8, буква б)***. **[Изм. 109]**

8а. ***Държавите членки могат да решат да приложат настоящия член за публичните администрации mutatis mutandis.*** **[Изм. 110]**

[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).

Член 15

Изпълнение и правоприлагане

1. Държавите членки гарантират, че компетентните органи ***и единичните звена за контакт*** получават ~~всички необходими~~ ***необходимите*** правомощия, за да ~~разследват случаите на неизпълнение~~ ***гарантират спазването*** от страна на ~~публичните администрации и~~ участниците на пазара на техните задължения съгласно член 14 и на последиците от тях за сигурността на мрежовите и информационните системи. **[Изм. 111]**

2. Държавите членки гарантират, че компетентните органи ***и единичните звена за контакт*** разполагат с правомощието да изискват от ~~публичните администрации и~~ участниците на пазара да: **[Изм. 112]**

   а) предоставят информацията, необходима за оценка на сигурността на техните мрежови и информационни системи, включително документирани политики за сигурност;

   б) ~~да преминават~~ ***предоставят доказателства за ефективното изпълнение на политиките за сигурност, като например резултатите от*** одит на сигурността, извършван от квалифицирана независима организация или национален орган, и да предоставят ~~резултатите от него~~ ***доказателствата*** на компетентния орган ***или на единното звено за контакт***. **[Изм. 113]**

При изпращане на това искане компетентните органи и единичните звена за контакт посочват целта на искането и уточняват в достатъчна степен каква информация се изисква. **[Изм. 114]**

3. Държавите членки гарантират, че компетентните органи ***и единичните звена за контакт*** разполагат с правомощието да издават задължителни инструкции за участниците на пазара~~и публичните администрации~~. **[Изм. 115]**

3а. Чрез дерогация от параграф 2, буква б) на настоящия член, държавите членки могат да решат, че компетентните органи или единичните звена за контакт, в зависимост от случая, могат да прилагат различна процедура за определени участници на пазара, въз основа на тяхното равнище на критичност, определено съгласно член 13а. В случай че държавата членка вземе такова решение:

а) компетентните органи или единните звена за контакт, в зависимост от случая, имат правомощието да представят достатъчно конкретно искане към участниците на пазара за предоставяне на доказателство за ефективното прилагане на политиките на сигурност, като например резултатите от одита на сигурността, извършен от квалифициран вътрешен одитор, и доказателството да бъде предоставено на компетентния орган или на единното звено за контакт;

б) когато е необходимо, след предоставяне от страна на участника на пазара на искането, посочено в буква а), компетентният орган или единното звено за контакт може да поиска допълнително доказателство или извършване на допълнителен одит от квалифициран независим орган или национален орган.

3б. ***Държавите членки може да вземат решение да намалят броя и интензивността на одитите за съответния участник на пазара, чийто одит на сигурността показва последователно спазване на задълженията съгласно глава IV.*** **[Изм. 116]**

4. Компетентните органи ***и единичните звена за контакт*** уведомяват ***съответните участници на пазара относно възможността за докладване на*** правоприлагащите органи ~~за инцидентите~~ ***на инциденти*** от предполагаемо сериозно престъпно естество. **[Изм. 117]**

5. ***Без да се засягат приложимите правила относно защитата на данните,*** компетентните органи ***и единичните звена за контакт*** работят в тясно сътрудничество с органите за защита на личните данни по инцидентите, които водят до нарушаване на сигурността на лични данни. ***Единичните звена за контакт и органите за защита на данните разработват в сътрудничество с ENISA механизми за обмен на информация и единен образец, който да се използва за уведомленията съгласно член 14, параграф 2 от настоящата директива и други разпоредби на законодателството на Съюза относно защитата на данните.*** **[Изм. 118]**

6. Държавите членки гарантират, че всички задължения, наложени на ~~публичните администрации и~~ участниците на пазара, могат да бъдат обект на съдебен контрол. **[Изм. 119]**

6а. ***Държавите членки могат да решат да приложат член 14 и настоящия член за публичните администрации mutatis mutandis.*** **[Изм. 120]**

Член 16

Стандартизация

1. С цел да гарантират последователно прилагане на член 14, параграф 1 държавите членки***, без да препоръчват използването на конкретна технология,*** насърчават използването на ***оперативно съвместими европейски или международни*** стандарти и/или спецификации, касаещи мрежовата и информационната сигурност. **[Изм. 121]**

2. Комисията ~~изготвя чрез актове за изпълнение~~ ***възлага на съответен европейски орган за стандартизация да изготви – след провеждане на консултации със заинтересованите участници –*** списък на стандартите ***и/или спецификациите,*** посочени в параграф 1. Списъкът се публикува в *Официален вестник на Европейския съюз*. **[Изм. 122]**

ГЛАВА V

ЗАКЛЮЧИТЕЛНИ разпоредби

Член 17

Санкции

1. Държавите членки определят правила относно санкциите в случаи на нарушения на националните разпоредби, приети съгласно настоящата директива, и предприемат всички необходими мерки, за да гарантират тяхното изпълнение. Предвидените санкции трябва да бъдат ефикасни, съразмерни и възпиращи. Държавите членки нотифицират тези разпоредби на Комисията не по-късно от датата на транспониране на настоящата директива и нотифицират без забавяне всякакви последващи изменения, които засягат тези разпоредби.

1а. Държавите членки гарантират, че санкциите, посочени в параграф 1 от настоящия член, се прилагат само когато участникът на пазара не е изпълнил задълженията си съгласно глава IV умишлено или в резултат на груба небрежност. **[Изм. 123]**

2. Държавите членки гарантират, че в случаите когато инцидент засяга лични данни, предвидените санкции са съгласувани със санкциите, предвидени в Регламента на Европейския парламент и на Съвета относно защитата на лицата по отношение на обработката на лични данни от институции и органи на Общността и за свободното движение на такива данни[1].

[1] SEC(2012)0072.

Член 18

Упражняване на делегирането

1. Правомощието да приема делегирани актове се предоставя на Комисията при спазване на предвидените в настоящия член условия.

2. Правомощието да приема делегирани актове, посочено в член 9, параграф 3 и член 10, параграф 5се предоставя на Комисията. Комисията изготвя доклад относно делегирането на правомощия не по-късно от девет месеца преди изтичането на петгодишния срок. Делегирането на правомощия се продължава мълчаливо за срокове с еднаква продължителност, освен ако Европейският парламент или Съветът не възразят срещу подобно продължаване не по-късно от три месеца преди изтичането на всеки срок.

3. Делегирането на правомощия, посочено в член 9, параграф 3 и член 10, параграф 5 ~~и член 14, параграф 5,~~ може да бъде оттеглено по всяко време от Европейския парламент или от Съвета. С решението за оттегляне се прекратява посоченото в него делегиране на правомощия. То поражда действие в деня след публикуването на решението в *Официален вестник на Европейския съюз* или на по-късна, посочена в решението дата. То не засяга действителността на делегираните актове, които вече са в сила. **[Изм. 124]**

4. Веднага след като приеме делегиран акт, Комисията нотифицира акта едновременно на Европейския парламент и Съвета.

5. Делегиран акт, приет съгласно член 9, параграф 3 и член 10, параграф 5 ~~и член 14, параграф 5,~~ влиза в сила единствено ако нито Европейският парламент, нито Съветът не са представили възражения в срок от два месеца след нотифицирането на акта на Европейския парламент и Съвета или ако преди изтичането на този срок и Европейският парламент, и Съветът са уведомили Комисията, че няма да представят възражения. Този срок се удължава с два месеца по инициатива на Европейския парламент или на Съвета. **[Изм. 125]**

Член 19

Процедура на комитет

1. Комисията се подпомага от комитет (Комитет по мрежова и информационна сигурност). Посоченият комитет е комитет по смисъла на Регламент (ЕС) № 182/2011.

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

3. При позоваване на настоящия параграф се прилага член 5 от Регламент (ЕС) № 182/2011.

Член 20

Преразглеждане

Комисията периодично преразглежда действието на настоящата директива***, по-специално списъка, изложен в приложение II,*** и докладва на Европейския парламент и Съвета. Първият доклад се предава не по-късно от три години след датата на транспониране, посочена в член 21. За тази цел Комисията може да поиска от държавите членки да предоставят информация без неоправдано забавяне. **[Изм. 126]**

Член 21

Транспониране

1. Държавите членки въвеждат в сила законовите, подзаконовите и административните разпоредби, необходими, за да се съобразят с настоящата директива не по-късно от [една година и половина след приемането] г. Те незабавно съобщават на Комисията текста на тези мерки.

   Те прилагат тези мерки от [една година и половина след приемането] г.

   Когато държавите членки приемат тези мерки, 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 законодателство, които те приемат в областта, уредена с настоящата директива.

Член 22

Влизане в сила

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

Член 23

Адресати

Адресати на настоящата директива са държавите членки.

Съставено в ...,

За Европейския парламент	*За Съвета*
Председател	*Председател*

ПРИЛОЖЕНИЕ I

Изисквания и задачи на екипите за незабавно реагиране при компютърни инциденти (CERT)

Изискванията към CERT и техните задачи се определят по подходящ начин и ясно, като в тяхна подкрепа има национални политики и/или законодателство. Те включват следните елементи:

(1) Изисквания към CERT

а) ***CERT***гарантират много добра наличност на своите комуникационни услуги, като не допускат съществуването на точки, повредата в които може да доведе до общ срив, и разполагат с няколко канала, по 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 заинтересованите страни и на партньорите от сътрудничеството. **[Изм. 128]**

б) CERT изпълняват и управляват мерки за сигурност, с които да гарантират поверителността, целостта, наличността и автентичността на информацията, която получават и с която работят.

в) Офисите на ***CERT*** и поддържащите дейността на CERT информационни системи се разполагат в помещения с гарантирана сигурност ***с осигурени мрежови информационни системи***. **[Изм. 129]**

г) Създава се система за качествено управление на услугите с цел проследяване представянето на CERT и гарантиране на траен процес на усъвършенстване. Тя се основава на ясно определени параметри, които включват формалните равнища на услугите и основни показатели на представянето.

д) Непрекъснатост на дейността

– CERT разполага с подходяща система за управление и разпределяне на заявките с цел да улесни предаването на задачите от един на друг изпълнител,

– CERT разполага с достатъчен персонал, който да гарантира, че CERT е постоянно на разположение,

– CERT разчита на инфраструктура с гарантирана непрекъснатост на дейността. За тази цел за CERT се създават резервирани системи и резервно работно пространство, чрез които да се гарантира постоянен достъп до комуникационните средства.

(2) Задачи на CERT

а) Задачите на CERT включват поне следните елементи:

– ***Откриване и*** следене на инцидентите на национално равнище, **[Изм. 130]**

– Осигуряване на ранни предупреждения, сигнали за тревога, съобщения и разпространяване на информация за инциденти и рискове сред съответните заинтересовани страни,

– Отговор на инциденти,

– Осигуряване на динамичен анализ на рисковете и инцидентите и информация за текущата ситуация,

– Постигане на мащабна обществена осведоменост за рисковете, свързани с онлайн дейностите,

– ***Активно участие в мрежи на Съюза за сътрудничество за CERT и в международни мрежи за сътрудничество за CERT,*** **[Изм. 131]**

– Организиране на кампании за МИС.

б) CERT изграждат отношения на сътрудничество с частния сектор.

в) С цел улесняване на сътрудничеството CERT насърчава възприемането и използването на общи практики за стандартизация за:

– процедури за действия при инциденти и рискове,

– системи за класификация на инциденти, рискове и информация,

– таксономии на параметрите,

– формати за обмен на информация за рискове и инциденти и договореност за системно именуване.

ПРИЛОЖЕНИЕ II

Списък на участниците на пазара

~~Посочени в член 3, параграф 8, буква а):~~

~~1. Платформи за електронна търговия~~

~~2. Портали за плащания в интернет~~

~~3. Социални мрежи~~

~~4. Машини за търсене~~

~~5. Услуги за изчисления в облак~~

~~6. Магазини за приложни програми~~

~~Посочени в член 3, параграф 8, буква б):~~ **[Изм. 132]**

1. Енергетика

а) Електроенергия

– доставчици ~~на електроенергия и природен газ~~

– оператори на ~~системи за електро- и газоразпределение и търговци на дребно~~ ***разпределителни мрежи и търговци на дребно***, работещи с крайните потребители

~~– оператори на газопреносни мрежи, оператори на хранилища, оператори на системи за съхранение и за ВПГ~~

– оператори на преносни мрежи за електроенергия

б) Нефт

– нефтопроводи и нефтохранилища

– ***оператори на съоръжения за добив, рафиниране и преработка, съхранение и пренос на нефт***

в) Природен газ

~~– участници на пазара на електроенергия и природен газ~~

– ***доставчици***

– ***оператори на разпределителни мрежи и търговци на дребно, работещи с крайните потребители***

– ***оператори на газопреносни мрежи, оператори на системи за съхранение и за втечнен природен газ***

– оператори на съоръжения за добив, рафиниране ~~и,~~ преработка**,** ***съхранение и пренос*** на нефт и природен газ

– ***участници на пазара на природен газ*** **[Изм. 133]**

2. Транспорт

~~– въздушни превозвачи (товарен и пътнически въздушен транспорт)~~

~~– морски превозвачи (компании за морски и крайбрежен воден транспорт на пътници и компании за морски и крайбрежен воден транспорт на товари)~~

~~– железопътен транспорт (управители на инфраструктура, интегрирани дружества и железопътни транспортни оператори)~~

~~– летища~~

~~– пристанища~~

~~– оператори ръководство на движението~~

~~– спомагателни логистични услуги (а) складове и съхранение, б) обработка на товари и в) други транспортни подпомагащи услуги)~~

а) Автомобилен транспорт

i) оператори ръководство на движението

ii*) *спомагателни логистични услуги:

– ***складиране и съхраняване,***

– ***обработка на товари и***

– ***други подпомагащи транспортни услуги***

б) Железопътен транспорт

i) железопътен транспорт (управители на инфраструктура, интегрирани дружества и железопътни транспортни оператори)

ii) оператори ръководство на движението

iii) спомагателни логистични услуги:

– *складиране и съхраняване,*

– *обработка на товари и*

– *други подпомагащи транспортни услуги*

в) Въздушен транспорт

i) въздушни превозвачи (товарен и пътнически въздушен транспорт)

ii) летища

iii) оператори ръководство на движението

iv) спомагателни логистични услуги:

– *складиране,*

– *обработка на товари и*

– *други подпомагащи транспортни услуги*

г) морски транспорт

i) морски превозвачи (компании за вътрешен, морски и крайбрежен воден транспорт на пътници и компании за вътрешен, морски и крайбрежен воден транспорт на товари) **[Изм. 134]**

3. Банково дело: кредитни институции в съответствие с член 4, точка 1 от Директива 2006/48/ЕО на Европейския парламент и на Съвета[1]

4. Инфраструктури на финансовия пазар: ~~фондови борси~~ ***регулирани пазари, многостранни търговски системи, организирани търговски системи*** и централни контрагенти клирингови къщи **[Изм. 135]**

5. Сектор на здравеопазването: здравни заведения (включително болници и частни клиники) и други субекти, участващи в предоставянето на здравни услуги.

5а. Добиване на вода и водоснабдяване **[Изм. 136]**

5б. Верига на доставка на храни **[Изм. 137]**

5в. Точки за обмен в интернет **[Изм. 138]**

[1] Директива 2006/48/ЕО на Европейския парламент и на Съвета от 14 юни 2006 г. относно предприемането и осъществяването на дейност от кредитните институции (ОВ L 177, 30.6.2006 г., стр. 1).