Rada
Európskej únie

V Bruseli 29. mája 2018
(OR. en)

9350/18

Medziinštitucionálny spis:
2017/0225 (COD)

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

POZNÁMKA

Od:	Predsedníctvo
Komu:	Rada
Č. predch. dok.:	8834/18
Č. dok. Kom.:	12183/17
Predmet:	Návrh NARIADENIA EURÓPSKEHO PARLAMENTU A RADY o Agentúre Európskej únie pre kybernetickú bezpečnosť ENISA, o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii bezpečnosti informačných a komunikačných technológií („akt/nariadenie o kybernetickej bezpečnosti“) – všeobecné smerovanie

I. ÚVOD

1. Komisia 13. septembra 2017 v rámci svojej stratégie pre jednotný digitálny trh prijala a postúpila Rade a Európskemu parlamentu uvedený návrh[1], ktorého právnym základom je článok 114 ZFEÚ. Tento návrh je súčasťou tzv. balíka pre kybernetickú bezpečnosť a zameriava sa na vysokú úroveň kybernetickej bezpečnosti, kybernetickej odolnosti a dôvery v Únii s cieľom zabezpečiť riadne fungovanie vnútorného trhu.

2. V navrhovanom nariadení sa stanovujú ciele, úlohy a organizačné aspekty agentúry Európskej únie pre kybernetickú bezpečnosť ENISA a vytvára rámec pre zriadenie európskych systémov certifikácie kybernetickej bezpečnosti s cieľom zaistiť primeranú úroveň kybernetickej bezpečnosti produktov a služieb IKT v Únii. K návrhu Komisie je priložené posúdenie vplyvu, v ktorom sa skúma konkrétny súbor ôsmich možností politiky, ktorý zahŕňa preskúmanie agentúry ENISA a certifikácie kybernetickej bezpečnosti IKT.

3. Navrhované nariadenie má dve hlavné zložky:

   - trvalý mandát agentúry s vymedzeným rozsahom pôsobnosti vzhľadom na potreby vyplývajúce z priorít a nástrojov novej politiky a obnovený súbor úloh a funkcií agentúry zameraný na účinnú a efektívnu podporu členských štátov, inštitúcií EÚ a ďalších zainteresovaných strán v ich úsilí o zaistenie bezpečného kybernetického priestoru;

   - Európsky rámec certifikácie kybernetickej bezpečnosti produktov a služieb IKT a pravidlá v oblasti európskych systémov certifikácie kybernetickej bezpečnosti, ktoré umožňujú, aby boli certifikáty vydané v rámci týchto systémov platné a uznávané vo všetkých členských štátoch, a aby sa riešila súčasná roztrieštenosť trhu.

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

4. Európska rada[2] v októbri 2017 vyzvala, aby Komisia vypracovala návrhy o kybernetickej bezpečnosti holisticky a včas a aby sa tieto návrhy bezodkladne preskúmali na základe akčného plánu, ktorý stanoví Rada.

5. Rada pre všeobecné záležitosti prijala 12. decembra 2017 akčný plán[3], ktorým sa vykonávajú závery Rady[4] o spoločnom oznámení[5] Európskemu parlamentu a Rade: Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti pre EÚ. Akčný plán odráža ambíciu Rady dosiahnuť všeobecné smerovanie k uvedenému návrhu do júna 2018.

6. V Európskom parlamente bola za spravodajkyňu vymenovaná Angelika NIEBLEROVÁ (ITRE, PPE). Výbor ITRE bude o svojej správe hlasovať 19. júna 2018.

7. Európsky hospodársky a sociálny výbor prijal svoje stanovisko 14. februára 2018.

II. PRÁCA V RADE

8. Komisia predložila tento návrh a posúdenie jeho vplyvu horizontálnej pracovnej skupine pre kybernetické otázky (ďalej len „pracovná skupina“) 26. septembra 2017; pracovná skupina preskúmala posúdenie vplyvu 20. októbra 2017. Následné diskusie boli venované operačnej kapacite agentúry a rozsahu interakcie s príslušnými vnútroštátnymi orgánmi, ako aj vplyvu certifikačného rámca na trh a konkurencieschopnosť podnikov. Vo všeobecnosti dostalo posúdenie vplyvu aj návrh pozitívnu odozvu delegácií.

---

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

9. Rokovania o samotnom návrhu sa v pracovnej skupine začali v novembri 2017 počas estónskeho predsedníctva a pokračovali počas bulharského predsedníctva. V súvislosti s týmto návrhom sa konalo 12 zasadnutí, ktoré viedli k ôsmim po sebe nasledujúcim revidovaným verziám návrhu s cieľom dosiahnuť dohodu o všeobecnom smerovaní na nadchádzajúcom zasadnutí Rady pre dopravu, telekomunikácie a energetiku (telekomunikácie), ktoré sa uskutoční 8. júna 2018.

10. Výsledok rokovaní pracovnej skupiny, ktoré sa konalo 14. – 15. mája 2018, ako aj revidované kompromisné znenie predsedníctva sa uvádzajú v prílohe k tejto poznámke. Odôvodnenia sa upravili tak, aby odrážali zmeny v normatívnych ustanoveniach. Všetky zmeny v porovnaní so znením návrhu Komisie sú označené **tučným písmom** alebo symbolom [...]. Zmeny v porovnaní s posledným dokumentom pracovnej skupiny v anglickom jazyku (8834/18) sú označené **tučným podčiarknutým písmom** a vypustený text symbolom **[...].**

III. ZÁVER

11. Kompromisné znenie predsedníctva uvedené v prílohe odráža úsilie predsedníctva a členských štátov dospieť k primerane vyváženému zneniu.

12. Výbor stálych predstaviteľov dosiahol 25. mája 2018 dohodu o kompromisnom znení predsedníctva s výhradou zmien v článku 19 ods. 5 a článku 48 ods. 5, ktoré sú uvedené v prílohe.

13. Rada sa preto vyzýva, aby prijala všeobecné smerovanie na zasadnutí 8. júna 2018 a poverila predsedníctvo začatím rokovaní o tomto spise so zástupcami Európskeho parlamentu a Európskej komisie.

PRÍLOHA

Návrh

NARIADENIE EURÓPSKEHO PARLAMENTU A RADY

o *[...] Agentúre Európskej únie pre kybernetickú bezpečnosť ENISA*, o zrušení nariadenia (EÚ) č. 526/2013 a o certifikácii kybernetickej bezpečnosti informačných a komunikačných technológií („akt o kybernetickej bezpečnosti“)

(Text s významom pre EHP)

EURÓPSKY PARLAMENT A RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie, a najmä na jej článok 114,

so zreteľom na návrh Európskej komisie,

po postúpení návrhu legislatívneho aktu národným parlamentom,

so zreteľom na stanovisko Európskeho hospodárskeho a sociálneho výboru[6],

so zreteľom na stanovisko Výboru regiónov[7],

konajúc v súlade s riadnym legislatívnym postupom,

[6] Ú. v. EÚ C …, …, s. ….
[7] Ú. v. EÚ C …, …, s. ….

keďže:

(1) Siete, informačné systémy a telekomunikačné siete a služby sú pre našu spoločnosť kľúčové a stali sa oporným pilierom hospodárskeho rastu. Na informačných a komunikačných technológiách sú založené komplexné systémy, ktoré podporujú spoločenské činnosti, udržujú chod kľúčových odvetví hospodárstva ako zdravotníctvo, energetika, financie či doprava, a najmä podporujú fungovanie vnútorného trhu.

(2) Občania, firmy i verejné orgány v Únii dnes využívajú siete a informačné systémy na každom kroku. Digitalizácia a prepojenie sa stávajú samozrejmosťou pre čoraz viac produktov a služieb, pričom sa očakáva, že s nástupom internetu vecí (IoT) prídu na trh EÚ v najbližšom desaťročí milióny, ak nie miliardy prepojených digitálnych zariadení. Na internet je pripojených čoraz viac zariadení, no ich bezpečnosť a odolnosť nie je vo fáze navrhovania dostatočne zohľadnená, čo vedie k nedostatočnej kybernetickej bezpečnosti. Keďže certifikácia sa v tomto kontexte využíva obmedzene, organizácie a jednotliví používatelia nie sú dostatočne informovaní o prvkoch kybernetickej bezpečnosti produktov a služieb IKT, čo znižuje dôveru v digitálne riešenia.

(3) Rastúca miera digitalizácie a prepojenia zvyšuje kyberneticko-bezpečnostné riziká, takže spoločnosť ako taká je zraniteľnejšia voči kybernetickým hrozbám a prehlbuje sa nebezpečenstvo pre jednotlivcov vrátane zraniteľných osôb, ako sú napríklad deti. V záujme zmiernenia rizík pre spoločnosť treba prijať všetky potrebné kroky na zvýšenie kybernetickej bezpečnosti v EÚ, aby boli siete a informačné systémy, telekomunikačné siete, digitálne produkty, služby a zariadenia, ktoré využívajú občania, verejné správy i podniky – od MSP až po prevádzkovateľov kritickej infraštruktúry – lepšie chránené pred kybernetickými hrozbami.

(4) Kybernetické útoky sú na vzostupe, takže potrebujeme lepšie brániť prepojené hospodárstvo a spoločnosť, ktoré sú voči kybernetickým hrozbám a útokom zraniteľnejšie. Zatiaľ čo kybernetické útoky sú často cezhraničné, politická reakcia orgánov zodpovedných za kybernetickú bezpečnosť a orgánov presadzovania práva prebieha prevažne na vnútroštátnej úrovni. Rozsiahle kybernetické incidenty by mohli narušiť poskytovanie základných služieb v celej EÚ. Táto situácia si vyžaduje účinnú reakciu a krízové riadenie na úrovni EÚ vychádzajúce z osobitných politík a všeobecnejších nástrojov pre európsku solidaritu a vzájomnú pomoc. Okrem toho je pre tvorcov politík, priemysel a používateľov dôležité pravidelné posudzovanie stavu kybernetickej bezpečnosti a odolnosti v Únii založené na spoľahlivých údajoch Únie, ako aj systematická predpoveď budúceho vývoja, výziev a hrozieb, a to tak na úrovni Únie, ako aj celosvetovo.

(5) Keďže výzvy, ktorým Únia v oblasti kybernetickej bezpečnosti čelí, sa stupňujú, je potrebný komplexný súbor opatrení, ktoré nadviažu na predošlé kroky Únie a zaistia synergiu cieľov. Zahŕňa to potrebu ďalej posilniť spôsobilosti a pripravenosť členských štátov i podnikov, ako aj zlepšiť spoluprácu a koordináciu medzi členskými štátmi a inštitúciami, agentúrami a orgánmi EÚ. Okrem toho, keďže kybernetické hrozby nepoznajú hranice, treba posilniť spôsobilosti na úrovni Únie, ktoré by mohli doplniť opatrenia členských štátov, najmä pri rozsiahlych cezhraničných kybernetických incidentoch a krízach. Viac treba urobiť aj v otázke informovanosti občanov a podnikov o otázkach kybernetickej bezpečnosti. Transparentné informácie o úrovni bezpečnosti produktov a služieb IKT by navyše mohli posilniť celkovú dôveru v digitálny jednotný trh. Tento cieľ môže uľahčiť celoúnijná certifikácia, ktorá poskytne spoločné kyberneticko-bezpečnostné požiadavky a hodnotiace kritériá naprieč vnútroštátnymi trhmi a odvetviami.

(6) Európsky parlament a Rada prijali v roku 2004 nariadenie (ES) č. 460/2004[8] o zriadení agentúry ENISA, ktoré malo prispieť k cieľom v oblasti zabezpečenia vysokej úrovne sieťovej a informačnej bezpečnosti v rámci Únie a vybudovaniu kultúry sieťovej a informačnej bezpečnosti v prospech občanov, spotrebiteľov, podnikov a verejnej správy. V roku 2008 prijal Európsky parlament a Rada nariadenie (ES) č. 1007/2008[9], ktorým sa predĺžil mandát agentúry do marca 2012. Nariadením (ES) č. 580/2011[10] sa tento mandát agentúry ďalej predĺžil do 13. septembra 2013. V roku 2013 prijal Európsky parlament a Rada nariadenie (EÚ) č. 526/2013[11] o Agentúre ENISA a o zrušení nariadenia (ES) č. 460/2004, ktorým sa mandát agentúry predĺžil do júna 2020.

---

8 Nariadenie Európskeho parlamentu a Rady (ES) č. 460/2004 z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií (Ú. v. EÚ L 77, 13.3.2004, s. 1).

9 Nariadenie Európskeho parlamentu a Rady (ES) č. 1007/2008 z 24. septembra 2008, ktorým sa mení a dopĺňa nariadenie (ES) č. 460/2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií, pokiaľ ide o dobu jej trvania (Ú. v. EÚ L 293, 31.10.2008, s. 1).

10 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 580/2011 z 8. júna 2011, ktorým sa mení a dopĺňa nariadenie (ES) č. 460/2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií, pokiaľ ide o jej trvanie (Ú. v. EÚ L 165, 24.6.2011, s. 3).

11 Nariadenie Európskeho parlamentu a Rady (EÚ) č. 526/2013 z 21. mája 2013 o Agentúre Európskej únie pre sieťovú a informačnú bezpečnosť (ENISA) a o zrušení nariadenia (ES) č. 460/2004 (Ú. v. EÚ L 165, 18.6.2013, s. 41).

(7) Únia už prijala dôležité kroky na zaistenie kybernetickej bezpečnosti a zvýšenie dôvery v digitálne technológie. V roku 2013 bola prijatá stratégia kybernetickej bezpečnosti EÚ, ktorá má viesť politickú reakciu Únie na kybernetické hrozby a riziká. V snahe lepšie chrániť Európanov v online svete prijala Únia v roku 2016 prvý legislatívny akt v oblasti kybernetickej bezpečnosti, a to smernicu (EÚ) 2016/1148 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii (tzv. smernica NIS). V smernici NIS sa stanovujú požiadavky na vnútroštátne spôsobilosti v oblasti kybernetickej bezpečnosti, zriaďujú sa prvé mechanizmy na posilnenie strategickej a operačnej spolupráce členských štátov a zavádzajú sa povinnosti prijímať bezpečnostné opatrenia a oznamovať incidenty v odvetviach, ktoré sú pre hospodárstvo a spoločnosť kľúčové (ako energetika, doprava, voda, bankovníctvo, infraštruktúry finančných trhov, zdravotníctvo, digitálna infraštruktúra), ako aj v prípade kľúčových poskytovateľov digitálnych služieb (vyhľadávače, služby cloud computingu a online trhoviská). Agentúre ENISA bola zverená kľúčová rola podpory vykonávania smernice NIS. Účinný boj proti počítačovej kriminalite je navyše dôležitou prioritou Európskeho programu v oblasti bezpečnosti a prispieva k celkovému cieľu vysokej úrovne kybernetickej bezpečnosti.

(8) Je zrejmé, že od prijatia stratégie kybernetickej bezpečnosti EÚ v roku 2013 a od posledného prehodnotenia mandátu agentúry sa celkový politický kontext výrazne zmenil, a to aj z hľadiska neistejšieho a menej bezpečného globálneho prostredia. V tejto súvislosti a v rámci novej kyberneticko-bezpečnostnej politiky Únie treba mandát agentúry ENISA zrevidovať s cieľom vymedziť jej rolu v zmenenom ekosystéme kybernetickej bezpečnosti, aby účinne prispievala k reakcii Únie na výzvy v tejto sfére vyplývajúce z tejto radikálne zmenenej povahy hrozieb, keďže ako potvrdilo hodnotenie samotnej agentúry, jej súčasný mandát na to nestačí.

(9) Agentúra zriadená týmto nariadením by mala byť nástupcom agentúry ENISA zriadenej nariadením (EÚ) č. 526/2013. Agentúra by mala vykonávať úlohy zverené týmto nariadením a právnymi aktmi Únie v oblasti kybernetickej bezpečnosti, okrem iného ako zdroj odborných poznatkov a poradenstva, ale i centrum informácií a znalostí v rámci Únie. Mala by podporovať výmenu osvedčených postupov medzi členskými štátmi a súkromnými aktérmi, ponúkať Európskej komisii a členským štátom politické návrhy, pôsobiť ako referenčný bod pre odvetvové politické iniciatívy Únie v otázkach kybernetickej bezpečnosti a podnecovať operačnú spoluprácu medzi členskými štátmi navzájom i vo vzťahu k európskym inštitúciám, agentúram a orgánom.

(10) V rozhodnutí 2004/97/ES, Euratom prijatom na zasadnutí Európskej rady 13. decembra 2003 zástupcovia členských štátov rozhodli, že agentúra ENISA má mať sídlo v gréckom meste, ktoré určí grécka vláda. Hostiteľský členský štát agentúry by mal zabezpečiť čo najlepšie podmienky pre bezproblémové a efektívne fungovanie agentúry. Pre riadne a efektívne plnenie jej úloh, prijímanie a udržanie zamestnancov a zvýšenie efektívnosti nadväzovania vzťahov je nevyhnutné, aby agentúra sídlila na vhodnom mieste, ktoré okrem iného poskytuje vhodné dopravné spojenia a zariadenia pre manželov (manželky) a deti sprevádzajúce zamestnancov agentúry. Potrebné opatrenia by sa mali stanoviť v dohode medzi agentúrou a hostiteľským členským štátom uzavretou po získaní súhlasu správnej rady agentúry.

(11) Keďže Únia čelí narastajúcim kyberneticko-bezpečnostným výzvam, mal by sa zvýšiť objem finančných a ľudských zdrojov pridelených agentúre, aby sa odzrkadlilo jej posilnené poslanie a úlohy a jej rozhodujúce postavenie v ekosystéme organizácií brániacich európsky digitálny ekosystém.

(12) Agentúra by mala zabezpečiť a udržiavať špičkové odborné poznatky a pôsobiť ako referenčný bod budujúci dôveru v jednotný trh svojou nezávislosťou, kvalitou poskytovaného poradenstva a šírených informácií, transparentnosťou svojich postupov a pracovných metód a dôslednosťou pri vykonávaní úloh. Agentúra by mala **podporovať** [...] vnútroštátne úsilie a **proaktívne prispievať** k snahám Únie, pričom by mala vykonávať svoje úlohy v plnej spolupráci s inštitúciami, [...] agentúrami a **orgánmi** Únie a s členskými štátmi. Okrem toho by agentúra mala nadväzovať na vstupy zo súkromného sektora a od ďalších relevantných zainteresovaných strán a na spoluprácu s nimi. Mal by sa stanoviť súbor úloh určujúcich, ako agentúra dosiahne svoje ciele, ktorý by mal umožniť flexibilitu jej činností.

(13) Agentúra by mala pomáhať Komisii poskytovaním poradenstva, stanovísk a analýz týkajúcich sa všetkých záležitostí Únie súvisiacich s vývojom, ako aj s tvorbou, aktualizáciou a revíziou politík a právnych predpisov v oblasti kybernetickej bezpečnosti a **jej odvetvových aspektov s cieľom posilniť relevantnosť európskych politík a právnych predpisov EÚ s rozmerom v oblasti kybernetickej bezpečnosti a umožniť konzistentnosť pri ich vykonávaní na vnútroštátnej úrovni** [...]. Agentúra by mala byť referenčným bodom poradenstva a odborných poznatkov pre odvetvové politické a legislatívne iniciatívy Únie zahŕňajúce rozmer kybernetickej bezpečnosti.

(14) Základnou úlohou agentúry je presadzovať dôsledné vykonávanie príslušného právneho rámca, a najmä účinné vykonávanie smernice NIS, ktorá je kľúčom k posilneniu kybernetickej odolnosti. Keďže kybernetické hrozby sú neustále v pohybe, je jasné, že členské štáty potrebujú podporu komplexnejšieho prierezového prístupu k budovaniu kybernetickej odolnosti.

(15) Agentúra by mala pomáhať členským štátom a inštitúciám, [...] agentúram a **orgánom** Únie v ich úsilí vybudovať a zdokonaľovať spôsobilosti a pripravenosť predchádzať kybernetickým [...] **hrozbám** a incidentom spojeným s bezpečnosťou sietí a informačných systémov, odhaľovať ich a reagovať na ne. Najmä by agentúra mala podporovať rozvoj a posilňovanie vnútroštátnych jednotiek CSIRT, aby v rámci Únie všetky dosiahli vysoký stupeň vývoja. **Činnosťami, ktoré vykonáva agentúra ENISA a ktoré sa týkajú operačných kapacít členských štátov, by sa mali len dopĺňať vlastné opatrenia, ktoré členské štáty prijali s cieľom splniť svoje povinnosti vyplývajúce zo smernice NIS, a preto by ich nemali nahrádzať** [...].

(15a) Zároveň by agentúra mala pomáhať pri príprave a aktualizácii stratégií Únie a na požiadanie aj členských štátov v oblasti bezpečnosti sietí a informačných systémov (najmä kybernetickej), podporovať ich šírenie a sledovať ich uplatňovanie. Mala by tiež verejným orgánom ponúkať školenia a vzdelávacie materiály a podľa potreby „školiť školiteľov“, aby členským štátom pomohla pri rozvoji ich vlastných školiacich kapacít.

(16) Agentúra by mala pomáhať skupine pre spoluprácu zriadenej smernicou NIS pri výkone jej úloh, a to najmä poskytovaním odborných poznatkov, poradenstva a sprostredkovaním výmeny osvedčených postupov, predovšetkým z hľadiska identifikácie prevádzkovateľov základných služieb členskými štátmi z pohľadu rizík a incidentov, a to aj v súvislosti s cezhraničnou previazanosťou.

(17) Na stimulovanie spolupráce verejného a súkromného sektora a v rámci súkromného sektora, by [...] **agentúra mala podporovať výmenu informácií v odvetviach a medzi nimi, najmä pokiaľ ide o odvetvia uvedené v prílohe II k smernici (EÚ) 2016/1148, a to poskytovaním najlepších postupov a usmernení k existujúcim nástrojom a postupom, ako aj usmerňovaním v otázke riešenia regulačných problémov spojených s výmenou informácií, napríklad uľahčovaním** [...] zriaďovania odvetvových stredísk pre výmenu a analýzu informácií (ISAC) [...].

(18) Agentúra by mala zhromažďovať a analyzovať **dobrovoľné zdieľané** správy vnútroštátnych jednotiek CSIRT a tímu CERT-EU na **účely pomoci členským štátom** pri stanovovaní spoločných [...] **postupov**, jazyka a terminológie na výmenu informácií. Okrem toho by agentúra mala angažovať aj súkromný sektor v zmysle smernice NIS, ktorá stanovila základ pre dobrovoľnú výmenu technických informácií na operačnej úrovni [...] v sieti jednotiek CSIRT

(19) Agentúra by mala prispievať k reakcii na úrovni EÚ v prípade rozsiahlych cezhraničných kybernetických incidentov a kríz. Táto funkcia **by sa mala vykonávať v súlade s jej mandátom podľa tohto nariadenia a prístupom, na ktorom sa dohodnú členské štáty v kontexte odporúčania Komisie o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu. To by mohlo** zahŕňať aj zber relevantných informácií a uľahčovanie interakcie medzi sieťou jednotiek CSIRT a technickou obcou či aktérmi zodpovednými za krízové riadenie. Okrem toho by agentúra mohla podporovať riešenie incidentov z technickej stránky uľahčovaním výmeny relevantných technických riešení medzi členskými štátmi a zabezpečením vstupov pre komunikáciu s verejnosťou. Agentúra by tento proces mala podporovať skúšaním rôznych možností takejto spolupráce na [...] **pravidelných** kyberneticko-bezpečnostných cvičeniach.

(20) [...] Agentúra by **na podporu** operačnej **spolupráce** mala [...] využívať dostupné **technické a operačné** odborné znalosti tímu CERT-EU prostredníctvom štruktúrovanej spolupráce [...].[...] Podľa potreby by sa mali medzi oboma organizáciami vytvoriť účelové dohody o fungovaní tejto spolupráce v praxi a **zabránení zdvojovaniu činností.**

(21) V súlade so svojimi úlohami [...] na **podporu operačnej spolupráce v rámci siete jednotiek CSIRT** by agentúra mala byť schopná poskytovať na **požiadanie** podporu členským štátom, napríklad tým, že bude poskytovať poradenstvo o tom, **ako zlepšiť ich spôsobilosti predchádzať incidentom, odhaľovať ich a reagovať na ne, a to tak, že bude uľahčovať [...] technické riešenie incidentov, ktoré majú významný alebo závažný vplyv [...]**, alebo zabezpečení analýzy hrozieb a incidentov. **Súčasťou uľahčovania technického riešenia incidentov, ktoré majú významný alebo závažný vplyv, by mala byť najmä podpora agentúry ENISA zameraná na dobrovoľnú výmenu technických riešení medzi členskými štátmi alebo to, že agentúra bude vypracúvať kombinované technické informácie, ako napríklad technické riešenia, ktoré dali dobrovoľne k dispozícii členské štáty.** V odporúčaní Komisie o koordinovanej reakcii na kybernetické incidenty a krízy veľkého rozsahu sa odporúča, aby členské štáty v dobrej viere spolupracovali a bez zbytočného odkladu sa vzájomne i s agentúrou ENISA delili o informácie o rozsiahlych kybernetických incidentoch a krízach. Tieto informácie by tiež mali agentúre ENISA pomôcť pri [...] **podpore operačnej spolupráce.**

(22) V rámci bežnej technickej spolupráce na podporu situačného povedomia Únie by mala agentúra pravidelne a **v úzkej spolupráci s členskými štátmi** vypracúvať technickú situačnú správu EÚ o kybernetických incidentoch a hrozbách, ktorá vychádza z verejne dostupných informácií, jej vlastných analýz a správ, ktoré jej poskytli jednotky CSIRT členských štátov [...] alebo jednotné kontaktné miesta podľa smernice NIS (**v oboch prípadoch na dobrovoľnom základe**), Európske centrum boja proti počítačovej kriminalite (EC3) pri Europole, CERT-EU a v náležitých prípadoch centrum EÚ pre spravodajské informácie (INTECEN) v rámci Európskej služby pre vonkajšiu činnosť (ESVČ). Táto správa by sa mala sprístupniť zodpovedným útvarom Rady, Komisie, vysokému predstaviteľovi Únie pre zahraničné veci a bezpečnostnú politiku a podpredsedovi Komisie a sieti jednotiek CSIRT.

(23) **Podpora agentúry pri e**[...]x post technickom **skúmaní** [...] incidentov s významným vplyvom na žiadosť [...] **dotknutého** členského štátu [...] by sa mala [...] zameriavať na predchádzanie incidentom v budúcnosti [...]. **Dotknuté členské štáty by mali agentúre poskytnúť potrebné informácie, aby mohla účinne podporiť technické skúmanie.**

(24) [...]

(25) Členské štáty môžu prizvať podniky dotknuté daným incidentom k spolupráci v podobe poskytnutia potrebných informácií a podpory agentúre bez toho, aby bolo dotknuté ich právo na ochranu citlivých obchodných informácií.

(26) Na lepšie pochopenie výziev v oblasti kybernetickej bezpečnosti a v záujme dlhodobého strategického poradenstva pre členské štáty a inštitúcie Únie musí agentúra analyzovať existujúce i nové riziká. Na to by agentúra mala v spolupráci s členskými štátmi a podľa potreby štatistickými orgánmi a ďalšími aktérmi zbierať relevantné **verejne dostupné alebo dobrovoľne zdieľané** informácie, analyzovať nové technológie a poskytovať tematické posúdenie očakávaných spoločenských, právnych, hospodárskych a regulačných vplyvov technologických inovácií na sieťovú a informačnú bezpečnosť, najmä kybernetickú. Agentúra by navyše mala členské štáty a inštitúcie, agentúry a orgány Únie podporovať pri identifikácii nastupujúcich trendov a pri predchádzaní [...] kybernetickým bezpečnostným **incidentom**, a to analýzou hrozieb a incidentov.

(27) V záujme posilnenia odolnosti Únie by agentúra mala rozvíjať špičkovú odbornosť vo sfére **kybernetickej** bezpečnosti **infraštruktúr, ktoré podporujú najmä odvetvia uvedené v prílohe II k smernici NIS, a tie, ktoré používajú poskytovatelia digitálnych služieb uvedených v prílohe III k uvedenej smernici**, [...] a to poskytovaním poradenstva, usmernení a najlepších postupov. S cieľom uľahčiť prístup k lepšie štruktúrovaným informáciám o kybernetických rizikách a ich možných riešeniach by agentúra mala zriadiť a prevádzkovať „informačné centrum“ Únie – portál s funkciou jednotného kontaktného miesta, ktorý bude verejnosti sprístupňovať informácie o kybernetickej bezpečnosti od inštitúcií, agentúr a orgánov EÚ i členských štátov.

(28) Agentúra by mala prispievať k zvyšovaniu verejného povedomia o rizikách spojených s kybernetickou bezpečnosťou a odporúčať jednotlivým používateľom – občanom i organizáciám osvedčené postupy. Agentúra by mala prispievať k propagácii osvedčených postupov a riešení u jednotlivcov a organizácii aj zberom a analýzou verejne dostupných informácií o závažných incidentoch a vypracúvaním správ s cieľom poskytnúť podnikom a občanom usmernenia a zvýšiť celkovú pripravenosť a odolnosť. Agentúra by navyše mala v spolupráci s členskými štátmi a inštitúciami, [...] agentúrami a **orgánmi** Únie organizovať pravidelné osvetové a vzdelávacie kampane pre verejnosť určené koncovým používateľom a zamerané na propagáciu bezpečnejšieho správania jednotlivcov na internete a zvyšovanie povedomia o potenciálnych hrozbách v kybernetickom priestore vrátane počítačovej kriminality, ako sú phishingové útoky, botnety, finančné a bankové podvody; zároveň by mala poskytovať rady v oblasti základnej autentifikácie a ochrany údajov. Agentúra by mala mať kľúčovú rolu pri urýchlenom zvyšovaní povedomia koncových používateľov o bezpečnosti zariadení.

(29) Na podporu podnikov pôsobiacich v odvetví kybernetickej bezpečnosti, ale i používateľov kyberneticko-bezpečnostných riešení by agentúra mala vytvoriť a prevádzkovať „monitor trhu“, ktorý bude pravidelne analyzovať a šíriť hlavné trendy na trhu kybernetickej bezpečnosti – tak na strane dopytu, ako aj ponuky.

(30) Na úplné splnenie svojich cieľov by agentúra mala udržiavať kontakty s relevantnými inštitúciami, agentúrami a orgánmi vrátane tímu CERT-EU, Európskeho centra boja proti počítačovej kriminalite (EC3) pri Europole, Európskej obrannej agentúry (EDA), Európskej agentúry na prevádzkové riadenie rozsiahlych informačných systémov (eu-LISA), Európskej agentúry pre bezpečnosť letectva (EASA), **Agentúry pre európsky globálny navigačný satelitný systém (agentúry GNSS)**, a prípadne ďalších agentúr EÚ angažovaných v otázkach kybernetickej bezpečnosti. Okrem toho by mala udržiavať kontakty aj s orgánmi zodpovednými za ochranu údajov s cieľom vymieňať si know-how a osvedčené postupy a poskytovať poradenstvo o kyberneticko-bezpečnostných aspektoch, ktoré môžu ovplyvniť ich prácu. Zástupcovia vnútroštátnych orgánov a orgánov Únie v oblasti presadzovania práva a ochrany údajov by mali byť oprávnení na účasť v stálej skupine zainteresovaných strán agentúry. Pri styku s orgánmi presadzovania práva v otázkach sieťovej a informačnej bezpečnosti, ktoré by mohli mať vplyv na ich prácu, by agentúra mala rešpektovať existujúce informačné kanály a zavedené siete.

(31) Agentúra by vo **svojej funkcii** [...] sekretariátu siete jednotiek CSIRT mala podporovať jednotky CSIRT členských štátov a tím CERT-EU v operačnej spolupráci v nadväznosti na všetky relevantné úlohy siete jednotiek CSIRT v zmysle smernice NIS. Ďalej by agentúra mala presadzovať a podporovať spoluprácu medzi príslušnými jednotkami CSIRT v prípade incidentov, útokov alebo narušení sietí či infraštruktúr pod ich správou alebo ochranou, v prípadoch, ktoré zahŕňajú alebo môžu zahŕňať aspoň dve jednotky CSIRT, pričom sa riadne zohľadnia štandardné operačné postupy siete jednotiek CSIRT.

(32) V záujme lepšej pripravenosti Únie reagovať na kybernetické incidenty by agentúra mala [...] **pravidelne** organizovať kyberneticko-bezpečnostné cvičenia na úrovni Únie a na požiadanie by mala podporiť členské štáty a inštitúcie, agentúry a orgány EÚ pri organizácii cvičení.

(33) Agentúra by mala ďalej rozvíjať a udržiavať odborné poznatky o certifikácii kybernetickej bezpečnosti v záujme podpory politiky Únie v tomto smere. Agentúra by mala podporovať využívanie certifikácie kybernetickej bezpečnosti certifikácie v Únii, a to aj prispievaním k vytvoreniu a uchovávaniu kyberneticko-bezpečnostného certifikačného rámca na úrovni Únie, aby sa posilnila transparentnosť dôveryhodnosti kybernetickej bezpečnosti produktov a služieb IKT, čím sa posilní dôvera v digitálny vnútorný trh.

(34) Účinné politiky kybernetickej bezpečnosti by mali vychádzať zo správne navrhnutých metód posudzovania rizika vo verejnom i v súkromnom sektore. Metódy posudzovania rizika sa používajú na rôznych úrovniach bez spoločného postupu ich účinného uplatňovania. Podpora a vývoj osvedčených postupov v oblasti posudzovania rizika a interoperabilných riešení riadenia rizika v organizáciách verejného a súkromného sektora zvýšia úroveň kybernetickej bezpečnosti v Únii. S týmto cieľom by agentúra mala podporovať spoluprácu zainteresovaných strán na úrovni Únie, pričom by mala uľahčovať ich úsilie o tvorbu a zavádzanie európskych a medzinárodných noriem pre riadenie rizík a merateľnú bezpečnosť elektronických produktov, systémov, sietí a služieb, ktoré spolu so softvérom tvoria sieťové a informačné systémy.

(35) Agentúra by mala podnecovať členské štáty a poskytovateľov služieb k sprísňovaniu svojich všeobecných bezpečnostných noriem tak, aby všetci používatelia internetu mohli podniknúť potrebné kroky na zaistenie svojej osobnej kybernetickej bezpečnosti. Najmä poskytovatelia služieb a výrobcovia produktov by mali z trhu stiahnuť či prepracovať produkty a služby, ktoré kyberneticko-bezpečnostným normám nevyhovujú. V spolupráci s príslušnými orgánmi môže agentúra ENISA šíriť informácie o úrovni kybernetickej bezpečnosti produktov a služieb ponúkaných na vnútornom trhu, varovať pred určitými poskytovateľmi a výrobcami a žiadať ich o zvýšenie bezpečnosti (vrátane kybernetickej) svojich produktov a služieb.

(36) Pri poskytovaní poradenstva inštitúciám, [...] agentúram a **orgánom** Únie a na požiadanie prípadne aj členským štátom o potrebách výskumu v oblasti [...] kybernetickej bezpečnosti, by agentúra mala plne zohľadňovať prebiehajúci výskum, vývoj a technologické posudzovanie, najmä v rámci rôznych výskumných iniciatív Únie. **S cieľom určiť potreby a priority v oblasti výskumu by agentúra mala konzultovať aj s príslušnými skupinami používateľov.**

(37) Kybernetické [...] **hrozby** sú globálnym problémom. Je potrebná užšia medzinárodná spolupráca s cieľom zlepšiť normy **kybernetickej** bezpečnosti vrátane vymedzenia spoločných noriem správania, zlepšiť zdieľanie informácií a presadzovať rýchlejšiu medzinárodnú spoluprácu pri reakcii na problémy sieťovej a informačnej bezpečnosti, ako aj spoločný globálny prístup k nim. Agentúra by na tento účel mala podporovať výraznejšie zapojenie Únie a spoluprácu s tretími krajinami a medzinárodnými organizáciami tým, že vo vhodných prípadoch poskytne potrebné odborné znalosti a analýzu príslušným inštitúciám, [...] agentúram **a orgánom** Únie.

(38) Agentúra by mala byť schopná reagovať na ad hoc žiadosti členských štátov a inštitúcií, agentúr a orgánov EÚ o poradenstvo a pomoc spadajúcu do rozsahu cieľov agentúry.

(39) Je potrebné uplatniť určité zásady týkajúce sa riadenia agentúry, aby sa dodržalo spoločné vyhlásenie a spoločný prístup dohodnutý medziinštitucionálnou pracovnou skupinou pre decentralizované agentúry EÚ v júli 2012, ktorých cieľom je zefektívniť činnosti agentúr a zlepšiť ich výkonnosť. Spoločné vyhlásenie a spoločný prístup by sa mali podľa potreby odraziť aj v pracovných programoch agentúry, jej hodnoteniach a praxi v oblasti podávania správ a administratívy.

(40) Správna rada zložená zo zástupcov členských štátov a Komisie by mala vymedziť všeobecné smerovanie činnosti agentúry a zabezpečiť, aby agentúra vykonávala svoje úlohy v súlade s týmto nariadením. Správna rada by mala mať potrebné právomoci na zostavovanie rozpočtu, overovanie jeho plnenia, prijatie vhodných rozpočtových pravidiel, navrhnutie transparentných pracovných postupov rozhodovania agentúry, prijatie jednotného programového dokumentu, prijatie vlastného rokovacieho poriadku, menovanie výkonného riaditeľa a rozhodovanie o predlžovaní či ukončení jeho funkčného obdobia.

(41) Aby agentúra mohla fungovať riadne a efektívne, Komisia a členské štáty by mali zabezpečiť, aby osoby, ktoré majú byť vymenované za členov správnej rady, mali zodpovedajúce odborné znalosti a skúsenosti v príslušných funkčných oblastiach. Komisia a členské štáty by mali vynaložiť úsilie aj na obmedzenie obmeny svojich zástupcov v správnej rade s cieľom zabezpečiť kontinuitu jej práce.

(42) Bezproblémové fungovanie agentúry vyžaduje, aby bol jej výkonný riaditeľ vymenovaný na základe zásluh a zdokumentovaných administratívnych a riadiacich schopností, ako aj na základe kvalifikácie a skúseností vo sfére kybernetickej bezpečnosti, a aby vykonával svoje povinnosti úplne nezávisle. Výkonný riaditeľ by mal pripraviť návrh pracovného programu agentúry po predchádzajúcej konzultácii s Komisiou a prijať všetky potrebné opatrenia na zabezpečenie riadneho vykonania pracovného programu agentúry. Výkonný riaditeľ by mal vypracovať výročnú správu, **ktorej súčasťou bude plnenie ročného pracovného programu agentúry**, ktorá sa predkladá správnej rade, návrh výkazu odhadov príjmov a výdavkov agentúry a mal by plniť rozpočet. Výkonný riaditeľ by okrem toho mal mať možnosť zriadiť ad hoc pracovné skupiny zamerané na osobitné záležitosti najmä vedeckého, technického, právneho či sociálno-ekonomického charakteru. Výkonný riaditeľ by mal zabezpečiť, aby sa členovia ad hoc pracovných skupín vyberali podľa najprísnejších požiadaviek na odbornosť, pričom by sa náležite zohľadnila reprezentatívna rovnováha medzi verejnými správami členských štátov, inštitúciami Únie, súkromným sektorom vrátane príslušného odvetvia, užívateľmi a akademickými expertmi v oblasti sieťovej a informačnej bezpečnosti, a to podľa konkrétnej tematiky.

(43) Výkonná rada by mala prispievať k efektívnej činnosti správnej rady. V rámci prípravných prác spojených s rozhodnutiami správnej rady by mala podrobne skúmať relevantné informácie a dostupné možnosti, radiť a ponúkať riešenia na prípravu príslušných rozhodnutí správnej rady.

(44) Agentúra by mala mať stálu skupinu zainteresovaných strán ako poradný orgán s cieľom zabezpečiť pravidelný dialóg so súkromným sektorom, organizáciami spotrebiteľov a inými príslušnými zainteresovanými stranami. Stála skupina zainteresovaných strán zriadená správnou radou na návrh výkonného riaditeľa by sa mala zameriavať na otázky dôležité pre zainteresované strany a upriamiť na ne pozornosť agentúry. Zloženie stálej skupiny zainteresovaných strán a úlohy zverené tejto skupine, s ktorou treba konzultovať najmä návrh [...]**p**racovného [...]**p**rogramu, by mali zabezpečiť dostatočné zastúpenie zainteresovaných strán na práci agentúry.

(45) Agentúra by mala disponovať pravidlami na predchádzanie konfliktu záujmov a jeho riadenie. Agentúra by mala uplatňovať príslušné pravidlá Únie týkajúce sa prístupu verejnosti k dokumentom, ako sa stanovujú v nariadení Európskeho parlamentu a Rady (ES) č. 1049/2001[12]. Na spracovanie osobných údajov agentúrou by sa malo vzťahovať nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov[13]. Agentúra by mala dodržiavať ustanovenia platné pre inštitúcie Únie, ako aj vnútroštátne právne predpisy o zaobchádzaní s informáciami, najmä s citlivými neutajovanými informáciami a utajovanými skutočnosťami EÚ.

---

[12] Nariadenie Európskeho parlamentu a Rady (ES) č. 1049/2001 z 30. mája 2001 o prístupe verejnosti k dokumentom Európskeho parlamentu, Rady a Komisie (Ú. v. ES L 145, 31.5.2001, s. 43).

[13] Ú. v. ES L 8, 12.1.2001, s. 1.

(46) S cieľom zaručiť úplnú autonómiu a nezávislosť agentúry a umožniť jej plniť ďalšie a nové úlohy vrátane nepredvídaných núdzových úloh by sa mal agentúre poskytnúť dostatočný a nezávislý rozpočet, ktorého príjmy pochádzajú predovšetkým z príspevku Únie a príspevkov tretích krajín, ktoré sa podieľajú na práci agentúry. Väčšina zamestnancov agentúry by mala byť priamo zapojená do operačného plnenia mandátu agentúry. Hostiteľský členský štát alebo akýkoľvek iný členský štát by mali mať možnosť dobrovoľne prispievať do príjmov agentúry. Rozpočtový postup Únie by sa mal naďalej uplatňovať, pokiaľ ide o všetky dotácie započítateľné do všeobecného rozpočtu Únie. Okrem toho by Dvor audítorov mal vykonať audit účtov agentúry v záujme transparentnosti a zodpovednosti.

(47) [...]

(48) Certifikácia kybernetickej bezpečnosti zohráva významnú úlohu pri posilňovaní dôvery v produkty a služby IKT, ako aj ich bezpečnosti. Digitálny jednotný trh, a najmä dátové hospodárstvo a internet vecí môžu prosperovať iba ak široká verejnosť verí, že takéto produkty a služby poskytujú určitú mieru dôveryhodnosti kybernetickej bezpečnosti. Prepojené a automatizované vozidlá, elektronické zdravotnícke pomôcky, automatické priemyselné riadiace systémy či inteligentné siete sú iba niektorými príkladmi odvetví, kde už sa certifikácia bežne využíva alebo sa začne využívať v blízkej budúcnosti. Smernica NIS pokrýva aj odvetvia, kde je certifikácia kybernetickej bezpečnosti kľúčová.

(49) Vo svojom oznámení s názvom „Posilnenie odolnosti kybernetického systému a podpora konkurencieschopného a inovačného odvetvia kybernetickej bezpečnosti v Európe“ z roku 2016 Komisia zdôraznila potrebu kvalitných, cenovo dostupných a interoperabilných produktov a riešení v oblasti kybernetickej bezpečnosti. Ponuka produktov a služieb IKT na jednotnom trhu je geograficky stále veľmi fragmentovaná. Dôvodom je, že vývoj odvetvia kybernetickej bezpečnosti v Európe sa do značnej miery riadil dopytom verejných správ jednotlivých štátov. Medzi ďalšie nedostatky ovplyvňujúce kybernetickú bezpečnosť na jednotnom trhu patrí absencia interoperabilných riešení (technických noriem), postupov a celoúnijných mechanizmov certifikácie. Na jednej strane to európskym firmám sťažuje možnosť konkurovať na národnej, európskej i svetovej úrovni. Na druhej sa okliešťuje ponuka reálne využiteľných kyberneticko-bezpečnostných technológií, ku ktorým majú jednotlivci a spoločnosti prístup. Podobne Komisia vo svojom preskúmaní vykonávania stratégie digitálneho jednotného trhu v polovici trvania zdôraznila potrebu bezpečných pripojených produktov a systémov a naznačila, že vytvorenie európskeho rámca bezpečnosti IKT, v ktorom sa stanovia pravidlá organizovania certifikácie bezpečnosti IKT v Únii, by mohlo zachovať dôveru v internet a zároveň vyriešiť súčasnú fragmentáciu trhu kybernetickej bezpečnosti.

(50) Certifikácia kybernetickej bezpečnosti **procesov**, produktov a služieb IKT sa dnes využíva iba obmedzene. Ak sa uplatňuje, je to zväčša na úrovni členských štátov alebo z iniciatívy odvetvia. V tomto kontexte certifikát vystavený niektorým orgánom kybernetickej bezpečnosti v zásade iné členské štáty neuznávajú. Môže sa teda stať, že spoločnosti musia svoje produkty a služby certifikovať v niekoľkých členských štátoch pôsobenia, napríklad ak sa chcú zapojiť do ich verejných obstarávaní. Okrem toho sa síce objavujú nové systémy, no nezdá sa, že by koherentne a holisticky pristupovali k horizontálnym otázkam kybernetickej bezpečnosti, ako je napríklad internet vecí. Existujúce systémy vykazujú výrazné nedostatky a rozdiely z hľadiska škály pokrytia produktov, úrovne dôveryhodnosti bezpečnosti, vecných kritérií a samotného využitia.

(51) V minulosti sa objavili určité snahy smerujúce k vzájomnému uznávaniu certifikátov v Európe. Úspešné však boli iba sčasti. Najvýznamnejším príkladom v tomto smere je dohoda skupiny vysokých úradníkov pre bezpečnosť informačných systémov (SOG-IS) o vzájomnom uznávaní (DVU). Hoci ide o najvýznamnejší model spolupráce a vzájomného uznávania v oblasti bezpečnostnej certifikácie, [...] zmluvnými stranami dohody SOG-IS je len niekoľko členských štátov Únie. Účinnosť dohody SOG-IS DVU na vnútornom trhu je teda obmedzená.

(52) Z uvedených dôvodov treba zriadiť európsky rámec certifikácie kybernetickej bezpečnosti, v ktorom sa stanovia základné horizontálne požiadavky európskych systémov certifikácie kybernetickej bezpečnosti, ktoré sa majú vypracovať, a umožní sa uznávanie a uplatňovanie certifikátov a **vyhlásení o zhode EÚ** pre produkty a služby IKT vo všetkých členských štátoch. Tento európsky rámec by mal plniť dvojaký účel: na jednej strane by mal prispievať k posilneniu dôvery v produkty a služby IKT certifikované podľa takýchto systémov. Na druhej strane by mal predchádzať množeniu nekompatibilných či prekrývajúcich sa národných certifikácií kybernetickej bezpečnosti, čím sa znížia náklady podnikov pôsobiacich na digitálnom jednotnom trhu. Systémy by mali byť nediskriminačné a založené na medzinárodných a/alebo [...]**európskych** normách, pokiaľ tieto nie sú neefektívne alebo nevhodné na plnenie legitímnych cieľov EÚ v tejto oblasti.

(53) Komisia by mala byť splnomocnená na prijímanie európskych systémov certifikácie kybernetickej bezpečnosti pre konkrétne skupiny **procesov**, produktov a služieb IKT. Uplatňovanie týchto systémov a dohľad nad nimi by mali vykonávať vnútroštátne orgány pre certifikáciu [...] **kybernetickej bezpečnosti**, pričom certifikáty vydané podľa týchto systémov by mali byť platné a uznávané v celej Únii. Z pôsobnosti nariadenia by sa mali vyňať certifikačné systémy, ktoré uplatňuje príslušné odvetvie alebo iné súkromné organizácie. Orgány, ktoré takéto systémy prevádzkujú, však môžu Komisii navrhnúť zváženie ich použitia ako základ pre schválenie v podobe európskeho systému.

(54) Ustanoveniami tohto nariadenia by nemala byť dotknutá legislatíva Únie stanovujúca konkrétne pravidlá certifikácie produktov a služieb IKT. Najmä všeobecné nariadenie o ochrane údajov obsahuje ustanovenia o zriadení certifikačných mechanizmov, pečatí a značiek ochrany údajov na preukázanie súladu spracovateľských operácií prevádzkovateľov a sprostredkovateľov s daným nariadením. Tieto certifikačné mechanizmy, pečate a značky ochrany údajov by mali dotknutým osobám umožniť rýchle vyhodnotenie, nakoľko príslušné produkty a služby chránia údaje. Týmto nariadením nie je dotknutá certifikácia operácií spracovania údajov podľa všeobecného nariadenia o ochrane údajov, čo platí aj pre prípady, keď sú takéto operácie súčasťou produktov a služieb.

(55) Účelom európskych systémov certifikácie kybernetickej bezpečnosti by malo byť, že sa zabezpečí, aby **procesy**, produkty a služby IKT, ktoré boli certifikované takýmto systémom, spĺňali uvedené požiadavky [...] s cieľom [...] **chrániť** dostupnosť, pravosť, integritu a dôvernosť uložených, prenášaných alebo spracúvaných údajov alebo súvisiacich funkcií či služieb, ktoré sa cez tieto produkty, procesy, služby a systémy ponúkajú alebo sprístupňujú, **a to počas ich celého životného cyklu** v zmysle tohto nariadenia. V tomto nariadení nie je možné stanoviť podrobné kyberneticko-bezpečnostné požiadavky na všetky **procesy**, produkty a služby IKT. **Procesy**, produkty a služby IKT, ako aj súvisiace kyberneticko-bezpečnostné potreby sú také rozmanité, že je veľmi ťažké stanoviť všeobecné požiadavky na kybernetickú bezpečnosť, ktoré by sa dali uplatniť plošne. Treba preto prijať širokozáberový a všeobecný koncept kybernetickej bezpečnosti na účely certifikácie doplnený súborom špecifických kyberneticko-bezpečnostných cieľov, ktoré treba pri návrhu európskych systémov certifikácie kybernetickej bezpečnosti zohľadniť. Spôsoby, ktorými sa tieto ciele pri konkrétnych **procesoch**, produktoch a službách IKT dosiahnu, by sa potom mali podrobnejšie vymedziť na úrovni príslušného systému certifikácie, ktorý prijme Komisia – napríklad s odvolaním sa na normy alebo technické špecifikácie, **ak vhodné normy nie sú k dispozícii.**

(55a) Technické špecifikácie, ktoré sa majú použiť v európskom systéme certifikácie kybernetickej bezpečnosti, by sa mali určiť dodržaním zásad stanovených v prílohe II k nariadeniu (EÚ) 1025/2012. Niektoré odchýlky od týchto zásad by sa však mohli považovať za potrebné v riadne odôvodnených prípadoch, ak sa tieto technické špecifikácie majú využívať v európskom systéme certifikácie kybernetickej bezpečnosti, ktorý sa vzťahuje na vysoký stupeň dôveryhodnosti. Dôvody týchto odchýlok sa musia uverejniť.

(55b) Certifikované posúdenie zhody je proces hodnotenia, či boli uvedené požiadavky týkajúce sa procesu, produktu alebo služby IKT splnené. Tento proces vykonáva nezávislý tretí subjekt, iný ako výrobca produktu alebo poskytovateľ služieb. Postup vydávania certifikátu nasleduje po postupe úspešného vyhodnotenia procesu, produktu alebo služby IKT. Mal by sa považovať za potvrdenie, že príslušné hodnotenie bolo vykonané správne. V závislosti od stupňa dôveryhodnosti by mal európsky systém kybernetickej bezpečnosti uvádzať, či certifikát vydal súkromný alebo verejný subjekt. Posúdenie zhody a certifikácia sama osebe nemôže zaručiť, že certifikované produkty a služby IKT sú kyberneticky bezpečné. Ide skôr o postup a technickú metodiku na potvrdenie toho, že produkty a služby IKT boli preskúšané a spĺňajú určité kyberneticko-bezpečnostné požiadavky stanovené inde, napríklad v technických normách.

(55c) Výber vhodného stupňa certifikácie a súvisiacich bezpečnostných požiadaviek zo strany používateľov, by mal byť založený na analýze rizika pri používaní procesu, produktu alebo služby IKT. Stupeň dôveryhodnosti by mal preto zodpovedať úrovni rizika spojeného s plánovaným využitím daného procesu, produktu alebo služby IKT.

(55d) Európsky systém certifikácie kybernetickej bezpečnosti by mohol dovoľovať, aby sa posúdenie zhody vykonalo na výhradnú zodpovednosť výrobcu alebo poskytovateľa produktov a služieb IKT (vlastné posúdenie zhody). V takýchto prípadoch stačí, aby výrobca alebo dodávateľ vykonal všetky kontroly sám s cieľom overiť zhodu procesov, produktov alebo služieb IKT so systémom certifikácie. Tento druh posudzovania zhody by sa mal považovať za vhodný pre menej zložité produkty a služby IKT (jednoduchý dizajn a produkčný mechanizmus), ktoré predstavujú nízke riziko pre verejný záujem. Okrem toho by sa predmetom vlastného posúdenia mohli stať len produkty a služby IKT, ktoré zodpovedajú základnému stupňu dôveryhodnosti.

(55e) Európsky systém certifikácie kybernetickej bezpečnosti by mohol umožňovať certifikáciu aj vlastné posúdenie zhody produktov a služieb IKT. V takomto prípade by systém mal stanoviť jasné a zrozumiteľné prostriedky pre spotrebiteľov alebo iných používateľov na rozlíšenie medzi produktmi a službami, ktoré sa posúdili na zodpovednosť výrobcu alebo poskytovateľa, a produktmi a službami, ktoré sú certifikované treťou stranou.

(55f) Výrobca alebo poskytovateľom produktov a služieb IKT, ktorý vykonáva vlastné posúdenie zhody, by mal v rámci procesu posudzovania zhody vypracovať a podpísať vyhlásenie o zhode EÚ. Vyhlásenie o zhode EÚ je dokument, v ktorom sa uvádza, že daný produkt alebo služba IKT spĺňajú požiadavky systému. Výrobca alebo poskytovateľ vypracovaním a podpisom vyhlásenie o zhode EÚ preberá zodpovednosť za súlad produktu alebo služby IKT s právnymi požiadavkami systému. Kópia vyhlásenia o zhode EÚ by sa mala predložiť vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti a agentúre ENISA.

(55g) Výrobca alebo poskytovateľ produktov a služieb IKT by mal ponechať vyhlásenie o zhode EÚ a technickú dokumentáciu všetkých relevantných informácií týkajúcich sa zhody produktov alebo služieb IKT so systémom k dispozícii príslušnému vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti počas obdobia vymedzeného v príslušnom európskom systéme certifikácie kybernetickej bezpečnosti. V technickej dokumentácii sa uvedú uplatniteľné požiadavky, a ak je to relevantné z hľadiska posúdenia, zahrnie sa do nej návrh, výroba a používanie produktu alebo služby IKT. Technická dokumentácia by mala byť zostavená tak, aby sa umožnilo posúdenie súladu produktu alebo služby IKT s príslušnými požiadavkami.

(55h) Členské štáty a organizácie zainteresovaných strán, ktoré o to prejavia záujem, by mali byť oprávnení navrhovať európskej skupine pre certifikáciu kybernetickej bezpečnosti vypracovanie kandidátskych systémov. Organizácie zainteresovaných strán sú zástupcovia priemyslu alebo spotrebiteľov vrátane zástupcov organizácií MSP, ktorí majú legitímny záujem o rozvoj konkrétneho európskeho systému certifikácie kybernetickej bezpečnosti. Tieto návrhy by sa mali preskúmať z hľadiska kritérií vypracovaných európskou skupinou pre certifikáciu kybernetickej bezpečnosti na základe usmernení založených na zásadách transparentnosti, otvorenosti, nestrannosti, konsenzu, efektívnosti, relevantnosti a súdržnosti.

(56) Komisia a **skupina** by mali byť splnomocnené požiadať agentúru ENISA o **bezodkladnú** prípravu kandidátskych systémov pre konkrétne **procesy**, produkty alebo služby IKT. Následne by Komisia mala byť splnomocnená na základe kandidátskeho systému navrhnutého agentúrou ENISA prijať európsky systém certifikácie kybernetickej bezpečnosti v podobe vykonávacích aktov. Zohľadňujúc všeobecný účel a bezpečnostné ciele identifikované v tomto nariadení, európske systémy certifikácie kybernetickej bezpečnosti prijaté Komisiou by mali zahŕňať minimálny súbor prvkov, ktoré sa vzťahujú na danú problematiku, ako aj rozsah a fungovanie daného systému. Okrem iného by sem mal patriť rozsah a predmet certifikácie kybernetickej bezpečnosti vrátane kategórií pokrytých **procesov**, produktov a služieb IKT, podrobného vymedzenia kybernetickobezpečnostných požiadaviek (napríklad s odvolaním na normy alebo technické špecifikácie), konkrétne hodnotiace kritériá a metódy, ako aj cieľový stupeň dôveryhodnosti: základný, pokročilý a/alebo vysoký a **prípadné stupne hodnotenia.**

(56a) Dôveryhodnosť európskeho systému certifikácie je dôvod na presvedčenie, že proces, produkt alebo služba IKT spĺňajú bezpečnostné požiadavky konkrétneho európskeho systému certifikácie kybernetickej bezpečnosti. S cieľom zabezpečiť konzistentnosť rámca pre certifikované procesy, produkty a služby IKT by európsky systém certifikácie kybernetickej bezpečnosti mohol špecifikovať stupne dôveryhodnosti pre európske certifikáty kybernetickej bezpečnosti a vyhlásenie o zhode EÚ vydané v rámci daného systému. V každom certifikáte by sa mohlo odkazovať na jeden zo stupňov dôveryhodnosti: základný, pokročilý a vysoký, pričom vyhlásenie o zhode EÚ by mohlo odkazovať len na základný stupeň dôveryhodnosti. Stupňami dôveryhodnosti sa zabezpečuje zodpovedajúca úroveň úsilia o vyhodnotenie [...] a sú charakterizované odkazom na súvisiace technické špecifikácie, normy a postupy, ktorých účelom je predchádzať kybernetickým bezpečnostným incidentom alebo zmierňovať ich následky. Každý stupeň dôveryhodnosti by mali byť konzistentný medzi jednotlivými sektorovými oblasťami, v ktorých sa uplatňuje certifikácia.

(56b) Európsky systém certifikácie kybernetickej bezpečnosti môže špecifikovať niekoľko stupňov hodnotenia v závislosti od prísnosti a hĺbky použitej metodiky hodnotenia, ktoré by mali zodpovedať jednému zo stupňov dôveryhodnosti a mali by byť spojené s vhodnou kombináciou zložiek dôveryhodnosti. Pre všetky stupne dôveryhodnosti by produkt alebo služba IKT mali obsahovať niekoľko zabezpečených funkcií vymedzených v systéme, čo môže zahŕňať: konfiguráciu zabezpečenia na priame použitie, podpísaný programovací kód, zabezpečenú aktualizáciu a zmierňovanie následkov zneužitia bezpečnostných dier (exploits) a plnú ochranu dynamicky a staticky prideľovanej pamäte (stack/heap). Tieto funkcie by sa mali vyvinúť a potom udržiavať vývojovým prístupom zameraným na bezpečnosť a súvisiacimi nástrojmi s cieľom zaručiť spoľahlivé zapracovanie účinných mechanizmov (softvérových aj hardvérových). Pri základnom stupni dôveryhodnosti by sa hodnotenie malo riadiť aspoň zložkami dôveryhodnosti: hodnotenie by malo zahŕňať aspoň preskúmanie technickej dokumentácie k produktu alebo službe IKT orgánom posudzovania zhody. Ak certifikácia zahŕňa procesy IKT, technické preskúmanie by sa malo vzťahovať aj na proces navrhnutia, vývoja a údržby produktu alebo služby IKT. Ak európsky systém certifikácie kybernetickej bezpečnosti stanovuje vlastné posúdenie zhody, malo by stačiť, ak výrobca alebo poskytovateľ vykonal vlastné posúdenie súladu procesov, produktov alebo služieb IKT s certifikačným systémom. Pri pokročilom stupni dôveryhodnosti by sa hodnotenie malo okrem požiadaviek základného stupňa dôveryhodnosti riadiť aspoň overením súladu bezpečnostných funkcií produktu alebo služby IKT s ich technickou dokumentáciou. Pri vysokom stupni dôveryhodnosti by sa hodnotenie malo okrem požiadaviek pokročilého stupňa dôveryhodnosti riadiť aspoň skúškou účinnosti, ktorou sa posúdi odolnosť bezpečnostných funkcií produktu alebo služby IKT proti tým, ktorí vedú prepracované kybernetické útoky a majú významné zručnosti a zdroje.

(56c) Pri príprave kandidátskeho systému by agentúra ENISA mala konzultovať so všetkými príslušnými zainteresovanými stranami, ako sú napríklad európske normalizačné organizácie, príslušné vnútroštátne orgány, organizácie založené na dohodách o vzájomnom uznávaní, ako napríklad SOG-IS DVU, MSP, spotrebiteľské organizácie, ako aj environmentálne a sociálne zainteresované strany.

(56d) Agentúra ENISA by mala udržiavať webovú stránku, ktorá bude poskytovať informácie o európskych systémoch certifikácie kybernetickej bezpečnosti a propagovať ich, pričom jej súčasťou by okrem iného mali byť požiadavky na prípravu kandidátskych európskych systémov certifikácie kybernetickej bezpečnosti, ako aj spätná väzba v rámci procesu konzultácií, ktorý uskutočňuje agentúra ENISA v prípravnej fáze. Takáto webová stránka by mala poskytovať aj informácie o certifikátoch a vyhláseniach o zhode EÚ vydávaných podľa tohto nariadenia.

(57) Využívanie európskej certifikácie kybernetickej bezpečnosti a **vyhlásení o zhode EÚ** by malo byť naďalej dobrovoľné, pokiaľ sa nestanovuje inak v právnych predpisoch Únie alebo vo vnútroštátnych právnych predpisoch **prijatých v súlade s právom Únie. Ak neexistujú harmonizované právne predpisy, členské štáty môžu v súlade so smernicou (EÚ) 2015/1535 prijať vnútroštátne technické predpisy, ktorými stanovia povinnú certifikáciu európskym systémom certifikácie kybernetickej bezpečnosti. Členské štáty by mohli využívať európsku certifikáciu kybernetickej bezpečnosti aj v súvislosti s verejným obstarávaním a so smernicou 2014/214/EÚ** [...].

(57a) Aby sa dosiahli ciele tohto nariadenia a aby sa predišlo fragmentácii vnútorného trhu, vnútroštátne systémy alebo postupy certifikácie kybernetickej bezpečnosti produktov a služieb IKT, na ktoré sa vzťahuje európsky systém certifikácie kybernetickej bezpečnosti, by mali stratiť účinky od dátumu, ktorý stanoví Komisia vo vykonávacom akte. Okrem toho by členské štáty nemali zavádzať nové vnútroštátne systémy certifikácie kybernetickej bezpečnosti v prípade produktov a služieb IKT, pre ktoré už existuje európsky systém certifikácie kybernetickej bezpečnosti. Členským štátom by sa však nemalo brániť vytvárať alebo zachovať vnútroštátne systémy certifikácie na účely národnej bezpečnosti.

(58) Po prijatí určitého európskeho systému certifikácie kybernetickej bezpečnosti by mali výrobcovia produktov alebo poskytovatelia služieb IKT môcť požiadať o certifikáciu svojich produktov alebo služieb ktorýmkoľvek orgánom posudzovania zhody, ktorý si zvolia. Orgány posudzovania zhody by mal akreditovať akreditačný orgán, ak spĺňajú určité požiadavky stanovené v tomto nariadení. Akreditácia by sa mala vydávať najviac na päť rokov, pričom ju možno obnoviť za rovnakých podmienok, pokiaľ orgán posudzovania zhody spĺňa požiadavky. Akreditačné orgány by mali orgánu posudzovania zhody akreditáciu **obmedziť, pozastaviť alebo** odňať, ak nie sú alebo prestanú byť splnené akreditačné podmienky, alebo ak kroky daného orgánu posudzovania zhody porušujú toto nariadenie.

(59) **[...]** Členské štáty **[...] by mali** určiť jeden **alebo viacero** orgánov pre certifikáciu kybernetickej bezpečnosti na účely dohľadu nad plnením **povinností vyplývajúcich z tohto nariadenia. Ak to členský štát považuje za vhodné, môže takýmito úlohami poveriť aj už existujúce orgány. Členské štáty by tiež mali mať možnosť rozhodnúť po vzájomnej dohode s iným členským štátom, že určia jeden alebo viacero orgánov dohľadu na území takéhoto iného členského štátu. Tento orgán by mal najmä monitorovať a presadzovať plnenie povinností výrobcu alebo poskytovateľa produktov a služieb IKT usadeného na jeho príslušných územiach vo vzťahu k vyhláseniu o zhode EÚ, pomáhať vnútroštátnym akreditačným orgánom pri monitorovaní činnosti orgánov posudzovania zhody a dohľadu nad nimi tým, že pre ne zabezpečí odborné znalosti a relevantné informácie, oprávňovať orgány posudzovania zhody vykonávať jeho úlohy, ak spĺňajú dodatočné požiadavky stanovené v systéme a monitorovať relevantný vývoj v oblasti certifikácie kybernetickej bezpečnosti** [...]. Vnútroštátne orgány pre certifikáciu [...] kybernetickej bezpečnosti by mali vybavovať sťažnosti fyzických alebo právnických osôb v súvislosti s certifikátmi, **ktoré vydali, alebo certifikátmi, ktoré vydali orgány posudzovania zhody, pokiaľ ide o vysoký stupeň dôveryhodnosti** [...], primerane prešetriť predmet danej sťažnosti a sťažovateľa v primeranej lehote informovať o pokroku a výsledku tohto prešetrenia. Okrem toho by mali spolupracovať s ostatnými vnútroštátnymi orgánmi pre certifikáciu **kybernetickej bezpečnosti** [...] alebo ďalšími verejnými orgánmi vrátane poskytovania informácií o možnom nesúlade produktov a služieb IKT s požiadavkami tohto nariadenia alebo konkrétnych kyberneticko-bezpečnostných systémov.

(60) V záujme konzistentného uplatňovania európskeho rámca certifikácie kybernetickej bezpečnosti by sa mala zriadiť európska skupina pre certifikáciu kybernetickej bezpečnosti (ďalej len „skupina“) zložená zo **zástupcov** vnútroštátnych [...] orgánov pre certifikáciu **kybernetickej bezpečnosti alebo iných príslušných vnútroštátnych orgánov.** Medzi hlavné úlohy tejto skupiny by mali patriť poradenstvo a pomoc Komisii v jej úsilí o zaistenie konzistentného vykonávania a uplatňovania európskeho rámca certifikácie kybernetickej bezpečnosti; pomoc agentúre a úzka spolupráca s ňou pri príprave kandidátskych systémov certifikácie kybernetickej bezpečnosti; odporúčania, na základe ktorých Komisia žiada agentúru o vypracovanie kandidátskeho európskeho systému certifikácie kybernetickej bezpečnosti; a prijímanie stanovísk pre **agentúru, pokiaľ ide o kandidátske systémy**, a pre Komisiu k udržiavaniu a prehodnocovaniu existujúcich európskych systémov certifikácie kybernetickej bezpečnosti.

(60a) Skupina by mala uľahčovať výmenu osvedčených postupov a odborných znalostí medzi vnútroštátnymi orgánmi pre certifikáciu kybernetickej bezpečnosti zodpovednými za oprávňovanie orgánov posudzovania zhody a vydávanie osvedčení. Skupina by mala podporovať zriadenie mechanizmu partnerského preskúmania v súvislosti s prípravou kandidátskeho systému a jeho využívanie pre orgány vydávajúce európske certifikáty kybernetickej bezpečnosti pre vysoký stupeň dôveryhodnosti. Takýmito partnerskými preskúmaniami by sa malo najmä posudzovať, či majú dotknuté orgány primerané odborné znalosti a či vykonávajú svoje úlohy harmonizovane. Výsledky partnerských preskúmaní by sa mali uverejniť. Uvedené orgány môžu prijať vhodné opatrenia na prispôsobenie svojich postupov a odborných znalostí.

(61) Na zvýšenie povedomia a uľahčenie akceptácie budúcich únijných systémov certifikácie kybernetickej bezpečnosti môže Európska komisia vydať všeobecné či odvetvové usmernenia o kybernetickej bezpečnosti – napríklad o osvedčených postupoch a zodpovednom správaní sa v tejto oblasti, pričom sa zdôrazní pozitívny účinok využívania certifikovaných produktov a služieb IKT.

(61a) S cieľom ďalej uľahčovať obchod a uznávajúc, že dodávateľské reťazce IKT sú globálne, môže Únia v súlade s článkom 218 ZFEÚ uzatvárať dohody o vzájomnom uznávaní týkajúce sa certifikátov vydaných systémami zriadenými na základe európskeho rámca certifikácie kybernetickej bezpečnosti. Komisia môže s prihliadnutím na poradenstvo od agentúry ENISA a európskej skupiny pre certifikáciu kybernetickej bezpečnosti odporučiť začatie príslušných rokovaní. V rámci každého systému by sa mali stanoviť konkrétne podmienky vzájomného uznávania s tretími krajinami.

(62) [...]

(63) [...]

(64) S cieľom zabezpečiť jednotné podmienky vykonávania tohto nariadenia by sa v prípadoch stanovených v tomto nariadení mali na Komisiu preniesť vykonávacie právomoci. Tieto právomoci by sa mali vykonávať v súlade s nariadením (EÚ) č. 182/2011.

(65) Postup preskúmania by sa mal uplatniť pri prijímaní vykonávacích aktov o európskych systémoch certifikácie kybernetickej bezpečnosti produktov a služieb IKT, o modalitách [...] **skúmania** zo strany agentúry, ako aj o okolnostiach, formátoch a postupoch, na základe ktorých majú vnútroštátne orgány pre certifikáciu **kybernetickej bezpečnosti** [...] Komisii oznamovať akreditované orgány posudzovania zhody.

(66) Činnosť agentúry by sa mala vyhodnocovať nezávisle. V rámci toho by sa malo posúdiť napĺňanie cieľov agentúry, jej pracovné postupy a relevantnosť jej úloh. Zároveň by sa v hodnotení mal posúdiť dosah, efektívnosť a účinnosť európskeho rámca certifikácie kybernetickej bezpečnosti.

(67) Nariadenie (EÚ) č. 526/2013 by sa malo zrušiť.

(68) Keďže ciele tohto nariadenia nemožno uspokojivo dosiahnuť na úrovni jednotlivých členských štátov, ale možno ich lepšie dosiahnuť na úrovni Únie, môže Únia prijať opatrenia v súlade so zásadou subsidiarity podľa článku 5 Zmluvy o Európskej únii. V súlade so zásadou proporcionality podľa uvedeného článku toto nariadenie neprekračuje rámec nevyhnutný na dosiahnutie tohto cieľa,

PRIJALI TOTO NARIADENIE:

HLAVA I
VŠEOBECNÉ USTANOVENIA

Článok 1

Predmet úpravy a rozsah pôsobnosti

1. S cieľom zaistiť riadne fungovanie vnútorného trhu pri vysokej úrovni kybernetickej bezpečnosti, odolnosti a dôvery v rámci Únie sa v tomto nariadení:

a) stanovujú ciele, úlohy a organizačné aspekty agentúry ENISA – [...] Agentúry **Európskej únie** pre **kybernetickú bezpečnosť** (ďalej len „agentúra“); a

b) stanovuje rámec vytvorenia európskych systémov certifikácie kybernetickej bezpečnosti na zaistenie primeranej úrovne kybernetickej bezpečnosti **procesov**, produktov a služieb IKT v Únii. Uplatňovaním tohto rámca nie sú dotknuté osobitné ustanovenia o dobrovoľnej či povinnej certifikácii podľa iných aktov Únie.

2. **Týmto nariadením nie sú dotknuté právomoci členských štátov v oblasti kybernetickej bezpečnosti a v žiadnom prípade na činnosti spojené s verejnou bezpečnosťou, obranou, národnou bezpečnosťou a na činnosti štátu v oblasti trestného práva.**

Článok 2

Vymedzenie pojmov

Na účely tohto nariadenia sa uplatňuje toto vymedzenie pojmov:

1) „kybernetická bezpečnosť“ zahŕňa všetky činnosti potrebné na ochranu sietí a informačných systémov, ich používateľov a dotknutých osôb pred kybernetickými hrozbami;

2) „sieť a informačný systém“ je systém v zmysle článku 4 bode 1 smernice (EÚ) 2016/1148;

3) „národná stratégia v oblasti bezpečnosti sietí a informačných systémov“ je rámec v zmysle článku 4 bode 3 smernice (EÚ) 2016/1148;

4) „prevádzkovateľ základných služieb“ je verejný alebo súkromný subjekt vymedzený v článku 4 bode 4 smernice (EÚ) 2016/1148;

5) „poskytovateľ digitálnych služieb“ je každá právnická osoba, ktorá poskytuje digitálnu službu, vymedzená v článku 4 bode 6 smernice (EÚ) 2016/1148;

6) „incident“ je každá udalosť vymedzená v článku 4 bode 7 smernice (EÚ) 2016/1148;

7) „riešenie incidentov“ je každý postup vymedzený v článku 4 bode 8 smernice (EÚ) 2016/1148;

8) „kybernetická hrozba“ je každá potenciálna okolnosť alebo udalosť, ktorá môže **poškodiť, narušiť alebo inak** negatívne ovplyvniť siete a informačné systémy, ich používateľov a dotknuté osoby;

9) „európsky systém certifikácie kybernetickej bezpečnosti“ je komplexný súbor pravidiel, technických požiadaviek, noriem a postupov vymedzený na úrovni Únie, ktorý sa uplatňuje na certifikáciu **alebo posúdenie zhody procesov**, produktov a služieb informačných a komunikačných technológií (ďalej len „IKT“) spadajúcich do rozsahu pôsobnosti príslušného systému;

9a) „vnútroštátny systém certifikácie kybernetickej bezpečnosti“ je komplexný súbor pravidiel, technických požiadaviek, noriem a postupov, ktorý vypracuje a prijme vnútroštátny orgán verejnej moci vo vzťahu k certifikácii alebo posudzovaniu zhody procesov, produktov a služieb IKT, na ktoré sa vzťahuje rozsah pôsobnosti daného konkrétneho systému;

10) „európsky certifikát kybernetickej bezpečnosti“ je dokument, ktorým sa [...] potvrdzuje, že daný proces, produkt alebo služba [...] IKT **bol vyhodnotený z hľadiska súladu s** konkrétnymi **bezpečnostnými** požiadavkami stanovenými v určitom európskom systéme certifikácie kybernetickej bezpečnosti;

11) „produkt IKT [...]“ je každý prvok alebo skupina prvkov sietí a informačných systémov;

11a) „služba IKT“ je akákoľvek služba pozostávajúca úplne alebo prevažne z prenosu, ukladania, získavania alebo spracovania informácií prostredníctvom sietí a informačných systémov;

11b) „proces IKT“ je akýkoľvek súbor činností vykonávaných s cieľom navrhovať, vyvíjať, poskytovať a udržiavať produkt alebo službu IKT;

12) „akreditácia“ je akreditácia vymedzená v článku 2 bode 10 nariadenia (ES) č. 765/2008;

13) „vnútroštátny akreditačný orgán“ je vnútroštátny akreditačný orgán vymedzený v článku 2 bode 11 nariadenia (ES) č. 765/2008;

14) „posudzovanie zhody“ je posudzovanie zhody vymedzené v článku 2 bode 12 nariadenia (ES) č. 765/2008;

15) „orgán posudzovania zhody“ je orgán posudzovania zhody vymedzený v článku 2 bode 13 nariadenia (ES) č. 765/2008;

16) „norma“ je norma vymedzená v článku 2 bode 1 nariadenia (EÚ) č. 1025/2012;

16a) „technická špecifikácia“ je dokument, v ktorom sa predpisujú technické požiadavky, ktoré musí spĺňať proces, produkt alebo služba IKT;

16b) „stupeň dôveryhodnosti“ je dôvod na presvedčenie, že proces, produkt alebo služba IKT spĺňajú bezpečnostné požiadavky konkrétneho európskeho systému certifikácie kybernetickej bezpečnosti, a obsahuje informáciu, na akej úrovni sa vyhodnotil; stupňom dôveryhodnosti sa nemeria bezpečnosť procesu, produktu alebo služby IKT samotnej.

HLAVA II

Agentúra ENISA – Agentúra [...] Európskej únie pre kybernetickú bezpečnosť

KAPITOLA I

MANDÁT A CIELE *[...]*

Článok 3

Mandát

1. Agentúra plní úlohy, ktoré jej ukladá toto nariadenie, s cieľom prispieť k vysokej úrovni kybernetickej bezpečnosti v [...] **celej** Únii **najmä tým, že podporuje členské štáty a inštitúcie, agentúry a orgány Únie pri zvyšovaní kybernetickej bezpečnosti. Agentúra pôsobí ako referenčný bod pre poradenstvo a odborné znalosti o kybernetickej bezpečnosti pre inštitúcie, agentúry a orgány Únie.**

2. Agentúra plní úlohy zverené aktmi Únie, v ktorých sa stanovujú opatrenia na aproximáciu zákonov, iných právnych predpisov a správnych opatrení členských štátov v oblasti kybernetickej bezpečnosti.

2a. Pri plnení úloh agentúra koná nezávisle a v čo najväčšej miere zohľadňuje vnútroštátne odborné znalosti príslušných úradov členských štátov, pričom predchádza zdvojovaniu činností.

3. [...]

Článok 4

Ciele

1. Agentúra pôsobí ako stredisko odborných poznatkov o kybernetickej bezpečnosti, pretože sa vyznačuje nezávislosťou, vedeckou a technickou kvalitou poskytovaného poradenstva, pomoci a šírených informácií, transparentnosťou svojich prevádzkových postupov a pracovných metód a dôslednosťou pri vykonávaní svojich úloh.

2. Agentúra pomáha inštitúciám, agentúram a orgánom Únie, ako aj členským štátom pri príprave a vykonávaní politík **Únie** súvisiacich s kybernetickou bezpečnosťou **vrátane odvetvových politík v oblasti kybernetickej bezpečnosti.**

3. Agentúra podporuje budovanie kapacít a pripravenosť v celej Únii tým, že inštitúciám, agentúram a orgánom Únie, ako aj členským štátom a verejným a súkromným zainteresovaným stranám pomáha pri zvyšovaní ochrany ich sietí a informačných systémov, **rozvoji a zlepšovaní kybernetickej odolnosti a kapacít reakcie a rozvoji** zručností a spôsobilostí v oblasti kybernetickej bezpečnosti [...].

4. Agentúra na úrovni Únie presadzuje spoluprácu a koordináciu členských štátov, inštitúcií, agentúr a orgánov Únie, ako aj relevantných **verejných a súkromných** zainteresovaných strán [...] v otázkach kybernetickej bezpečnosti.

5. Agentúra **prispieva k posilňovaniu** spôsobilostí v oblasti kybernetickej bezpečnosti na úrovni Únie s cieľom [...] **pomáhať** členským štátom pri prevencii kybernetických hrozieb a reakcii na ne, najmä pri cezhraničných incidentoch.

6. Agentúra podporuje používanie certifikácie s **cieľom predchádzať roztrieštenosti systémov certifikácie v EÚ. Agentúra konkrétne prispieva** [...] k vytvoreniu a údržbe rámca certifikácie kybernetickej bezpečnosti na úrovni Únie v súlade s hlavou III tohto nariadenia, aby sa posilnila transparentnosť uistenia o dôveryhodnosti kybernetickej bezpečnosti produktov a služieb IKT, čím sa posilní dôvera v digitálny vnútorný trh.

7. Agentúra presadzuje vysoké povedomie občanov a podnikov o otázkach kybernetickej bezpečnosti.

KAPITOLA IA

ÚLOHY

Článok 5

*[...] **Tvorba a vykonávanie politiky a legislatívy Únie***

Agentúra prispieva k tvorbe a vykonávaniu politiky a legislatívy Únie tým, že:

1. pomáha a radí, najmä poskytuje nezávislé stanoviská a zabezpečuje prípravné práce k vypracovaniu a preskúmaniu politiky a legislatívy Únie v oblasti kybernetickej bezpečnosti, ale i odvetvových politík a legislatívnych iniciatív, ktoré rozmer kybernetickej bezpečnosti zahŕňajú;

2. pomáha členským štátom pri konzistentnom vykonávaní politiky a legislatívy Únie v oblasti kybernetickej bezpečnosti, najmä v súvislosti so smernicou (EÚ) 2016/1148, a to aj poskytovaním stanovísk, usmernení, poradenstva a osvedčených postupov v oblastiach ako riadenie rizík, oznamovanie incidentov a zdieľanie informácií, a zároveň v tomto smere uľahčuje výmenu informácií o osvedčených postupoch medzi príslušnými orgánmi;

3. prispieva k práci skupiny pre spoluprácu v zmysle článku 11 smernice (EÚ) 2016/1148 v podobe odborných poznatkov a poradenstva;

4. podporuje:

   1) tvorbu a vykonávanie politiky Únie v oblasti elektronickej identifikácie a dôveryhodných služieb, najmä formou poradenstva a technických usmernení, ako aj uľahčovaním výmeny osvedčených postupov medzi príslušnými orgánmi;

   2) presadzovanie zvýšenej úrovne bezpečnosti elektronických komunikácií, a to aj formou odborných poznatkov a poradenstva, ako aj uľahčovaním výmeny osvedčených postupov medzi príslušnými orgánmi;

5. podporuje pravidelné preskúmanie politickej činnosti Únie poskytovaním výročnej správy o stave vykonávania príslušného právneho rámca z hľadiska:

   a) oznámení členských štátov o incidentoch, ktoré podľa článku 10 ods. 3 smernice (EÚ) 2016/1148 skupine pre spoluprácu poskytujú jednotné kontaktné miesta;

   b) oznámení o narušeniach bezpečnosti a integrity u poskytovateľov dôveryhodných služieb, ktoré agentúre poskytujú orgány dohľadu podľa článku 19 ods. 3 nariadenia (EÚ) 910/2014;

   c) oznámení o [...] bezpečnostných **incidentoch**, ktoré podávajú podniky poskytujúce verejné komunikačné siete alebo verejne dostupné elektronické komunikačné služby a ktoré agentúre postupujú príslušné orgány podľa článku 40 [smernice, ktorou sa stanovuje európsky kódex elektronickej komunikácie].

Článok 6

[...] ***Budovanie kapacít***

1. Agentúra pomáha:

a) členským štátom v ich úsilí zlepšovať prevenciu, odhaľovanie a analýzu kybernetických [...] **hrozieb** [...] a incidentov a schopnosť na ne reagovať vrátane poskytovania potrebných vedomostí a odborných poznatkov;

b) inštitúciám, agentúram a **orgánom** Únie v ich úsilí zlepšovať prevenciu, odhaľovanie a analýzu kybernetických [...] **hrozieb** [...] a incidentov a schopnosť na ne reagovať, a to **najmä** primeranou podporou tímu reakcie na núdzové počítačové situácie v európskych inštitúciách, orgánoch a agentúrach („tím CERT-EU“);

c) členským štátom na požiadanie pri tvorbe vnútroštátnych jednotiek pre riešenie počítačových bezpečnostných incidentov (ďalej len „jednotky CSIRT“) podľa článku 9 ods. 5 smernice (EÚ) 2016/1148;

d) členským štátom na požiadanie pri vypracúvaní národných stratégií v oblasti bezpečnosti sietí a informačných systémov podľa článku 7 ods. 2 smernice (EÚ) 2016/1148; v záujme propagácie osvedčených postupov agentúra zároveň podporuje šírenie týchto stratégií v Únii a **[...] sleduje** ich vykonávanie;

e) inštitúciám Únie pri príprave a revízii kyberneticko-bezpečnostných stratégií Únie, podpore ich šírenia a monitorovaní pokroku v ich vykonávaní;

f) jednotkám CSIRT členských štátov a Únie pri zdokonaľovaní ich spôsobilostí, a to i presadzovaním dialógu a výmeny informácií s cieľom zabezpečiť, aby sa s ohľadom na aktuálny stupeň vývoja každá jednotka CSIRT vyznačovala spoločným súborom minimálnych spôsobilostí a aby fungovala v súlade s osvedčenými postupmi;

g) členským štátom organizáciou **pravidelných** [...] kyberneticko-bezpečnostných cvičení na úrovni Únie v zmysle článku 7 ods. 6 a formulovaním politických odporúčaní na základe hodnotenia týchto cvičení a takto získaných poznatkov;

h) relevantným verejným orgánom poskytovaním školení v oblasti kybernetickej bezpečnosti, podľa potreby v spolupráci so zainteresovanými stranami;

i) skupine pre spoluprácu **pri** [...] výmene [...] osvedčených postupov v zmysle článku 11 ods. 3 písm. l) smernice (EÚ) 2016/1148, najmä z hľadiska identifikácie prevádzkovateľov základných služieb členskými štátmi, pokiaľ ide o riziká a incidenty, a to aj v súvislosti s cezhraničnou previazanosťou.

2. Agentúra podporuje **výmenu informácií v odvetviach a medzi nimi** [...], a to najmä v odvetviach uvedených v prílohe II k smernici (EÚ) 2016/1148, poskytovaním osvedčených postupov a usmernení o dostupných nástrojoch, postupoch i riešeniach regulačných otázok spojených s výmenou informácií.

Článok 7

*[...] **Úlohy spojené s operačnou spoluprácou na úrovni Únie***

1. Agentúra podporuje operačnú spoluprácu medzi **členskými štátmi, inštitúciami, agentúrami a** [...] orgánmi Únie a medzi zainteresovanými stranami.

2. Agentúra na operačnej úrovni spolupracuje a vytvára synergie s inštitúciami, agentúrami a **orgánmi** [...] Únie vrátane tímu CERT-EU, útvarov, ktoré sa zaoberajú počítačovou kriminalitou, a orgánov dohľadu zodpovedných za ochranu súkromia a osobných údajov, na účely riešenia otázok spoločného záujmu, a to aj:

a) výmenou know-how a osvedčených postupov;

b) poskytovaním poradenstva a usmernení k otázkam spojeným s kybernetickou bezpečnosťou;

c) zavedením praktických opatrení na výkon konkrétnych úloh po konzultácii s Komisiou.

3. Agentúra zabezpečuje sekretariát siete jednotiek CSIRT podľa článku 12 ods. 2 smernice (EÚ) 2016/1148 a **týmto** [...] podporuje výmenu informácií a spoluprácu jej členov.

4. Agentúra **podporuje** [...] operačnú spoluprácu v rámci siete jednotiek CSIRT podporou členských štátov tak, že na **ich žiadosť**:

a) im radí, ako zdokonaliť spôsobilosť predchádzať incidentom, odhaľovať ich a reagovať na ne;

b) [...] **uľahčuje technické riešenie** [...] incidentov, ktoré majú významný alebo závažný vplyv, a **to najmä podporou dobrovoľnej výmeny technických riešení medzi členskými štátmi;**

c) analyzuje zraniteľné miesta [...] a incidenty;

ca) poskytuje podporu ex post technickému skúmaniu incidentov, ktoré majú významný alebo závažný vplyv, v súlade so smernicou (EÚ) 2016/1148.

Pri výkone týchto úloh agentúra a tím CERT-EU štruktúrovane spolupracujú s cieľom využiť synergie a **predchádzať zdvojovaniu činností** [...].

5. [...]

[...]

6. Agentúra **pravidelne** [...] organizuje kyberneticko-bezpečnostné cvičenia na úrovni Únie a na požiadanie podporuje členské štáty a inštitúcie, agentúry a orgány EÚ pri organizácií ich cvičení. **Súčasťou takýchto cvičení na úrovni Únie môžu byť technické, operačné alebo strategické prvky** [...]. **Raz za dva roky sa zorganizuje rozsiahle cvičenie, ktoré bude obsahovať všetky tieto prvky.** Agentúra zároveň prispieva a podľa potreby pomáha organizovať odvetvové kyberneticko-bezpečnostné cvičenia spolu s relevantnými [...] **organizáciami, ktoré sa môžu** zúčastňovať aj na kyberneticko-bezpečnostných cvičeniach na úrovni [...] Únie.

7. Agentúra vypracúva v **úzkej spolupráci s členskými štátmi** pravidelnú technickú situačnú správu EÚ o kybernetických incidentoch a hrozbách, ktorá vychádza z verejne dostupných informácií, jej vlastných analýz a správ, ktoré okrem iných poskytli: jednotky CSIRT členských štátov [...] alebo jednotné kontaktné miesta podľa smernice NIS (**v oboch prípadoch na dobrovoľnom základe** [...]), Európske centrum boja proti počítačovej kriminalite (EC3) pri Europole a tím CERT-EU.

8. Agentúra prispieva k vypracovaniu spoločnej reakcie (na úrovni Únie i na úrovni členských štátov) na rozsiahle cezhraničné incidenty alebo krízy v oblasti kybernetickej bezpečnosti, a to najmä:

   a) zhromažďovaním **dobrovoľne zdieľaných** správ z národných zdrojov s cieľom prispieť k vytvoreniu spoločného situačného povedomia;

   b) zaistením efektívneho toku informácií a zabezpečením eskalačných mechanizmov medzi sieťou jednotiek CSIRT a subjektmi zodpovednými za technické a politické rozhodnutia na úrovni Únie;

c) [...] **uľahčovaním** technického riešenia incidentov alebo kríz na **žiadosť členských štátov**, a to najmä [...] **podporou dobrovoľnej** výmeny technických riešení medzi členskými štátmi;

d) podporou **inštitúcií, agentúr a orgánov EÚ a na požiadanie aj členských štátov** pri verejnej komunikácii o incidente alebo kríze;

e) **podporou členských štátov na ich žiadosť**, pokiaľ ide o skúšanie [...] plánov spolupráce v rámci reakcie na takéto incidenty alebo krízy.

Článok 8

*[...] **Trh, certifikácia kybernetickej bezpečnosti a normalizácia***

Agentúra:

a) podporuje a presadzuje tvorbu a vykonávanie politiky Únie v oblasti certifikácie kybernetickej bezpečnosti **procesov**, produktov a služieb IKT v zmysle hlavy III tohto nariadenia, a to tak, že:

1) vypracúva kandidátske európske systémy certifikácie kybernetickej bezpečnosti **procesov**, produktov a služieb IKT v **spolupráci s príslušným odvetvím** a v súlade s článkom 44 tohto nariadenia;

2) pomáha Komisii pri zabezpečovaní funkcie sekretariátu európskej skupiny pre certifikáciu kybernetickej bezpečnosti podľa článku 53 tohto nariadenia;

3) zostavuje a uverejňuje usmernenia a vypracúva osvedčené postupy z hľadiska kyberneticko-bezpečnostných požiadaviek na produkty a služby IKT, a to v spolupráci s vnútroštátnymi orgánmi pre certifikáciu **kybernetickej bezpečnosti** [...] a príslušným odvetvím;

3a) odporúča vhodné technické špecifikácie týkajúce sa využitia rozvoja európskych systémov certifikácie kybernetickej bezpečnosti podľa článku 47 ods. 1 písm. b) v prípadoch, keď normy nie sú k dispozícii;

3b) prispieva k vybudovaniu dostatočnej kapacity pre procesy hodnotenia a certifikácie zostavením a uverejnením usmernení, ako aj poskytovaním podpory členským štátom na ich žiadosť;

b) podporuje zavádzanie a využívanie európskych i medzinárodných noriem v oblasti riadenia rizík a bezpečnosti **procesov**, produktov a služieb IKT [...]**;**

ba) v spolupráci s členskými štátmi pripravuje odporúčania a usmernenia v technických oblastiach spojených s bezpečnostnými požiadavkami kladenými na prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb, ako aj v oblasti už existujúcich noriem vrátane vnútroštátnych noriem členských štátov, podľa článku 19 ods. 2 smernice (EÚ) 2016/1148;

c) vykonáva a šíri pravidelné analýzy hlavných trendov na trhu kybernetickej bezpečnosti, tak na strane dopytu, ako aj ponuky, s cieľom podporiť trh kybernetickej bezpečnosti v Únii.

Článok 9

*[...]**Znalosti a informácie***[...]

Agentúra:

a) analyzuje nastupujúce technológie a poskytuje tematicky zamerané posúdenia očakávaných spoločenských, právnych, hospodárskych a regulačných účinkov technologickej inovácie na kybernetickú bezpečnosť;

b) vykonáva dlhodobé strategické analýzy kybernetických hrozieb a incidentov s cieľom identifikovať nové trendy a pomôcť predchádzať [...] kybernetickým bezpečnostným **incidentom**;

c) v spolupráci s odborníkmi orgánov členských štátov poskytuje poradenstvo, usmernenia a osvedčené postupy v oblasti bezpečnosti sietí a informačných systémov, a najmä bezpečnosti infraštruktúr, [...] o ktoré sa opierajú odvetvia uvedené v prílohe II k smernici (EÚ) 2016/1148 a **ktoré využívajú poskytovatelia digitálnych služieb uvedených v prílohe III k danej smernici**;

d) zhromažďuje, organizuje a na vyhradenom portáli uverejňuje informácie o kybernetickej bezpečnosti, ktoré poskytli inštitúcie, agentúry a orgány Únie **a, na dobrovoľnom základe, členské štáty a súkromné a verejné zainteresované strany;**

e) [...]

f) zhromažďuje a analyzuje verejne dostupné informácie o závažných incidentoch a pripravuje správy s cieľom poskytnúť usmernenia pre podniky i občanov v celej Únii;

g) [...]

Článok 9a

Zvyšovanie povedomia a vzdelávanie

Agentúra:

a) zvyšuje verejné povedomie o kyberneticko-bezpečnostných rizikách a odporúča jednotlivým používateľom – občanom i organizáciám osvedčené postupy;

b) v spolupráci s členskými štátmi a inštitúciami, agentúrami a orgánmi Únie organizuje pravidelné osvetové kampane na zvýšenie kybernetickej bezpečnosti a jej viditeľnosti v Únii;

c) pomáha členským štátom v ich úsilí zvyšovať povedomie o kybernetickej bezpečnosti a podporovať vzdelávanie v oblasti kybernetickej bezpečnosti;

d) podporuje užšiu koordináciu a výmenu najlepších postupov medzi členskými štátmi, pokiaľ ide o zvyšovanie povedomia a vzdelávanie v oblasti kybernetickej bezpečnosti tým, že uľahčuje budovanie a udržiavanie siete národných vzdelávacích kontaktných miest.

Článok 10

[...] ***Výskum a inovácia***

V oblasti výskumu a inovácií agentúra:

a) radí Únii a členským štátom o potrebách a prioritách výskumu v oblasti kybernetickej bezpečnosti s cieľom umožniť účinnú reakciu na existujúce i nové riziká a hrozby, a to i v súvislosti s novými a nastupujúcimi informačnými a komunikačnými technológiami, a účinne používať technológie na prevenciu rizika;

b) ak na ňu Komisia deleguje príslušné právomoci, podieľa sa na implementačnej fáze programov financovania výskumu a inovácie, alebo sa na nich zúčastňuje ako príjemca.

Článok 11

[...] ***Medzinárodná spolupráca***

Agentúra prispieva k úsiliu Únie o spoluprácu s tretími krajinami a medzinárodnými organizáciami s cieľom podporiť medzinárodnú spoluprácu v kyberneticko-bezpečnostných otázkach, a to tým, že:

a) sa v náležitých prípadoch angažuje ako pozorovateľ pri organizácii medzinárodných cvičení, analyzuje ich výsledky a podáva o nich správy správnej rade;

b) **v príslušných rámcoch medzinárodnej spolupráce** [...] uľahčuje výmenu najlepších postupov [...].

c) na požiadanie poskytuje Komisii odborné poznatky;

ca) v spolupráci s európskou skupinou pre certifikáciu kybernetickej bezpečnosti zriadenou podľa článku 53 poskytuje poradenstvo a podporu Komisii v záležitostiach týkajúcich sa dohôd o vzájomnom uznávaní certifikátov kybernetickej bezpečnosti s tretími krajinami.

KAPITOLA II
ORGANIZÁCIA AGENTÚRY

Článok 12

Štruktúra

Administratívna a riadiaca štruktúra agentúry pozostáva z týchto prvkov:

a) správna rada, ktorá plní funkcie stanovené v článku 14;

b) výkonná rada, ktorá plní funkcie stanovené v článku 18;

c) výkonný riaditeľ, ktorý plní povinnosti stanovené v článku 19; [...]

d) stála skupina zainteresovaných strán, ktorá plní funkcie stanovené v článku 20**;**

da) sieť národných styčných dôstojníkov, ktorá plní funkcie stanovené v článku 20a.

ODDIEL 1
SPRÁVNA RADA

Článok 13

Zloženie správnej rady

1. Správnu radu tvorí jeden zástupca každého členského štátu a dvaja zástupcovia vymenovaní Komisiou. Všetci zástupcovia majú hlasovacie právo.

2. Každý člen správnej rady má náhradníka, ktorý zastupuje člena v jeho neprítomnosti.

3. Členovia správnej rady a ich náhradníci sa vymenúvajú na základe ich znalostí v oblasti kybernetickej bezpečnosti s prihliadnutím na relevantné riadiace, administratívne a rozpočtové zručnosti. Komisia a členské štáty sa vynasnažia obmedziť fluktuáciu svojich zástupcov v správnej rade s cieľom zabezpečiť kontinuitu jej práce. Komisia a členské štáty sa usilujú o vyvážené zastúpenie mužov a žien v správnej rade.

4. Funkčné obdobie členov správnej rady a ich náhradníkov je štyri roky. Toto obdobie je obnoviteľné.

Článok 14

Funkcie správnej rady

1. Správna rada:

a) vymedzuje všeobecné smerovanie činnosti agentúry a zabezpečuje, aby agentúra pracovala v súlade s pravidlami a zásadami stanovenými v tomto nariadení. Zabezpečuje aj súlad práce agentúry s činnosťami vykonávanými členskými štátmi i na úrovni Únie;

b) prijíma návrh jednotného programového dokumentu uvedeného v článku 21 pred jeho predložením Komisii na posúdenie;

c) zohľadňujúc posúdenie Komisie prijíma jednotný programový dokument agentúry dvojtretinovou väčšinou členských hlasov v súlade s článkom 17;

ca) dohliada na vykonávanie viacročného a ročného programovania začleneného do jednotného programového dokumentu;

d) dvojtretinovou väčšinou členských hlasov prijíma ročný rozpočet agentúry a vykonáva ostatné funkcie spojené s rozpočtom agentúry podľa kapitoly III;

e) posudzuje a prijíma konsolidovanú výročnú správu o činnosti agentúry, pričom posúdenie i správu do 1. júla nasledujúceho roka zasiela Európskemu parlamentu, Rade, Komisii a Dvoru audítorov. Výročná správa zahŕňa účtovné výkazy a opisuje sa v nej, do akej miery agentúra splnila svoje ukazovatele výkonnosti. Výročná správa sa zverejní;

f) prijíma rozpočtové pravidlá platné pre agentúru v súlade s článkom 29;

g) prijíma stratégiu boja proti podvodom, ktorá musí byť primeraná riziku podvodov so zreteľom na analýzu efektívnosti nákladov na opatrenia, ktoré sa majú vykonávať;

h) prijíma pravidlá predchádzania konfliktom záujmov svojich členov a ich riešenia;

i) zabezpečí primerané následné opatrenia v nadväznosti na zistenia a odporúčania vyplývajúce z vyšetrovania Európskeho úradu pre boj proti podvodom (OLAF) a rôznych správ a hodnotení interného alebo externého auditu;

j) prijíma svoj rokovací poriadok;

k) v súlade s odsekom 2 vykonáva vo vzťahu k pracovníkom agentúry právomoci udelené služobným poriadkom zamestnancov menovaciemu orgánu a podmienkami zamestnávania ostatných zamestnancov Európskej únie orgánu oprávnenému uzatvárať pracovné zmluvy (ďalej len „právomoci menovacieho orgánu“);

l) prijíma predpisy vykonávajúce služobný poriadok a podmienky zamestnávania ostatných zamestnancov v súlade s postupom uvedeným v článku 110 služobného poriadku;

m) vymenúva výkonného riaditeľa a v náležitých prípadoch predlžuje jeho funkčné obdobie alebo ho z funkcie odvoláva v súlade s článkom 33 tohto nariadenia;

n) vymenúva účtovníka, ktorým môže byť účtovník Komisie a ktorý je pri výkone svojich povinností úplne nezávislý;

o) prijíma všetky rozhodnutia o zriadení vnútorných štruktúr agentúry a v prípade potreby o ich zmene, pričom prihliada na potreby činnosti agentúry a zásadu riadneho finančného hospodárenia;

p) schvaľuje dohadovanie modalít spolupráce v súlade s článkami 7 a 39.

2. Správna rada v súlade s článkom 110 služobného poriadku prijíma rozhodnutie na základe článku 2 ods. 1 služobného poriadku a článku 6 podmienok zamestnávania ostatných zamestnancov, ktorým deleguje príslušné právomoci menovacieho orgánu na výkonného riaditeľa a ktorým vymedzuje podmienky, za ktorých možno toto delegovanie právomoci pozastaviť. Výkonný riaditeľ je oprávnený tieto právomoci delegovať ďalej.

3. Ak si to vyžadujú mimoriadne okolnosti, správna rada môže na základe rozhodnutia dočasne pozastaviť delegovanie právomocí menovacieho orgánu na výkonného riaditeľa a na subjekty, ktorým ďalej delegoval právomoc, a tieto právomoci vykonávať sama alebo ich delegovať na jedného zo svojich členov alebo na zamestnanca, ktorý nie je výkonným riaditeľom.

Článok 15

Predseda správnej rady

Správna rada spomedzi svojich členov dvojtretinovou väčšinou hlasov volí svojho predsedu a zástupcu predsedu na obdobie štyroch rokov, ktoré je obnoviteľné raz. Ak však ich členstvo v správnej rade kedykoľvek počas ich funkčného obdobia zanikne, ich funkčné obdobie sa automaticky končí k danému dátumu. Ak predseda nie je schopný plniť si svoje povinnosti, zástupca predsedu ho nahradí *ex officio*.

Článok 16

Zasadnutia správnej rady

1. Zasadnutia správnej rady zvoláva jej predseda.

2. Riadne zasadnutia správnej rady sa konajú aspoň dvakrát ročne. Na žiadosť predsedu, Komisie alebo najmenej tretiny svojich členov zasadá správna rada aj mimoriadne.

3. Výkonný riaditeľ sa zúčastňuje na zasadnutiach správnej rady, avšak bez hlasovacieho práva.

4. Na zasadnutiach správnej rady sa môžu na pozvanie predsedu zúčastniť členovia stálej skupiny zainteresovaných strán, avšak bez hlasovacieho práva.

5. Členom správnej rady a ich náhradníkom môžu v súlade s rokovacím poriadkom pomáhať poradcovia alebo experti.

6. Sekretariát pre správnu radu zabezpečuje agentúra.

Článok 17

Pravidlá hlasovania správnej rady

1. Správna rada prijíma rozhodnutia väčšinou hlasov svojich členov.

2. Dvojtretinová väčšina hlasov všetkých členov správnej rady sa vyžaduje v prípade jednotného programového dokumentu, ročného rozpočtu, menovania a odvolania výkonného riaditeľa či predĺženia jeho funkčného obdobia.

3. Každý člen má jeden hlas. Ak je člen správnej rady neprítomný, toto hlasovacie právo uplatňuje jeho náhradník.

4. Predseda sa na hlasovaní zúčastňuje.

5. Výkonný riaditeľ sa na hlasovaní nezúčastňuje.

6. V rokovacom poriadku správnej rady sa stanovujú podrobnejšie mechanizmy hlasovania, najmä podmienky, za ktorých môže člen konať v mene iného člena.

ODDIEL 2
VÝKONNÁ RADA

Článok 18

Výkonná rada

1. Správnej rade pomáha výkonná rada.

2. Výkonná rada:

   a) pripravuje rozhodnutia, ktoré má prijať správna rada;

   b) spolu so správnou radou zabezpečuje prijatie vhodných opatrení v nadväznosti na zistenia a odporúčania vyplývajúce z vyšetrovaní úradu OLAF a z rôznych interných alebo externých audítorských správ a hodnotení;

   c) bez toho, aby boli dotknuté zodpovednosti výkonného riaditeľa stanovené v článku 19, pomáha a radí výkonnému riaditeľovi pri vykonávaní rozhodnutí správnej rady v administratívnej a rozpočtovej oblasti podľa článku 19.

3. Výkonná rada pozostáva z piatich členov vymenovaných spomedzi členov správnej rady, z ktorých jedným je predseda správnej rady, ktorý môže predsedať aj výkonnej rade, a ďalším je jeden zo zástupcov Komisie. Výkonný riaditeľ sa zúčastňuje na zasadnutiach výkonnej rady, ale nemá hlasovacie právo.

4. Funkčné obdobie členov výkonnej rady je štyri roky. Toto obdobie je obnoviteľné.

5. Výkonná rada zasadá aspoň raz za tri mesiace. Predseda výkonnej rady zvoláva ďalšie zasadnutia na žiadosť jej členov.

6. Rokovací poriadok výkonnej rady stanovuje správna rada.

7. [...]

ODDIEL 3
VÝKONNÝ RIADITEĽ

Článok 19

Zodpovednosti výkonného riaditeľa

1. Agentúru riadi jej výkonný riaditeľ, ktorý je pri výkone svojich povinností nezávislý. Výkonný riaditeľ sa zodpovedá správnej rade.

2. Výkonný riaditeľ podáva na vyzvanie Európskemu parlamentu správu o plnení svojich povinností. Rada môže vyzvať výkonného riaditeľa, aby podal správu o plnení svojich povinností.

3. Výkonný riaditeľ je zodpovedný za:

a) každodennú správu agentúry;

b) vykonávanie rozhodnutí prijatých správnou radou;

c) prípravu návrhu jednotného programového dokumentu a jeho predloženie správnej rade na schválenie pred tým, než sa predloží Komisii;

d) vykonávanie jednotného programového dokumentu a zodpovedajúce informovanie správnej rady;

e) vypracovanie konsolidovanej výročnej správy o činnostiach agentúry **vrátane plnenia ročného pracovného programu** a jej predloženie správnej rade na posúdenie a prijatie;

f) vypracovanie akčného plánu v nadväznosti na závery spätných hodnotení a predloženie správy o pokroku Komisii každé dva roky;

g) prípravu akčného plánu v nadväznosti na závery správ z interného alebo externého auditu, ako aj z vyšetrovaní Európskeho úradu pre boj proti podvodom (OLAF) a za predkladanie správ o pokroku, a to dvakrát ročne Komisii a pravidelne správnej rade;

h) prípravu návrhu rozpočtových pravidiel platných pre agentúru;

i) prípravu návrhu výkazu odhadov príjmov a výdavkov agentúry a plnenie jej rozpočtu;

j) ochranu finančných záujmov Únie uplatňovaním preventívnych opatrení proti podvodom, korupcii a akýmkoľvek iným nezákonným činnostiam, účinnými kontrolami, ak sa zistia nezrovnalosti spätným získaním neoprávnene vyplatených súm, a prípadne účinnými, primeranými a odradzujúcimi administratívnymi a finančnými sankciami;

k) vypracovanie stratégie agentúry pre boj proti podvodom a jej predloženie správnej rade na schválenie;

l) nadviazanie a udržiavanie kontaktov s podnikateľskou komunitou a spotrebiteľskými organizáciami na zabezpečenie pravidelného dialógu s príslušnými zainteresovanými stranami;

la) pravidelnú výmenu informácií s inštitúciami, agentúrami a orgánmi Únie, pokiaľ ide o ich činnosti v oblasti kybernetickej bezpečnosti na zabezpečenie súladu pri vypracúvaní a vykonávaní politiky EÚ;

m) ostatné úlohy, ktoré sú výkonnému riaditeľovi pridelené týmto nariadením.

4. V prípade potreby môže výkonný riaditeľ v rámci mandátu agentúry a v súlade s jej cieľmi a úlohami vytvoriť ad hoc pracovné skupiny zložené z expertov vrátane tých, ktorí pochádzajú z príslušných orgánov členských štátov. Správna rada o tom musí byť vopred informovaná. Postupy týkajúce sa najmä zloženia týchto pracovných skupín, menovania príslušných expertov výkonným riaditeľom a fungovania pracovných skupín sa spresnia vo vnútorných pravidlách činnosti agentúry.

5. **V prípade potreby, na účely efektívneho a účinného plnenia úloh agentúry a na základe primeranej analýzy nákladov a prínosov môže** výkonný riaditeľ rozhodnúť, **že sa** [...] **zriadi jeden alebo viacero miestnych úradov v jednom alebo viacerých členských štátoch.** Pred rozhodnutím o zriadení miestneho úradu výkonný riaditeľ **požiada o stanovisko dotknutého členského štátu alebo štátov vrátane členského štátu, v ktorom má agentúra sídlo, a** získa predchádzajúci súhlas Komisie a správnej rady [...]. **V prípade sporu medzi výkonným riaditeľom a dotknutým členským štátom v priebehu konzultačného procesu sa záležitosť predloží na prerokovanie v Rade.** V danom rozhodnutí sa vymedzí rozsah činností, ktoré sa majú v miestnej kancelárii vykonávať, a to tak, aby sa zabránilo vzniku zbytočných nákladov a duplicite administratívnych funkcií agentúry.**[...] Počet zamestnancov v miestnych úradoch je minimálny a <u>celkovo</u> neprekročí 40 % počtu <u>[...]</u> zamestnancov agentúry v <u>členskom štáte, v ktorom sa nachádza jej sídlo.</u> Počet zamestnancov v žiadnom miestnom úrade neprekročí 10 % <u>[...]</u> počtu <u>[..]</u> zamestnancov agentúry v <u>členskom štáte, v ktorom sa nachádza jej sídlo.</u>**

ODDIEL 4
STÁLA SKUPINA ZAINTERESOVANÝCH STRÁN

Článok 20

Stála skupina zainteresovaných strán

1. Správna rada konajúca na návrh výkonného riaditeľa zriadi stálu skupinu zainteresovaných strán zloženú z uznávaných expertov zastupujúcich príslušné zainteresované strany, ako sú odvetvie IKT, poskytovatelia verejne dostupných elektronických komunikačných sietí alebo služieb, **prevádzkovatelia základných služieb**, spotrebiteľské skupiny, akademickí experti na kybernetickú bezpečnosť a zástupcovia príslušných orgánov notifikovaní podľa [smernice, ktorou sa stanovuje európsky kódex elektronickej komunikácie], ako aj orgánov presadzovania práva a ochrany údajov.

2. Postupy stálej skupiny zainteresovaných strán, najmä z hľadiska počtu, zloženia a menovania jej členov správnou radou, návrhu výkonného riaditeľa a činnosti tejto skupiny sa vymedzia vo vnútorných pravidlách činnosti agentúry a zverejnia sa.

3. Stálej skupine zainteresovaných strán predsedá výkonný riaditeľ alebo ktorákoľvek osoba, ktorú výkonný riaditeľ v jednotlivých prípadoch vymenuje.

4. Funkčné obdobie členov stálej skupiny zainteresovaných strán je dva a pol roka. Členovia správnej rady nemôžu byť členmi stálej skupiny zainteresovaných strán. Experti z Komisie a členských štátov sú oprávnení zúčastňovať sa na zasadnutiach stálej skupiny zainteresovaných strán a podieľať sa na jej práci. Na zasadnutia stálej skupiny zainteresovaných strán a k účasti na jej práci možno prizvať aj zástupcov iných orgánov, ktoré výkonný riaditeľ považuje za relevantné a ktoré nie sú členmi stálej skupiny zainteresovaných strán.

5. Stála skupina zainteresovaných strán agentúre radí v súvislosti s vykonávaním jej činností. Predovšetkým radí výkonnému riaditeľovi pri vypracúvaní návrhu pracovného programu agentúry a pri zabezpečovaní komunikácie s príslušnými zainteresovanými stranami o všetkých otázkach týkajúcich sa pracovného programu.

5a. Stála skupina zainteresovaných strán pravidelne informuje správnu radu o svojich činnostiach.

ODDIEL 4A
SIEŤ NÁRODNÝCH STYČNÝCH DÔSTOJNÍKOV

Článok 20a

Sieť národných styčných dôstojníkov

1. Správna rada konajúca na návrh výkonného riaditeľa zriadi sieť národných styčných dôstojníkov zloženú zo zástupcov členských štátov.

2. Sieť národných styčných dôstojníkov sa skladá zo zástupcov všetkých členských štátov. Každý členský štát vymenuje jedného zástupcu. Zasadnutia siete sa môžu konať v rôznych expertných zloženiach.

3. Sieť národných styčných dôstojníkov najmä uľahčuje výmenu informácií medzi agentúrou ENISA a členskými štátmi. Konkrétne podporuje agentúru ENISA pri šírení jej činností, zistení a odporúčaní príslušným zainteresovaným stranám v celej EÚ.

4. Národní styční dôstojníci pôsobia ako ústredné kontaktné miesta na vnútroštátnej úrovni s cieľom uľahčiť spoluprácu medzi agentúrou ENISA a národnými expertmi pri plnení programu agentúry ENISA.

5. Národní styční dôstojníci by síce mali úzko spolupracovať so zástupcami správnej rady z ich príslušných krajín, ale sieť samotná nezdvojuje prácu riadiacej rady ani iných fór EÚ.

6. Funkcie a postupy siete národných styčných dôstojníkov sa stanovia vo vnútorných pravidlách činnosti agentúry a zverejnia sa.

ODDIEL 5
ČINNOSŤ

Článok 21

Jednotný programový dokument

1. Agentúra vykonáva svoje činnosti v súlade s jednotným programovým dokumentom, ktorý zahŕňa jej ročné a viacročné plánovanie vrátane všetkých jej plánovaných činností.

2. Výkonný riaditeľ každý rok vypracúva návrh jednotného programového dokumentu, ktorý obsahuje ročné a viacročné plánovanie vrátane plánovania zodpovedajúcich ľudských a finančných zdrojov v súlade s článkom 32 delegovaného nariadenia Komisie (EÚ) č. 1271/2013[14], pričom zohľadní usmernenia stanovené Komisiou.

3. Správna rada každoročne jednotný programový dokument uvedený v odseku 1 prijme do 30. novembra a zašle ho Európskemu parlamentu, Rade a Komisii najneskôr 31. januára nasledujúceho roka, pričom im zasiela aj všetky neskôr aktualizované verzie uvedeného dokumentu.

4. Jednotný programový dokument nadobudne konečné znenie po konečnom prijatí všeobecného rozpočtu Únie, pričom sa podľa potreby náležite upraví.

5. Ročný pracovný program zahŕňa podrobné ciele a očakávané výsledky vrátane ukazovateľov výkonnosti. Obsahuje aj opis opatrení, ktoré sa majú financovať, a odhad finančných a ľudských zdrojov vyčlenených na každé opatrenie v súlade so zásadami zostavovania rozpočtu a riadenia podľa činností. Ročný pracovný program musí byť súlade s viacročným pracovným programom uvedeným v odseku 7. Jasne sa v ňom vymedzia úlohy, ktoré sa oproti predošlému rozpočtovému roku pridali, zmenili alebo zrušili.

---

[14] Delegované nariadenie Komisie (EÚ) č. 1271/2013 z 30. septembra 2013 o rámcovom nariadení o rozpočtových pravidlách pre subjekty uvedené v článku 208 nariadenia Európskeho parlamentu a Rady (EÚ, Euratom) č. 966/2012 (Ú. v. EÚ L 328, 7.12.2013, s. 42).

6. Ak sa agentúre zverí nová úloha, správna rada prijatý ročný pracovný program zmení. Každá podstatná zmena ročného pracovného programu sa prijíma rovnakým postupom ako pôvodný ročný pracovný program. Právomoc vykonávať nepodstatné zmeny ročného pracovného programu môže správna rada delegovať na výkonného riaditeľa.

7. Vo viacročnom pracovnom programe sa stanovuje všeobecné strategické plánovanie vrátane cieľov, očakávaných výsledkov a ukazovateľov výkonnosti. Zároveň sa ňom uvádza plánovanie zdrojov vrátane viacročného rozpočtu a zamestnancov.

8. Plánovanie zdrojov sa každoročne aktualizuje. Strategické plánovanie sa aktualizuje podľa potreby, najmä so zámerom zohľadniť výsledky hodnotenia uvedeného v článku 56.

Článok 22

Vyhlásenie o záujmoch

1. Výkonný riaditeľ, ako aj každý člen správnej rady a každý úradník dočasne vyslaný členským štátom predloží vyhlásenie o záväzkoch a vyhlásenie o absencii alebo existencii akýchkoľvek priamych alebo nepriamych záujmov, ktoré by sa mohli považovať za záujmy ovplyvňujúce ich nezávislosť. Vyhlásenia musia byť presné a úplné, každoročne sa poskytujú písomne a podľa potreby sa aktualizujú.

2. Členovia správnej rady, výkonný riaditeľ a externí experti, ktorí sa zúčastňujú v ad hoc pracovných skupinách, presne a úplne oznámia najneskôr na začiatku každého zasadnutia akékoľvek záujmy, ktoré by sa mohli považovať za záujmy ovplyvňujúce ich nezávislosť v súvislosti s bodmi programu, a zdržia sa účasti na diskusiách k týmto bodom a na hlasovaní o nich.

3. Agentúra vo svojich vnútorných pravidlách činnosti stanoví praktické opatrenia pre pravidlá o vyhláseniach o záujmoch uvedených v odsekoch 1 a 2.

Článok 23

Transparentnosť

1. Agentúra vykonáva svoje činnosti s vysokým stupňom transparentnosti a v súlade s článkom 25.

2. Agentúra zabezpečí, aby verejnosť a všetky zainteresované strany dostávali náležité, objektívne, spoľahlivé a ľahko dostupné informácie, najmä o výsledkoch jej práce. Agentúra takisto zverejňuje vyhlásenia o záujmoch predkladané podľa článku 22.

3. Správna rada konajúc na návrh výkonného riaditeľa môže subjektom, ktoré majú záujem, povoliť pozorovanie postupov niektorých činností agentúry.

4. Agentúra vo svojich vnútorných pravidlách činnosti stanoví praktické opatrenia na vykonávanie pravidiel transparentnosti uvedených v odsekoch 1 a 2.

Článok 24

Dôvernosť informácií

1. Bez toho, aby bol dotknutý článok 25, agentúra nesmie poskytovať tretím stranám informácie, ktoré spracúva alebo získava a v súvislosti s ktorými bola podaná odôvodnená žiadosť o úplné alebo čiastočné dôverné zaobchádzanie.

2. Členovia správnej rady, výkonný riaditeľ, členovia stálej skupiny zainteresovaných strán, externí experti zúčastňujúci sa ad hoc pracovných skupín a zamestnanci agentúry vrátane úradníkov dočasne vyslaných členskými štátmi musia spĺňať aj po skončení povinností požiadavky na dôvernosť informácií podľa článku 339 Zmluvy o fungovaní Európskej únie (ZFEÚ).

3. Agentúra vo svojich vnútorných pravidlách činnosti stanoví praktické opatrenia na vykonávanie pravidiel týkajúcich sa dôvernosti informácií uvedených v odsekoch 1 a 2.

4. Ak je to potrebné pre vykonávanie úloh agentúry, správna rada rozhodne, že agentúre povolí pracovať s utajovanými skutočnosťami. V takom prípade správna rada po dohode s útvarmi Komisie prijme vnútorné pravidlá činnosti, ktorými sa uplatňujú zásady bezpečnosti stanovené v rozhodnutiach Komisie (EÚ, Euratom) 2015/443[15] a 2015/444[16]. Tieto pravidlá musia zahŕňať ustanovenia týkajúce sa výmeny, spracovania a uchovávania utajovaných skutočností.

---

[15] Rozhodnutie Komisie (EÚ, Euratom) 2015/443 z 13. marca 2015 o bezpečnosti v Komisii (Ú. v. EÚ L 72, 17.3.2015, s. 41).

[16] Rozhodnutie Komisie (EÚ, Euratom) 2015/444 z 13. marca 2015 o bezpečnostných predpisoch na ochranu utajovaných skutočností EÚ (Ú. v. EÚ L 72, 17.3.2015, s. 53).

Článok 25

Prístup k dokumentom

1. Na dokumenty, ktoré má agentúra v držbe, sa vzťahuje nariadenie (ES) č. 1049/2001.

2. Správna rada prijme opatrenia na vykonanie nariadenia (ES) č. 1049/2001 do šiestich mesiacov od zriadenia agentúry.

3. Rozhodnutia prijaté agentúrou podľa článku 8 nariadenia (ES) č. 1049/2001 môžu byť predmetom sťažnosti podanej ombudsmanovi podľa článku 228 ZFEÚ alebo konania pred Súdnym dvorom Európskej únie podľa článku 263 ZFEÚ.

KAPITOLA III
ZOSTAVOVANIE A ŠTRUKTÚRA ROZPOČTU

Článok 26

Zostavovanie rozpočtu

1. Výkonný riaditeľ každoročne vypracúva návrh výkazu odhadov príjmov a výdavkov agentúry na nasledujúci rozpočtový rok a postupuje ho správnej rade spolu s návrhom plánu pracovných miest. Príjmy a výdavky musia byť v rovnováhe.

2. Správna rada každý rok na základe návrhu výkazu odhadov príjmov a výdavkov uvedeného v odseku 1 vytvorí výkaz odhadov príjmov a výdavkov agentúry na nasledujúci rozpočtový rok.

3. Výkaz odhadov uvedený v odseku 2, ktorý je súčasťou návrhu jednotného programového dokumentu, správna rada každoročne do 31. januára zasiela Komisii a tretím krajinám, s ktorými Únia uzatvorila dohody v súlade s článkom 39.

4. Komisia na základe tohto výkazu odhadov zaradí do návrhu rozpočtu Únie odhady, ktoré pokladá za potrebné pre plán pracovných miest, a výšku príspevku, ktorá sa má uhradiť zo všeobecného rozpočtu, ktoré predloží Európskemu parlamentu a Rade v súlade s článkom 313 a 314 ZFEÚ.

5. Európsky parlament a Rada schvaľujú rozpočtové prostriedky na príspevok agentúre.

6. Európsky parlament a Rada prijímajú plán pracovných miest agentúry.

7. Správna rada prijíma rozpočet agentúry spolu s jednotným programovým dokumentom. Rozpočet sa stáva konečným po prijatí všeobecného rozpočtu Únie s konečnou platnosťou. Správna rada v prípade potreby upraví rozpočet a jednotný programový dokument agentúry v súlade so všeobecným rozpočtom Únie.

Článok 27

Štruktúra rozpočtu

1. Bez toho, aby boli dotknuté iné zdroje, príjmy agentúry zahŕňajú:

   a) príspevok z rozpočtu Únie;

   b) príjmy určené na krytie konkrétnych výdavkových položiek v súlade s jej rozpočtovými pravidlami uvedenými v článku 29;

   c) finančné prostriedky Únie na základe dohôd o príspevku alebo ad hoc grantov v súlade s jej rozpočtovými pravidlami uvedenými v článku 29 a s ustanoveniami príslušných nástrojov na podporu politík Únie;

d) príspevky tretích krajín podieľajúcich sa na činnosti agentúry podľa článku 39;

e) prípadné peňažné či nepeňažné dobrovoľné príspevky členských štátov; členským štátom, ktoré poskytujú dobrovoľné príspevky, za ne nevzniká nárok na žiadne osobitné práva alebo služby.

2. Medzi výdavky agentúry patria výdavky na zamestnancov, administratívnu a technickú podporu, infraštruktúru a prevádzku a výdavky vyplývajúce zo zmlúv uzatvorených s tretími stranami.

Článok 28

Plnenie rozpočtu

1. Výkonný riaditeľ je zodpovedný za plnenie rozpočtu agentúry.

2. Vnútorný audítor Komisie má rovnaké právomoci nad agentúrou ako nad oddeleniami Komisie.

3. Účtovník agentúry zasiela do 1. marca po každom rozpočtovom roku (1. marca roku N + 1) účtovníkovi Komisie a Dvoru audítorov predbežnú účtovnú závierku.

4. Po doručení pripomienok Dvora audítorov k predbežnej účtovnej závierke agentúry vypracuje účtovník agentúry na vlastnú zodpovednosť konečnú účtovnú závierku agentúry.

5. Výkonný riaditeľ predkladá konečnú účtovnú závierku na posúdenie správnej rade.

6. Výkonný riaditeľ zasiela do 31. marca roka N + 1 Európskemu parlamentu, Rade, Komisii a Dvoru audítorov správu o rozpočtovom a finančnom hospodárení.

7. Účtovník do 1. júla roka N + 1 zasiela konečnú účtovnú závierku Európskemu parlamentu, Rade, účtovníkovi Komisie a Dvoru audítorov spolu so stanoviskom správnej rady.

8. V deň zaslania konečnej účtovnej závierky účtovník zároveň zasiela Dvoru audítorov vyhlásenie k tejto konečnej účtovnej závierke a jeho kópiu zasiela účtovníkovi Komisie.

9. Výkonný riaditeľ uverejňuje konečnú účtovnú závierku do 15. novembra nasledujúceho roka.

10. Výkonný riaditeľ zasiela Dvoru audítorov do 30. septembra roka N + 1 odpoveď na jeho pripomienky, pričom kópiu tejto odpovede zasiela správnej rade a Komisii.

11. Výkonný riaditeľ predloží Európskemu parlamentu na jeho žiadosť všetky informácie potrebné na bezproblémové uplatnenie postupu udelenia absolutória za daný rozpočtový rok, ako sa stanovuje v článku 165 ods. 3 nariadenia o rozpočtových pravidlách.

12. Európsky parlament konajúc na odporúčanie Rady do 15. mája roka N + 2 udelí výkonnému riaditeľovi absolutórium za plnenie rozpočtu za rok N.

Článok 29

Rozpočtové pravidlá

Rozpočtové pravidlá agentúry prijme správna rada po porade s Komisiou. Nesmú sa odchyľovať od nariadenia (EÚ) č. 1271/2013, pokiaľ takáto odchýlka nie je osobitne potrebná na prevádzku agentúry a Komisia s ňou vopred súhlasila.

Článok 30

Boj proti podvodom

1. V záujme uľahčenia boja proti podvodom, korupcii a ďalším nezákonným činnostiam podľa nariadenia Európskeho parlamentu a Rady (ES) č. 883/2013[17] agentúra do šiestich mesiacov odo dňa začatia svojej činnosti pristúpi k medziinštitucionálnej dohode z 25. mája 1999, ktorá sa týka vnútorných vyšetrovaní Európskym úradom pre boj proti podvodom (OLAF), a prijme vhodné ustanovenia uplatniteľné na všetkých zamestnancov agentúry, pričom použije vzor uvedený v prílohe k uvedenej dohode.

2. Dvor audítorov je oprávnený vykonávať audit na základe dokumentov a na mieste u všetkých príjemcov grantov, dodávateľov a subdodávateľov, ktorým agentúra poskytla finančné prostriedky Únie.

[17] Nariadenie Európskeho parlamentu a Rady (EÚ, Euratom) No 883/2013 z 11. septembra 2013 o vyšetrovaniach vykonávaných Európskym úradom pre boj proti podvodom (OLAF), ktorým sa zrušuje nariadenie Európskeho parlamentu a Rady (ES) č. 1073/1999 a nariadenie Rady (Euratom) č. 1074/1999 (Ú. v. EÚ L 248, 18.9.2013, s. 1).

3. OLAF môže vykonávať vyšetrovania vrátane kontrol a inšpekcií na mieste v súlade s ustanoveniami a postupmi stanovenými v nariadení Európskeho parlamentu a Rady (EÚ, Euratom) č. 883/2013 a v nariadení Rady (Euratom, ES) č. 2185/96[18] z 11. novembra 1996 o kontrolách a inšpekciách na mieste vykonávaných Komisiou s cieľom ochrany finančných záujmov Únie pred spreneverou a inými podvodmi, aby zistil, či v súvislosti s grantom alebo zmluvou financovanými agentúrou nedošlo k podvodu, korupcii alebo akémukoľvek inému nezákonnému konaniu poškodzujúcemu finančné záujmy Únie.

4. Bez toho, aby boli dotknuté odseky 1, 2 a 3, dohody o spolupráci s tretími krajinami a s medzinárodnými organizáciami, zmluvy, dohody o grante a rozhodnutia agentúry o grante musia obsahovať ustanovenia, ktorými sa Dvoru audítorov a úradu OLAF výslovne udeľuje právomoc vykonávať takéto audity a vyšetrovania v súlade s ich príslušnými právomocami.

KAPITOLA IV
PERSONÁL AGENTÚRY

Článok 31

Všeobecné ustanovenia

Na zamestnancov agentúry sa vzťahuje služobný poriadok a podmienky zamestnávania ostatných zamestnancov, ako aj pravidlá prijaté na základe dohody medzi inštitúciami Únie týkajúce sa vykonávania služobného poriadku.

[18] Nariadenie Rady (Euratom, ES) č. 2185/96 z 11. novembra 1996 o kontrolách a inšpekciách na mieste, vykonávaných Komisiou s cieľom ochrany finančných záujmov Európskych spoločenstiev pred spreneverou a inými podvodmi (Ú. v. ES L 292, 15.11.1996, s. 2).

Článok 32

Výsady a imunity

Na agentúru a jej zamestnancov sa vzťahuje Protokol č. 7 o výsadách a imunitách Európskej únie, ktorý je pripojený k Zmluve o Európskej únii a k ZFEÚ.

Článok 33

Výkonný riaditeľ

1. Výkonný riaditeľ pôsobí ako dočasný zástupca agentúry podľa článku 2 písm. a) podmienok zamestnávania ostatných zamestnancov.

2. Výkonného riaditeľa vymenúva správna rada zo zoznamu kandidátov navrhnutých Komisiou pri uplatnení otvoreného a transparentného výberového konania.

3. Na účely uzatvorenia zmluvy s výkonným riaditeľom zastupuje agentúru predseda správnej rady.

4. Kandidát, ktorého vybrala správna rada, sa pred vymenovaním vyjadrí pred príslušným výborom Európskeho parlamentu a odpovie na otázky jeho členov.

5. Funkčné obdobie výkonného riaditeľa trvá **štyri** [...] roky. Na konci tohto obdobia Komisia vykoná posúdenie, v ktorom zohľadní hodnotenie výsledkov činnosti výkonného riaditeľa a budúce úlohy a výzvy agentúry.

6. Správna rada prijíma rozhodnutia o vymenovaní výkonného riaditeľa, predĺžení jeho funkčného obdobia alebo jeho odvolaní z funkcie na základe dvojtretinovej väčšiny hlasov členov s hlasovacím právom.

7. Správna rada konajúc na návrh Komisie, v ktorom sa zohľadní posúdenie uvedené v odseku 5, môže predĺžiť funkčné obdobie výkonného riaditeľa raz, najviac o **štyri** [...] roky.

8. Správna rada informuje Európsky parlament o svojom úmysle predĺžiť funkčné obdobie výkonného riaditeľa. Počas troch mesiacov pred takýmto predĺžením funkčného obdobia sa výkonný riaditeľ, ak k tomu bude vyzvaný, vyjadrí pred príslušným výborom Európskeho parlamentu a odpovie na otázky jeho členov.

9. Výkonný riaditeľ, ktorého funkčné obdobie sa predĺžilo, sa nemôže zúčastniť na ďalšom výberovom konaní na rovnakú funkciu.

10. Výkonný riaditeľ môže byť odvolaný z funkcie len na základe rozhodnutia správnej rady [...].

Článok 34

Vyslaní národní experti a ďalší pracovníci

1. Agentúra môže využívať vyslaných národných expertov alebo ďalších pracovníkov, ktorých nezamestnáva. Služobný poriadok a podmienky zamestnávania ostatných zamestnancov sa na týchto pracovníkov nevzťahujú.

2. Správna rada prijme rozhodnutie, v ktorom stanoví pravidlá vysielania národných expertov do agentúry.

KAPITOLA V
VŠEOBECNÉ USTANOVENIA

Článok 35

Právne postavenie agentúry

1. Agentúra je orgánom Únie a má právnu subjektivitu.

2. Agentúra má v každom členskom štáte najširšiu právnu spôsobilosť, akú jeho právo priznáva právnickým osobám. Môže najmä nadobúdať hnuteľný a nehnuteľný majetok a nakladať s ním, ako aj byť účastníkom súdnych konaní [...].

3. Agentúru navonok zastupuje jej výkonný riaditeľ.

Článok 36

Zodpovednosť agentúry

1. Zmluvná zodpovednosť agentúry sa spravuje rozhodným právom pre danú zmluvu.

2. Súdny dvor Európskej únie má právomoc rozhodovať podľa akejkoľvek arbitrážnej doložky obsiahnutej v zmluve uzatvorenej agentúrou.

3. V prípade mimozmluvnej zodpovednosti agentúra nahradí v súlade so všeobecnými zásadami spoločnými pre práva členských štátov všetky škody, ktoré spôsobila agentúra alebo jej zamestnanci pri vykonávaní svojich povinností.

4. Vo všetkých sporoch súvisiacich s náhradou takejto škody má právomoc rozhodovať Súdny dvor Európskej únie.

5. Osobná zodpovednosť zamestnancov agentúry voči nej sa riadi príslušnými podmienkami uplatniteľnými na zamestnancov agentúry.

Článok 37

Pravidlá používania jazykov

1. Na agentúru sa vzťahuje nariadenie Rady č. 1[19]. Členské štáty a ostatné nimi menované orgány sa môžu obrátiť na agentúru a dostať odpoveď v úradnom jazyku inštitúcií Únie podľa ich výberu.

2. Prekladateľské služby potrebné na prevádzku agentúry zabezpečuje Prekladateľské stredisko pre orgány Európskej únie.

Článok 38

Ochrana osobných údajov

1. Spracovávanie osobných údajov agentúrou podlieha nariadeniu Európskeho parlamentu a Rady (ES) č. 45/2001[20].

2. Správna rada prijme vykonávacie opatrenia uvedené v článku 24 ods. 8 nariadenia (ES) č. 45/2001. Správna rada môže prijať dodatočné opatrenia potrebné na uplatňovanie nariadenia (ES) č. 45/2001 agentúrou.

---

[19] Nariadenie č. 1, ktorým sa určujú jazyky používané Európskym spoločenstvom pre atómovú energiu (Ú. v. ES L 17, 6.10.1958, s. 401).

[20] Nariadenie Európskeho parlamentu a Rady (ES) č. 45/2001 z 18. decembra 2000 o ochrane jednotlivcov so zreteľom na spracovanie osobných údajov inštitúciami a orgánmi Spoločenstva a o voľnom pohybe takýchto údajov (Ú. v. ES L 8, 12.1.2001, s. 1).

Článok 39

Spolupráca s tretími krajinami a medzinárodnými organizáciami

1. V rozsahu potrebnom na dosiahnutie cieľov stanovených v tomto nariadení môže agentúra spolupracovať s príslušnými orgánmi tretích krajín a/alebo s medzinárodnými organizáciami. Na tento účel môže agentúra s výhradou predchádzajúceho schválenia Komisiou dohodnúť modality spolupráce s uvedenými orgánmi tretích krajín a medzinárodnými organizáciami. Týmito modalitami nevznikajú Únii ani jej členským štátom žiadne právne záväzky.

2. Agentúra je otvorená účasti tretích krajín, ktoré na tento účel uzavreli dohody s Úniou. Podľa príslušných ustanovení týchto dohôd sa prijmú opatrenia určujúce predovšetkým povahu, rozsah a spôsob, akým sa tieto krajiny budú podieľať na práci agentúry, vrátane ustanovení týkajúcich sa účasti na iniciatívach uskutočňovaných agentúrou, finančných príspevkov a personálnych otázok. Pokiaľ ide o personálne otázky, musia byť tieto opatrenia za každých okolností v súlade so služobným poriadkom.

3. Správna rada prijme stratégiu pre vzťahy s tretími krajinami alebo medzinárodnými organizáciami v otázkach spadajúcich do právomoci agentúry. Komisia sa uistí, že agentúra vykonáva svoje činnosti v súlade s mandátom a platným inštitucionálnym rámcom, a to uzavretím primeraných pracovných dojednaní s výkonným riaditeľom agentúry.

Článok 40

Bezpečnostné predpisy v oblasti ochrany utajovaných skutočností a citlivých neutajovaných skutočností

Agentúra v konzultácii s Komisiou prijme vlastné bezpečnostné predpisy, v ktorých uplatní bezpečnostné zásady obsiahnuté v bezpečnostných predpisoch Komisie na ochranu utajovaných skutočností Európskej únie (EUCI) a citlivých neutajovaných skutočností podľa rozhodnutí Komisie (EÚ, Euratom) 2015/443, resp. 2015/444. Okrem iného ide o ustanovenia týkajúce sa výmeny, spracovania a uchovávania takýchto skutočností.

Článok 41

Dohoda o sídle a prevádzkové podmienky

1. Potrebné ustanovenia o poskytnutí sídla agentúre v hostiteľskom členskom štáte a o zariadeniach, ktoré má tento členský štát sprístupniť, ako aj osobitné pravidlá, ktoré sa v hostiteľskom členskom štáte vzťahujú na výkonného riaditeľa, členov správnej rady, zamestnancov agentúry a členov ich rodín, sa vymedzia v dohode o sídle uzatvorenej medzi agentúrou a členským štátom, v ktorom sa nachádza sídlo, po schválení správnou radou najneskôr [dva roky po nadobudnutí účinnosti tohto nariadenia].

2. Hostiteľský členský štát agentúry vytvorí [...] podmienky s cieľom zabezpečiť jej riadne fungovanie vrátane dostupnosti miesta, zabezpečenia adekvátnych vzdelávacích zariadení pre deti zamestnancov, vhodného prístupu na trh práce, k sociálnemu zabezpečeniu a zdravotnej starostlivosti pre deti a manželov (manželky).

Článok 42

Administratívna kontrola

Nad činnosťou agentúry dohliada v súlade s článkom 228 ZFEÚ ombudsman.

HLAVA III
RÁMEC CERTIFIKÁCIE KYBERNETICKEJ BEZPEČNOSTI

Článok 43

Európsky rámec certifikácie kybernetickej **bezpečnosti** [...]

1. **Zriaďuje sa európsky rámec certifikácie kybernetickej bezpečnosti s cieľom zlepšiť podmienky fungovania vnútorného trhu zvýšením úrovne kybernetickej bezpečnosti v Únii. Zavádza sa ním správa, ktorou sa umožní harmonizovaný prístup na úrovni EÚ v oblasti európskych systémov certifikácie kybernetickej bezpečnosti s cieľom vytvoriť jednotný digitálny trh pre procesy, produkty a služby IKT.**

2. **Európskym rámcom certifikácie kybernetickej bezpečnosti sa vymedzí mechanizmus zriadenia** [...] európskych systém**ov** [...] certifikácie kybernetickej bezpečnosti a osvedčovania, že **procesy**, produkty a služby IKT [...] **vyhodnotené** v rámci týchto systémov spĺňajú špecifikované **bezpečnostné** požiadavky [...] s **cieľom [...] chrániť** dostupnosť, pravosť, integritu a dôvernosť uložených, prenášaných alebo spracúvaných údajov alebo funkcií či služieb, ktoré sa cez tieto produkty, procesy, a služby [...] ponúkajú alebo sprístupňujú, a to **počas ich celého životného cyklu.**

Článok 44

Vypracovanie a prijatie európskeho systému certifikácie kybernetickej bezpečnosti

1. Agentúra ENISA na žiadosť Komisie **alebo európskej skupiny pre certifikáciu kybernetickej bezpečnosti („skupina“) zriadenej podľa článku 53** vypracuje kandidátsky európsky systém certifikácie kybernetickej bezpečnosti, ktorý spĺňa požiadavky stanovené v článkoch 45, 46 a 47 tohto nariadenia.[...]

1a. Prípravu kandidátskeho európskeho systému certifikácie kybernetickej bezpečnosti môžu skupine navrhnúť členské štáty alebo organizácie zainteresovaných strán. Skupina posúdi takéto návrhy na základe kritérií, ktoré sama vymedzí prostredníctvom usmernení v súlade s článkom 53 ods. 3 písm. ca), a o prípravu kandidátskeho európskeho systému certifikácie kybernetickej bezpečnosti môže požiadať agentúru ENISA.

2. Pri vypracúvaní kandidátskeho systému podľa odseku 1 tohto článku sa agentúra ENISA radí **prostredníctvom transparentných konzultačných procesov** so všetkými relevantnými zainteresovanými stranami a úzko spolupracuje so skupinou. Skupina poskytuje agentúre ENISA pomoc a odborné poradenstvo [...] v súvislosti s prípravou kandidátskeho systému a **pred jeho predložením Komisii prijme k nemu stanovisko** [...]. **Agentúra ENISA zabezpečuje, že kandidátske systémy sú v súlade s uplatniteľnou harmonizovanou normou používanou na akreditáciu orgánu posudzovania zhody.**

3. Agentúra ENISA **pred predložením** [...] kandidátskeho [...] systému pripraveného podľa odseku 2 tohto článku Komisii v **čo najväčšej miere zohľadňuje stanovisko skupiny.**

4. Komisia môže na základe kandidátskeho systému navrhnutého agentúrou ENISA prijať vykonávacie akty v súlade s článkom 55 ods. 2, v ktorých sa stanovia európske systémy certifikácie kybernetickej bezpečnosti **procesov**, produktov a služieb IKT, ktoré spĺňajú požiadavky článkov 45, 46 a 47 tohto nariadenia.

5. [...]

Článok 44a

Údržba európskeho systému certifikácie kybernetickej bezpečnosti

1. Agentúra udržiava osobitnú webovú stránku, ktorá obsahuje informácie o európskych systémoch certifikácie kybernetickej bezpečnosti, certifikátoch a vyhláseniach o zhode EÚ vydaných podľa článku 47a a propraguje ich.

2. Agentúra v úzkej spolupráci so skupinou aspoň každých päť rokov preskúma prijaté európske systémy certifikácie kybernetickej bezpečnosti, pričom berie do úvahy spätnú väzbu zainteresovaných strán. Ak sa to bude považovať za potrebné, Komisia alebo skupina môžu požiadať agentúru, aby začala proces vypracovania revidovaného kandidátskeho systému v súlade s článkom 44 ods. 2 a 3.

Článok 45

Bezpečnostné ciele európskych systémov certifikácie kybernetickej bezpečnosti

Európsky systém certifikácie kybernetickej bezpečnosti musí byť navrhnutý tak, aby podľa potreby [...] **plnil aspoň** tieto bezpečnostné ciele:

a) chrániť uložené, prenášané alebo inak spracúvané údaje pred neúmyselným či neoprávneným ukladaním, spracovaním, prístupom alebo únikom **počas celého životného cyklu procesu, produktu alebo služby;**

b) chrániť uložené, prenášané alebo inak spracúvané údaje pred neúmyselným či neoprávneným zničením, [...] stratou alebo pozmenením alebo nedostatočnou dostupnosť **počas celého životného cyklu procesu, produktu alebo služby;**

c) [...] oprávnené osoby, programy alebo zariadenia môžu mať prístup výlučne k tým údajom, službám alebo funkciám, na ktoré sa vzťahujú ich prístupové práva;

d) zaznamenávať, ktoré údaje, funkcie alebo služby [...] **boli predmetom prístupu, použité alebo inak spracované**, kedy a kým;

e) [...] možnosť overiť, ktoré údaje, funkcie alebo služby [...] boli predmetom prístupu, použité **alebo inak spracované**, kedy a kým;

f) v prípade fyzického alebo technického incidentu promptne obnoviť dostupnosť údajov, služieb a funkcií a prístup k nim;

g) [...] **procesy**, produkty a služby IKT sa poskytujú aktualizovaným softvérom a **hardvérom** [...] bez **verejne známych** bezpečnostných dier a využívajú mechanizmy na bezpečnú [...] aktualizáciu.

ga) procesy, produkty a služby IKT sa vyvíjajú, vyrábajú a dodávajú v súlade s bezpečnostnými požiadavkami uvedenými v konkrétnom systéme.

Článok 46

Stupne dôveryhodnosti európskych systémov certifikácie kybernetickej bezpečnosti

1. Európsky systém certifikácie kybernetickej bezpečnosti môže pre **procesy**, produkty a služby IKT [...] uvádzať jeden alebo viacero z týchto stupňov dôveryhodnosti: základný, pokročilý a/alebo vysoký. **Stupeň dôveryhodnosti zodpovedá úrovni rizika spojeného s plánovaným využitím daného procesu, produktu alebo služby IKT.**

2. Základný, pokročilý a vysoký [...] **stupeň dôveryhodnosti odkazujú na certifikát alebo vyhlásenie o zhode EÚ vydané v rámci európskeho systému certifikácie kybernetickej bezpečnosti, v ktorom sa pre každý stupeň dôveryhodnosti ustanovujú bezpečnostné požiadavky vrátane bezpečnostných funkcií a zodpovedajúca úroveň úsilia pri hodnotení procesu, produktu alebo služby IKT. Certifikát alebo vyhlásenie o zhode EÚ je charakterizované odkazom na s ním súvisiace technické špecifikácie, normy a postupy vrátane technických kontrol, ktorých účelom je takéto znižovanie rizika alebo prevencia kybernetických bezpečnostných incidentov:**

a) **európsky certifikát kybernetickej bezpečnosti alebo vyhlásenie o zhode EÚ, v ktorom sa odkazuje na** základný stupeň dôveryhodnosti **predstavuje uistenie, že procesy, produkty a služby IKT spĺňajú príslušné bezpečnostné požiadavky vrátane bezpečnostných funkcií a boli vyhodnotené na úrovni, ktorej cieľom je minimalizovať známe základné riziká kybernetických incidentov a kybernetických útokov. Hodnotiace činnosti zahŕňajú aspoň preskúmanie technickej dokumentácie alebo, keď to neprichádza do úvahy, náhradné činnosti s rovnocenným účinkom** [...];

b) **európsky certifikát kybernetickej bezpečnosti, v ktorom sa odkazuje na** pokročilý stupeň dôveryhodnosti predstavuje **uistenie, že procesy, produkty a služby IKT spĺňajú príslušné bezpečnostné požiadavky vrátane bezpečnostných funkcií a boli vyhodnotené na úrovni, ktorej cieľom je minimalizovať známe kybernetické riziká, kybernetické incidenty a kybernetické útoky, ktoré vykonávajú subjekty s obmedzenými zručnosťami a zdrojmi. Hodnotiace činnosti zahŕňajú minimálne: preskúmanie nevyužiteľnosti verejne známych bezpečnostných dier a skúšku, či procesy, produkty alebo služby IKT správne vykonávajú potrebné bezpečnostné funkcie; alebo náhradné činnosti s rovnocenným účinkom, ak uvedené činnosti neprichádzajú do úvahy** [...];

c) **európsky certifikát kybernetickej bezpečnosti, v ktorom sa odkazuje na** vysoký stupeň dôveryhodnosti predstavuje **uistenie, že procesy, produkty a služby IKT spĺňajú príslušné bezpečnostné požiadavky vrátane bezpečnostných funkcií a boli vyhodnotené na úrovni, ktorej cieľom je minimalizovať riziko najpokročilejších kybernetických útokov, ktoré vykonávajú subjekty so značnými zručnosťami a zdrojmi. Hodnotiace činnosti zahŕňajú minimálne: preskúmanie nevyužiteľnosti verejne známych bezpečnostných dier, skúšku, či procesy, produkty alebo služby IKT správne vykonávajú najpokročilejšie potrebné bezpečnostné funkcie, a posúdenie ich odolnosti proti zručným útočníkom prostredníctvom penetračného testu;** alebo **náhradné činnosti s rovnocenným účinkom, ak uvedené činnosti neprichádzajú do úvahy** [...].

2a. Európsky systém certifikácie kybernetickej bezpečnosti môže špecifikovať viaceré úrovne hodnotenia v závislosti od prísnosti a hĺbky metodiky hodnotenia. Každá z úrovní hodnotenia musí zodpovedať jednému zo stupňov dôveryhodnosti a byť vymedzená vhodnou kombináciou zložiek dôveryhodnosti.

Článok 47

Prvky európskych systémov certifikácie kybernetickej bezpečnosti

1. Európsky systém certifikácie kybernetickej bezpečnosti musí zahŕňať **minimálne** tieto prvky:

a) predmet úpravy a rozsah pôsobnosti **systému** certifikácie vrátane typu alebo kategórií **procesov**, produktov a služieb IKT, **ako aj informácií o tom, ako systém certifikácie plní potreby očakávaných cieľových skupín;**

b) [...] odkaz [...] na medzinárodné, **európske [...] alebo vnútroštátne** normy **používané pri hodnotení. Ak normy nie sú k dispozícii, uvedie sa odkaz na** [...] **technické špecifikácie, ktoré spĺňajú požiadavky prílohy II k nariadeniu č. 1025/2012, alebo, ak tieto nie sú k dispozícii, na technické špecifikácie alebo iné požiadavky kybernetickej bezpečnosti vymedzené v systéme;**

c) podľa potreby jeden alebo viacero stupňov dôveryhodnosti;

ca) prípadné osobitné alebo dodatočné požiadavky na orgány posudzovania zhody s cieľom zabezpečiť ich technickú spôsobilosť na hodnotenie požiadaviek v oblasti kybernetickej bezpečnosti;

d) konkrétne použité hodnotiace kritériá a metódy vrátane typov hodnotenia s cieľom preukázať, že sa dosiahli konkrétne ciele uvedené v článku 45;

e) **prípadné** informácie, ktoré má orgánom posudzovania zhody poskytnúť **alebo inak sprístupniť** žiadateľ a ktoré sú potrebné na certifikáciu;

f) ak systém zahŕňa označenia alebo značky, podmienky, za ktorých možno takéto označenia alebo značky použiť;

g) [...] pravidlá monitorovania súladu s požiadavkami certifikátov **alebo vyhlásenia o zhode EÚ** vrátane mechanizmov na preukázanie trvalého súladu so stanovenými kybernetickobezpečnostnými požiadavkami;

h) prípadné podmienky udelenia a **obnovenia certifikátu, ako aj** zachovania, pokračovania, rozšírenia **alebo** zúženia jeho rozsahu pôsobnosti;

i) pravidlá týkajúce sa dôsledkov v prípade nesúladu certifikovaných **alebo vlastným posúdením posúdených** produktov a služieb IKT s [...] požiadavkami systému;

j) pravidlá nahlasovania a riešenia predtým nezistených zraniteľných miest **procesov**, produktov a služieb IKT z hľadiska kybernetickej bezpečnosti;

k) **prípadné** pravidlá uchovávania záznamov orgánmi posudzovania zhody;

l) určenie vnútroštátnych **alebo medzinárodných** systémov certifikácie kybernetickej bezpečnosti, ktoré sa vzťahujú na rovnaký typ alebo kategóriu **procesov**, produktov a služieb IKT, **bezpečnostných požiadaviek a kritérií a metód hodnotenia**;

m) obsah vydaného certifikátu **alebo vyhlásenia o zhode EÚ;**

ma) dobu, po ktorú výrobca alebo poskytovateľ produktov alebo služieb IKT uchováva vyhlásenia o zhode EÚ a technickú dokumentáciu so všetkými relevantnými informáciami;

mb[...]) maximálna doba platnosti certifikátov;

mc[...]) politika zverejňovania informácií o udelených, zmenených a odobratých certifikátoch;

md[...]) podmienky vzájomného uznávanie systémov certifikácie s tretími krajinami;

me[...]) prípadné pravidlá týkajúce sa mechanizmu partnerského preskúmania v prípade orgánov vydávajúcich európske certifikáty kybernetickej bezpečnosti pre vysoký stupeň dôveryhodnosti [...] podľa článku 48 ods. 4a.

2. Stanovené požiadavky daného systému nesmú byť v rozpore so žiadnymi platnými zákonnými požiadavkami, najmä s požiadavkami, ktoré vyplývajú z harmonizovanej legislatívy Únie.

3. Ak sa to stanovuje v osobitnom akte Únie, certifikáciu **alebo vyhlásenie o zhode EÚ** v rámci európskeho systému certifikácie kybernetickej bezpečnosti možno použiť na preukázanie predpokladu zhody s požiadavkami daného aktu.

4. Ak harmonizovaná legislatíva Únie absentuje, vo vnútroštátnom práve členských štátov sa zároveň môže stanoviť, že európsky systém certifikácie kybernetickej bezpečnosti možno použiť na určenie predpokladu zhody so zákonnými požiadavkami.

Článok 47a

Vlastné posúdenie zhody

1. Európsky systém certifikácie kybernetickej bezpečnosti môže povoliť vykonávanie posudzovania zhody na výhradnú zodpovednosť výrobcu alebo poskytovateľa produktov a služieb IKT. Takéto posudzovanie zhody sa uplatňuje iba na produkty a služby IKT s nízkym rizikom, ktoré zodpovedá základnému stupňu dôveryhodnosti.

2. Výrobca alebo dodávateľ produktov a služieb IKT môže vydať vyhlásenie o zhode EÚ, ktorým potvrdí, že sa preukázalo splnenie požiadaviek stanovených v systéme. Vydaním takéhoto vyhlásenia výrobcu alebo poskytovateľ produktov a služieb IKT preberá zodpovednosť za súlad produktu alebo služby IKT s požiadavkami stanovenými systémom.

3. Výrobca alebo poskytovateľ produktov a služieb IKT ponecháva vyhlásenie o zhode EÚ a technickú dokumentáciu všetkých relevantných informácií týkajúcich sa zhody produktov alebo služieb IKT so systémom k dispozícii vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti uvedenému v článku 50 ods. 1 počas obdobia vymedzeného v príslušnom európskom systéme certifikácie kybernetickej bezpečnosti. Kópia vyhlásenia o zhode EÚ sa predloží vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti a agentúre ENISA.

4. Vydanie vyhlásenie o zhode EÚ je dobrovoľné, pokiaľ nie je ustanovené inak v práve Únie alebo v práve členských štátov.

5. Vyhlásenie o zhode EÚ vydané podľa tohto článku sa uznáva vo všetkých členských štátoch.

Článok 48

Certifikácia kybernetickej bezpečnosti

1. **Procesy**, produkty a služby IKT certifikované v rámci európskeho systému certifikácie kybernetickej bezpečnosti prijatého podľa článku 44 sa považujú za vyhovujúce požiadavkám daného systému.

2. Pokiaľ sa v práve Únie **alebo práve členských štátov** nestanovuje inak, certifikácia je dobrovoľná.

3. Európsky certifikát kybernetickej bezpečnosti podľa tohto článku, **ktorý odkazuje na základný alebo pokročilý stupeň dôveryhodnosti**, vydávajú orgány posudzovania zhody uvedené v článku 51 na základe kritérií zahrnutých v európskom systéme certifikácie kybernetickej bezpečnosti prijatom podľa článku 44.

4. Odchylne [...] od odseku 3 sa v riadne odôvodnených prípadoch môže v konkrétnom európskom systéme certifikácie kybernetickej bezpečnosti určiť, že výsledný európsky certifikát kybernetickej bezpečnosti môže vydať len verejný orgán. Ide o jeden z týchto **[...]** orgánov:

a) vnútroštátny orgán pre [...] certifikáciu **kybernetickej bezpečnosti** uvedený v článku 50 ods. 1;

b) orgán **verejnej moci** akreditovaný ako orgán posudzovania zhody podľa článku 51 ods. 1 [...]

c) [...]

4a. Ak európsky systém certifikácie kybernetickej bezpečnosti podľa článku 44 vyžaduje vysoký stupeň dôveryhodnosti, certifikát môže vydať iba vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti uvedený v článku 50 ods. 1 alebo orgán posudzovania zhody uvedený v článku 51, a to za týchto podmienok:

a) na základe predchádzajúceho schválenia každého jednotlivého certifikátu, ktorý vydal orgán posudzovania zhody, zo strany daného vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti; alebo

b) po predchádzajúcom všeobecnom delegovaní tejto úlohy na orgán posudzovania zhody zo strany vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti.

5. Fyzická či právnická osoba, ktorá podrobuje svoje **procesy**, produkty alebo služby IKT mechanizmu certifikácie, [...] **sprístupní** orgánu posudzovania zhody uvedenému v článku 51 **alebo vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti uvedenému v článku 50** [...], **ak je tento orgán orgánom vydávajúcim certifikát**, všetky informácie potrebné pre postup certifikácie.

5a. Držiteľ certifikátu informuje orgán, ktorý certifikát vydal, o všetkých neskoršie zistených bezpečnostných dierach alebo nezrovnalostiach týkajúcich sa bezpečnosti certifikovaného procesu, produktu alebo služby IKT, ktoré môžu mať vplyv na požiadavky týkajúce sa certifikácie. Orgán bezodkladne postúpi tieto informácie vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti.

6. Certifikáty sa vydávajú na [...] **obdobie vymedzené v príslušnom systéme certifikácie**, pričom ich možno obnoviť, [...] pokiaľ sa naďalej plnia relevantné požiadavky.

7. Európsky certifikát kybernetickej bezpečnosti vydaný podľa tohto článku sa uzná vo všetkých členských štátoch.

Článok 49

Vnútroštátne systémy certifikácie a certifikáty kybernetickej bezpečnosti

1. Bez toho, aby bol dotknutý odsek 3, strácajú vnútroštátne systémy certifikácie kybernetickej bezpečnosti a súvisiace postupy pre **procesy**, produkty a služby IKT, na ktoré sa vzťahuje európsky systém certifikácie kybernetickej bezpečnosti, účinok k dátumu stanovenému vo vykonávacom akte prijatom podľa článku 44 ods. 4. Existujúce vnútroštátne systémy certifikácie kybernetickej bezpečnosti a súvisiace postupy pre **procesy**, produkty a služby IKT, na ktoré sa žiaden európsky systém certifikácie kybernetickej bezpečnosti nevzťahuje, existujú naďalej.

2. Členské štáty nesmú zavádzať nové vnútroštátne systémy certifikácie kybernetickej bezpečnosti tých **procesov**, produktov a služieb IKT, na ktoré sa vzťahuje platný európsky systém certifikácie kybernetickej bezpečnosti.

3. Existujúce certifikáty vydané na základe vnútroštátnych systémov certifikácie kybernetickej bezpečnosti, na **ktoré sa súčasne vzťahuje európsky systém certifikácie kybernetickej bezpečnosti**, platia naďalej až do konca ich platnosti.

Článok 50

Vnútroštátne orgány [...] ***pre certifikáciu*** **kybernetickej bezpečnosti**

1. Každý členský štát **určí [...] jeden alebo viacero** vnútroštátnych orgánov pre certifikáciu [...] **kybernetickej bezpečnosti na jeho území alebo, po vzájomnej dohode s iným členským štátom, jeden alebo viacero orgánov zriadených v danom inom členskom štáte, ktoré budú zodpovedné za dohľad v určujúcom členskom štáte.**

2. Každý členský štát oznámi Komisii určené orgány **[...] a úlohy, ktoré im boli zverené.**

3. **Bez toho, aby bol dotknutý článok 48 ods. 4 písm. a) a článok 48 ods. 4a**, [...] každý vnútroštátny dozorný pre [...] certifikáciu **kybernetickej bezpečnosti** je nezávislý od subjektov, na ktoré dohliada, pokiaľ ide o jeho organizáciu, rozhodnutia o financovaní, právnu štruktúru a rozhodovanie.

3a. Členské štáty zabezpečia, aby činnosti vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti týkajúce sa vydávania certifikátov v súlade s článkom 48 ods. 4 písm. a) a článkom 48 ods. 4a boli prísne oddelené, pokiaľ ide o úlohy a povinnosti, od činností dohľadu uvedených v tomto článku, a aby obe činnosti fungovali nezávisle od seba.

4. Členské štáty zabezpečia, aby vnútroštátne orgány pre [...] certifikáciu **kybernetickej bezpečnosti** mali primerané zdroje na výkon svojich právomocí a aby zverené úlohy vykonávali účinne a efektívne.

5. V záujme účinného vykonávania tohto nariadenia je vhodné, aby sa tieto orgány aktívne, efektívne, účinne a bezpečne zapájali do práce európskej skupiny pre certifikáciu kybernetickej bezpečnosti zriadenej podľa článku 53.

6. Vnútroštátne orgány pre [...] certifikáciu **kybernetickej bezpečnosti**:

a) [...]

aa) monitorujú a presadzujú povinnosti výrobcu alebo poskytovateľa produktov a služieb IKT usadeného na ich príslušných územiach stanovené v článku 47a ods. 2 a 3 a v príslušnom európskom systéme certifikácie kybernetickej bezpečnosti;

b) [...] **bez toho, aby bol dotknutý článok 51 ods. 1b, pomáhajú vnútroštátnym akreditačným orgánom pri monitorovaní** činností orgánov posudzovania zhody a **dohliadaní na tieto činnosti** na účely tohto nariadenia [...];

ba) monitorujú činnosti subjektov uvedených v článku 48 ods. 4 a dohliadajú na tieto činnosti;

bb) splnomocňujú orgány posudzovania zhody uvedené v článku 51 ods. 1b a obmedzujú, pozastavujú alebo odoberajú existujúce splnomocnenia v prípade nesúladu s požiadavkami tohto nariadenia;

c) vybavujú sťažnosti fyzických alebo právnických osôb v súvislosti s certifikátmi, ktoré vydal [...] **vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti alebo, v súlade s článkom 48 ods. 4a, orgány posudzovania zhody**, primerane prešetrujú predmet danej sťažnosti a sťažovateľa v primeranej lehote informujú o pokroku a výsledku tohto prešetrenia;

d) spolupracujú s ostatnými vnútroštátnymi orgánmi pre [...] certifikáciu kybernetickej bezpečnosti alebo ďalšími verejnými orgánmi vrátane poskytovania informácií o možnom nesúlade **procesov**, produktov a služieb IKT s požiadavkami tohto nariadenia alebo konkrétnych európskych systémov certifikácie kybernetickej bezpečnosti;

e) monitorujú relevantné trendy vo sfére certifikácie kybernetickej bezpečnosti.

7. Každý vnútroštátny orgán [...] pre certifikáciu **kybernetickej bezpečnosti** má minimálne tieto právomoci:

a) žiadať od orgánov posudzovania zhody, [...] držiteľov európskych certifikátov kybernetickej bezpečnosti a **vydavateľov vyhlásenia o zhode EÚ** akékoľvek informácie, ktoré potrebuje na plnenie svojich úloh;

b) viesť vyšetrovanie v podobe auditov orgánov posudzovania zhody, [...] držiteľov európskych certifikátov kybernetickej bezpečnosti a **vydavateľov vyhlásenia o zhode EÚ** na overenie súladu s ustanoveniami hlavy III;

c) prijímať primerané opatrenia v súlade s vnútroštátnym právom na zaistenie súladu orgánov posudzovania zhody, [...] držiteľov certifikátov a **vydavateľov vyhlásenia o zhode EÚ** s týmto nariadením alebo európskym systémom certifikácie kybernetickej bezpečnosti;

d) získať prístup do akýchkoľvek priestorov orgánov posudzovania zhody a držiteľov európskych certifikátov kybernetickej bezpečnosti na účely vyšetrovania v súlade s procesným právom Únie alebo daného členského štátu;

e) v súlade s vnútroštátnym právom odoberať certifikáty, ktoré vydal **vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti alebo, v súlade s článkom 48 ods. 4a, orgány posudzovania zhody**, ktoré nie sú v súlade s týmto nariadením alebo európskym systémom certifikácie kybernetickej bezpečnosti;

f) ukladať sankcie v zmysle článku 54 v súlade s vnútroštátnym právom a vyžadovať okamžité ukončenie porušovania povinností stanovených v tomto nariadení.

8. Vnútroštátne orgány pre [...] certifikáciu kybernetickej bezpečnosti navzájom i s Komisiou spolupracujú, a najmä si vymieňajú informácie, skúsenosti a osvedčené postupy v oblasti certifikácie kybernetickej bezpečnosti a technických otázok súvisiacich s kybernetickou bezpečnosťou **procesov**, produktov a služieb IKT.

Článok 51

Orgány posudzovania zhody

1. Orgány posudzovania zhody akredituje vnútroštátny akreditačný orgán vymenovaný podľa nariadenia (ES) č. 765/2008, iba ak spĺňajú požiadavky stanovené v prílohe k tomuto nariadeniu.

1a. V prípadoch, keď vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti vydal v súlade s článkom 48 ods. 4 písm. a) a článkom 48 ods. 4a európsky certifikát kybernetickej bezpečnosti, certifikačný orgán vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti sa akredituje orgán posudzovania zhody podľa odseku 1 tohto článku.

1b. V prípade potreby vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti splnomocní orgány posudzovania zhody na vykonávanie jeho úloh, ak spĺňajú osobitné alebo dodatočné požiadavky stanovené v európskom systéme certifikácie podľa článku 47 ods. 1 písm. ca).

2. Akreditácia sa udeľuje najviac na päť rokov a možno ju obnoviť za rovnakých podmienok, pokiaľ orgán posudzovania zhody spĺňa požiadavky stanovené v tomto článku. Akreditačné orgány **prijmú v primeranom časovom rámci všetky vhodné opatrenia s cieľom obmedziť, pozastaviť** alebo odňať orgánu posudzovania zhody akreditáciu v zmysle odseku 1 tohto článku, ak nie sú alebo prestanú byť splnené akreditačné podmienky, alebo ak daný orgán svojím konaním porušuje toto nariadenie.

Článok 52

Oznamovanie

1. Pri každom európskom systéme certifikácie kybernetickej bezpečnosti prijatom podľa článku 44 vnútroštátne orgány pre [...] certifikáciu kybernetickej bezpečnosti oznámia Komisii orgány posudzovania zhody, ktoré sú [...] a **prípadne splnomocnené podľa článku 51 ods. 1b** na vydávanie certifikátov pri určených stupňoch dôveryhodnosti v zmysle článku 46, a bezodkladne aj akékoľvek následné zmeny v tomto smere.

2. Rok po nadobudnutí účinnosti každého európskeho systému certifikácie kybernetickej bezpečnosti Komisia v úradnom vestníku uverejní zoznam oznámených orgánov posudzovania zhody.

3. Ak Komisia dostane oznámenie po lehote stanovenej v odseku **2** [...], v *Úradnom vestníku Európskej únie* uverejní zmeny zoznamu uvedeného v odseku 2 do dvoch mesiacov od prijatia daného oznámenia.

4. Vnútroštátny orgán pre [...] certifikáciu **kybernetickej bezpečnosti** môže Komisii predložiť žiadosť o vyňatie niektorého orgánu posudzovania zhody, ktorý daný vnútroštátny orgán dohľadu nad certifikáciou oznámil, zo zoznamu uvedeného v odseku 2 tohto článku. Komisia v *Úradnom vestníku Európskej únie* uverejní príslušné zmeny zoznamu do jedného mesiaca od prijatia predmetnej žiadosti vnútroštátneho orgánu pre [...] certifikáciu **kybernetickej bezpečnosti**

5. Komisia môže vo vykonávacích aktoch vymedziť okolnosti, formáty a postupy oznamovania uvedeného v odseku 1 tohto článku. Dané vykonávacie akty sa prijmú v súlade s postupom preskúmania uvedeným v článku 55 ods. 2.

Článok 53

Európska skupina pre certifikáciu kybernetickej bezpečnosti

1. Zriadi sa európska skupina pre certifikáciu kybernetickej bezpečnosti (ďalej len „skupina“).

2. Skupina sa skladá zo **zástupcov** vnútroštátnych orgánov pre [...] certifikáciu **kybernetickej bezpečnosti alebo zástupcov iných príslušných vnútroštátnych orgánov.** [...] **Každý člen skupiny môže zastupovať najviac jeden ďalší členský štát.**

3. Skupina má tieto úlohy:

a) radiť a pomáhať Komisii v jej úsilí o zabezpečenie konzistentného vykonávania a uplatňovania tejto hlavy, najmä z hľadiska politických otázok spojených s certifikáciou kybernetickej bezpečnosti, koordinácie politických prístupov a vypracovania európskych systémov certifikácie kybernetickej bezpečnosti;

b) radiť a pomáhať agentúre ENISA a spolupracovať s ňou pri vypracúvaní kandidátskych systémov v súlade s článkom 44 tohto nariadenia;

ba) prijať stanovisko o kandidátskom systéme podľa článku 44 tohto nariadenia;

c) [...] **požiadať** agentúru o vypracovanie kandidátskeho európskeho systému certifikácie kybernetickej bezpečnosti v súlade s článkom 44 tohto nariadenia;

ca) vypracovať a prijať usmernenia týkajúce sa kritérií posudzovania návrhov na prípravu kandidátskeho systému predložených [...] skupine podľa článku 44 (1a);

d) prijímať stanoviská pre Komisiu k udržiavaniu a prehodnocovaniu existujúcich európskych systémov certifikácie kybernetickej bezpečnosti;

e) skúmať relevantné trendy vo sfére certifikácie kybernetickej bezpečnosti a vymieňať si osvedčené postupy v oblasti systémov certifikácie kybernetickej bezpečnosti;

f) uľahčovať spoluprácu medzi vnútroštátnymi orgánmi pre [...] certifikáciu **kybernetickej bezpečnosti** podľa tejto hlavy **budovaním kapacít**, výmenou informácií, najmä vytvorením metód efektívnej výmeny informácií o všetkých otázkach spojených s certifikáciou kybernetickej bezpečnosti**;**

fa) podporovať vykonávanie mechanizmu partnerského preskúmania medzi orgánmi v súlade s pravidlami stanovenými v európskom systéme certifikácie kybernetickej bezpečnosti podľa článku 47 ods. 1 písm. md) tohto nariadenia.

4. Skupine **ako moderátor** predsedá a jej sekretariát zabezpečuje Komisia za pomoci agentúry ENISA v zmysle článku 8 písm. a).

Článok 53a

***Právo podať sťažnosť na vnútroštátny orgán pre [...] certifikáciu* kybernetickej bezpečnosti**

1. Fyzické osoby alebo právnické osoby majú právo podať sťažnosť na vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti v súvislosti s certifikátom, ktorý vydal tento orgán alebo, v súlade s článkom 48 ods. 4a, orgány posudzovania zhody.

2. Vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti, na ktorom sa sťažnosť podala, informuje sťažovateľa o pokroku a výsledku sťažnosti vrátane možnosti uplatnenia súdneho prostriedku nápravy podľa článku 53b.

Článok 53b

Právo na účinný súdny prostriedok nápravy

1. Fyzické alebo právnické osoby majú právo na účinný súdny prostriedok nápravy voči právne záväznému rozhodnutiu vnútroštátneho orgánu pre certifikáciu kybernetickej bezpečnosti, ktoré sa ich týka.

2. Fyzické alebo právnické osoby majú právo na účinný súdny prostriedok nápravy, ak vnútroštátny orgán pre certifikáciu kybernetickej bezpečnosti sťažnosť nevybavuje.

3. Návrh na začatie konania proti vnútroštátnemu orgánu pre certifikáciu kybernetickej bezpečnosti sa podáva na súdoch členského štátu, v ktorom má orgán sídlo.

Článok 54

Sankcie

Členské štáty stanovia pravidlá sankcionovania porušení ustanovení tejto hlavy a európskych systémov certifikácie kybernetickej bezpečnosti a prijmú všetky potrebné opatrenia na zaistenie ich uplatňovania. Stanovené sankcie musia byť účinné, primerané a odrádzajúce. Členské štáty [do .../bezodkladne] oznámia uvedené pravidlá a opatrenia Komisii a informujú ju o všetkých následných zmenách, ktoré na ne majú vplyv.

HLAVA IV
ZÁVEREČNÉ USTANOVENIA

Článok 55

Postup výboru

1. Komisii pomáha výbor. Tento výbor je výborom v zmysle nariadenia (EÚ) č. 182/2011.

2. Ak sa odkazuje na tento odsek, uplatňuje sa článok 5 **ods. 4 písm. b)** nariadenia (EÚ) č. 182/2011.

Článok 56

Hodnotenie a preskúmanie

1. Najneskôr do piatich rokov od dátumu uvedeného v článku 58 a následne každých päť rokov Komisia posúdi dosah, účinnosť a efektívnosť agentúry a jej pracovných postupov, ako aj prípadnú potrebu upraviť mandát agentúry a finančné dôsledky takýchto prípadných úprav. Pri tomto hodnotení sa zohľadní každá prípadná spätná väzba, ktorú agentúra dostala v nadväznosti na svoje činnosti. Ak sa Komisia domnieva, že existencia agentúry už nie je vzhľadom na jej stanovené ciele, mandát a úlohy odôvodnená, môže navrhnúť zmenu tohto nariadenia z hľadiska ustanovení, ktoré sa týkajú agentúry.

2. V hodnotení sa zároveň posúdi vplyv, účinnosť a efektívnosť ustanovení hlavy III z hľadiska cieľov zaistiť primeranú kybernetickú bezpečnosť produktov a služieb IKT v Únii a zlepšiť fungovanie vnútorného trhu.

3. Komisia predloží hodnotiacu správu spolu s jej závermi Európskemu parlamentu, Rade a správnej rade. Zistenia z hodnotiacej správy sa zverejnia.

Článok 57

Zrušenie a nástupníctvo

1. Nariadenie (ES) č. 526/2013 sa zrušuje s účinnosťou od [….].

2. Odkazy na nariadenie (ES) č. 526/2013 a na agentúru ENISA sa považujú za odkazy na toto nariadenie a na agentúru.

3. Agentúra je nástupcom agentúry, ktorá bola zriadená nariadením (ES) č. 526/2013, pokiaľ ide o vlastníctvo, dohody, právne záväzky, pracovné zmluvy, finančné záväzky a zodpovednosť. Všetky existujúce rozhodnutia správnej rady a výkonnej rady zostávajú v platnosti, pokiaľ nie sú v rozpore s ustanoveniami tohto nariadenia.

4. Agentúra sa zriaďuje na neurčité obdobie od […].

5. Výkonný riaditeľ menovaný podľa článku 24 ods. 4 nariadenia (ES) č. 526/2013 zostáva výkonným riaditeľom agentúry až do konca svojho funkčného obdobia.

6. Členovia správnej rady a ich náhradníci menovaní podľa článku 6 nariadenia (ES) č. 526/2013 zostávajú členmi správnej rady agentúry a náhradníkmi až do konca svojho funkčného obdobia.

Článok 58

Nadobudnutie účinnosti

1. Toto nariadenie nadobúda účinnosť dvadsiatym dňom po jeho uverejnení v *Úradnom vestníku Európskej únie*.

1a. Toto nariadenie sa uplatňuje od [...] s výnimkou článkov 50, 51, 52, 53a, 53b a 54, ktoré sa začínajú uplatňovať [24 mesiacov po dni jeho uverejnenia v *Úradnom vestníku Európskej únie*].

2. Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Bruseli

Za Európsky parlament	*Za Radu*
predseda	*predseda*

PRÍLOHA

POŽIADAVKY, KTORÉ MUSIA SPĹŇAŤ ORGÁNY POSUDZOVANIA ZHODY

Orgány posudzovania zhody žiadajúce o akreditáciu musia spĺňať tieto požiadavky:

1. Orgán posudzovania zhody je zriadený podľa vnútroštátneho práva a má právnu subjektivitu.

2. Orgán posudzovania zhody je treťou stranou nezávislou od organizácie alebo produktov či služieb IKT, ktoré posudzuje.

3. Ak sa preukáže jeho nezávislosť a absencia konfliktu záujmov, za orgán posudzovania zhody možno považovať subjekt patriaci do obchodného alebo profesijného združenia, ktoré zastupuje podniky zapojené do navrhovania, produkcie, poskytovania, inštalácie, používania alebo údržby produktov alebo služieb IKT, ktoré posudzuje.

4. Orgán posudzovania zhody, jeho vrcholový manažment a zamestnanci zodpovední za výkon úloh posudzovania zhody nesmú byť projektanti, zhotovitelia, dodávatelia, subjekty vykonávajúce inštaláciu alebo údržbu, obstarávatelia, vlastníci ani používatelia posudzovaného produktu alebo služby IKT, ani splnomocnení zástupcovia žiadnej z uvedených strán. To nevylučuje možnosť použitia posudzovaných produktov, ktoré sú potrebné na vykonávanie činností orgánu posudzovania zhody, ani ich použitia na osobné účely.

5. Orgán posudzovania zhody, jeho vrcholový manažment a zamestnanci zodpovední za vykonávanie úloh posudzovania zhody nesmú byť priamo zapojení do navrhovania, zhotovovania alebo výroby, uvádzania na trh, inštalácie, používania alebo údržby príslušných produktov alebo služieb IKT, ani zastupovať osoby zapojené do týchto činností. Nesmú sa podieľať na žiadnych činnostiach, ktoré by mohli ovplyvniť ich nezávislý úsudok alebo bezúhonnosť z hľadiska tých činností posudzovania zhody, v súvislosti s ktorými sú oznámení. Vzťahuje sa to najmä na poradenské služby.

6. Orgány posudzovania zhody zabezpečia, aby činnosti ich dcérskych spoločností alebo subdodávateľov nemali vplyv na dôvernosť, objektivitu a nestrannosť ich činností posudzovania zhody.

7. Orgány posudzovania zhody a ich zamestnanci vykonávajú činnosti posudzovania zhody na najvyššej úrovni profesionálnej čestnosti a požadovanej technickej spôsobilosti v danej oblasti a nesmú podliehať žiadnym tlakom ani stimulom vrátane finančných, ktoré by mohli ovplyvniť ich úsudok alebo výsledky ich činností posudzovania zhody, najmä zo strany osôb alebo skupín osôb, ktoré majú záujem na výsledku týchto činností.

8. Orgán posudzovania zhody musí byť schopný vykonať všetky úlohy posudzovania zhody, ktorými je poverený podľa tohto nariadenia, či už ich vykoná samotný orgán posudzovania zhody niekto iný v jeho mene a na jeho zodpovednosť.

9. Orgán posudzovania zhody má neustále pre každý postup posudzovania zhody a pre každú kategóriu alebo podkategóriu produktov a služieb IKT v potrebnej miere k dispozícii:

a) pracovníkov s odbornými znalosťami a dostatočnými a primeranými skúsenosťami na vykonávanie úloh posudzovania zhody;

b) opisy postupov, podľa ktorých sa vykonáva posudzovanie zhody a ktorými sa zabezpečuje transparentnosť a opakovateľnosť uvedených postupov. Musí mať zavedené vhodné politiky a postupy odlišujúce úlohy, ktoré vykonáva ako oznámený orgán, od ostatných činností;

c) postupy vykonávania činností, ktoré náležite zohľadňujú veľkosť každého podniku, odvetvie, v ktorom podnik pôsobí, jeho štruktúru, stupeň zložitosti technológie daného produktu alebo služby IKT a hromadný či sériový charakter produkčného procesu.

10. Orgán posudzovania zhody musí mať prostriedky potrebné na riadne plnenie technických a administratívnych úloh spojených s posudzovaním zhody, ako aj prístup k všetkým potrebným zariadeniam a vybaveniu.

11. Pracovníci zodpovední za výkon činností posudzovania zhody musia mať:

a) absolvovanú dôkladnú technickú a odbornú prípravu pokrývajúcu všetky príslušné činnosti posudzovania zhody;

b) dostatočné znalosti požiadaviek posudzovaní, ktoré vykonávajú, a primeranú právomoc vykonávať tieto posudzovania;

c) primerané znalosti a pochopenie platných požiadaviek a skúšobných noriem;

d) schopnosť vypracovať certifikáty, záznamy a protokoly preukazujúce, že sa vykonalo posúdenie.

12. Musí byť zaručená nestrannosť orgánov posudzovania zhody, ich vrcholového manažmentu a pracovníkov, ktorí vykonávajú posudzovanie.

13. Odmeňovanie vrcholového manažmentu orgánu na posudzovanie zhody a jeho pracovníkov, ktorí vykonávajú posudzovanie, nesmie závisieť od počtu vykonaných posúdení ani od výsledkov týchto posúdení.

14. Orgány posudzovania zhody musia uzavrieť poistenie zodpovednosti za škodu, ak túto zodpovednosť podľa vnútroštátneho práva nenesie štát, alebo ak nie je za posudzovanie zhody priamo zodpovedný samotný členský štát.

15. Pracovníci orgánu posudzovania zhody sú povinní dodržiavať služobné tajomstvo, pokiaľ ide o všetky informácie získané pri vykonávaní ich úloh podľa tohto nariadenia alebo podľa akéhokoľvek ustanovenia vnútroštátneho práva, ktorým sa vykonáva, nie však vo vzťahu k príslušným orgánom členských štátov, v ktorých daný orgán vykonáva svoju činnosť.

16. Orgány na posudzovanie zhody spĺňajú požiadavky **príslušnej** normy **harmonizovanej podľa nariadenia (ES) č. 765/2008 týkajúcej sa akreditácie orgánov posudzovania zhody, ktoré vykonávajú certifikáciu procesov, produktov alebo služieb**[...].

17. Orgány posudzovania zhody zabezpečia, aby skúšobné laboratóriá používané na účely posudzovania zhody spĺňali požiadavky **príslušnej** normy **harmonizovanej podľa nariadenia (ES) č. 765/2008 týkajúcej sa akreditácie laboratórií, ktoré vykonávajú skúšky**[...].