

SL

SL

SL



EVROPSKA KOMISIJA

Bruselj, 30.9.2010  
COM(2010) 521 konč.

2010/0275 (COD)

Predlog

**UREDBA EVROPSKEGA PARLAMENTA IN SVETA**

**o Evropski agenciji za varnost omrežij in informacij (ENISA)**

{SEC(2010) 1126}

{SEC(2010) 1127}

## OBRAZLOŽITVENI MEMORANDUM

### 1. OZADJE PREDLOGA

#### 1.1. Ozadje politike

Evropska agencija za varnost omrežij in informacij (ENISA) je bila ustanovljena marca 2004 z Uredbo (ES) št. 460/2004<sup>1</sup> sprva za pet let, zagotovila pa naj bi predvsem „visoko in učinkovito raven varnosti omrežij in informacij v [Uniji] in [...] razvoj kulture varnosti omrežij in informacij v korist državljanov, potrošnikov, podjetij in organizacij javnega sektorja Evropske unije, da bi tako prispevala k nemotenemu delovanju notranjega trga“. Z Uredbo (ES) št. 1007/2008<sup>2</sup> je bil njen mandat podaljšan do marca 2012.

S podaljšanjem mandata ENISA leta 2008 se je odprla razprava o splošni usmeritvi evropskih prizadevanj na področju varnosti omrežij in informacij (NIS), ki jo je Komisija podprla z javnim posvetovanjem o možnih ciljih okrepljene politike NIS na ravni Unije. Posvetovanje je potekalo od novembra 2008 do januarja 2009, zbranih pa je bilo skoraj 600 prispevkov<sup>3</sup>.

Komisija je 30. marca 2009 sprejela Sporočilo o zaščiti kritične informacijske infrastrukture<sup>4</sup> (CIIP), v katerem je poudarila, da je treba Evropo pred kibernetскими napadi in prekinitvami zaščititi tako, da se poveča njeno pripravljenost, varnost in odpornosti. Sporočilo vsebuje tudi akcijski načrt, v katerem ima ENISA pomembno vlogo zlasti pri zagotavljanju pomoči državam članicam. Akcijski načrt so močno podprli ministri med razpravo na konferenci o zaščiti kritične informacijske strukture (CIIP), ki je potekala v estonskem Talinu od 27. do 28. aprila 2009<sup>5</sup>. Predsedstvo Evropske unije je v sklepih konference poudarilo, da je pomembno „povečati operativno podporo“ ENISA: ministri so izjavili, da ENISA „predstavlja pomemben instrument za okrepitev prizadevanj za sodelovanje na tem področju po vsej Uniji“, in izpostavili, da je treba mandat agencije vsebinsko in formalno ponovno preučiti, da se bo ta „lahko bolje osredotočila na prednosti in potrebe EU, da bo njena sposobnost reagiranja prožnejša, da bo razvila kvalifikacije in sposobnosti ter povečala operativno učinkovitost in splošni vpliv agencije“, s čimer bi se agenciji zagotovila „stalna sredstva za vsako državo članico kot tudi celotno Evropsko unijo“.

Po razpravi Sveta za telekomunikacije 11. junija 2009, na kateri so države članice podprle, da se zaradi velikega pomena NIS in nastajajočih izzivov na tem področju mandat ENISA podaljša ter povečajo njeni viri, se je razprava pod švedskim predsedovanjem Unije končala. Svet je v resoluciji z dne 18. decembra 2009 o skupnem evropskem pristopu do NIS<sup>6</sup> potrdil

---

<sup>1</sup> Uredba (ES) št. 460/2004 Evropskega Parlamenta in Sveta z dne 10. marca 2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij (UL L 77, 13.3.2004, str. 1).

<sup>2</sup> Uredba (ES) št. 1007/2008 Evropskega parlamenta in Sveta z dne 24. septembra 2008 o spremembi Uredbe (ES) št. 460/2004 Evropskega Parlamenta in Sveta z dne 10. marca 2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij glede njenega trajanja (UL L 293, 31.10.2008, str. 1).

<sup>3</sup> Rezultati javnega posvetovanja „Za okrepljeno politiko varnosti omrežij in informacij v Evropi“ so povzeti v poročilu v Prilogi 11 ocene učinka, ki je priložena temu predlogu.

<sup>4</sup> COM(2009) 149, 30.3.2009.

<sup>5</sup> Dokument za razpravo: [http://www.tallinnciip.eu/doc/discussion\\_paper\\_-\\_tallinn\\_ciip\\_conference.pdf](http://www.tallinnciip.eu/doc/discussion_paper_-_tallinn_ciip_conference.pdf)  
Sklepi predsedstva: [http://www.tallinnciip.eu/doc/EU\\_Presidency\\_Conclusions\\_Tallinn\\_CIIP\\_Conference.pdf](http://www.tallinnciip.eu/doc/EU_Presidency_Conclusions_Tallinn_CIIP_Conference.pdf)

<sup>6</sup> Resolucija Sveta z dne 18. decembra 2009 o skupnem evropskem pristopu do varnosti omrežij in informacij (UL C 321, 29.12.2009, str. 1), <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:C:2009:321:0001:0004:EN:PDF>.

vlogo in potencial ENISA ter potrebo po „*nadaljnem razvoju ENISA v učinkovit organ*“. Poudaril je tudi, da je treba agencijo posodobiti in okrepiti, da bi lahko Komisiji in državam članicam pomagala pri premostitvi razkoraka med tehnologijo in politiko ter bila strokovni center Unije za vprašanja NIS.

## **1.2. Splošno ozadje**

Informacijske in komunikacijske tehnologije (IKT) so postale steber evropskega gospodarstva in družbe kot celote. Dovzetne so za nevarnosti, ki presegajo nacionalne meje in ki se spreminjajo z razvojem tehnologije in trga. Ker imajo IKT svetovno razsežnost ter so med seboj povezane in odvisne od ostale infrastrukture, njihove varnosti in odpornosti ne moremo zagotoviti zgolj z nacionalnimi in neuskkljenimi pristopi. Hkrati je tudi varnost omrežij in informacij podvržena zelo hitrim spremembam. Omrežni in informacijski sistemi morajo biti učinkovito zaščiteni pred vsemi vrstami motenj in izpadi, med drugim tudi pred napadi, ki jih povzročijo človek.

Politike varnosti omrežij in informacij (NIS) imajo v digitalni agendi za Evropo (DAE)<sup>7</sup>, vodilni pobudi strategije EU 2020, osrednjo vlogo, saj bo z njimi mogoče izkoristiti in povečati potencial IKT ter ga pretvoriti v trajnostno rast in inovacije. Spodbujati uvedbo IKT ter povečevati zaupanje v informacijsko družbo sta glavni prednostni nalogi digitalne agende.

ENISA je bila sprva ustanovljena z namenom, da zagotovi visoko in učinkovito varnost omrežij in informacij v Uniji. Izkušnje z agencijo ter izzivi in nevarnosti so še dodatno izpostavili potrebo po posodobitvi njenega mandata, da se bo lahko bolje odzvala na potrebe Evropske unije, nastale zaradi:

- razdrobljenih nacionalnih pristopov za reševanje nastajajočih izzivov;
- pomanjkanja modelov sodelovanja pri izvajanju politik NIS;
- nezadostne pripravljenosti, med drugim tudi zaradi omejene sposobnosti EU za zgodnje opozarjanje in odzivanje;
- pomanjkanja zanesljivih evropskih podatkov in omejenega znanja o nastajajočih težavah;
- majhne ozaveščenosti o tveganjih in izzivih, ki jih prinašajo NIS;
- izzivov pri vključevanju vidikov NIS v politike s ciljem, da se učinkovito prepreči kibernetiski kriminal.

## **1.3. Cilji politike**

Splošni cilj predlagane uredbe je omogočiti Uniji, državam članicam in zainteresiranim stranem, da razvijejo visoko sposobnost reagiranja in pripravljenosti za preprečevanje, odkrivanje in boljše odzivanje na težave, povezane z NIS. Ta bo pomagala vzpostaviti zaupanje v razvoj informacijske družbe, izboljšati konkurenčnost evropskih podjetij in zagotoviti učinkovito delovanje notranjega trga.

---

<sup>7</sup> COM(2010) 245, 19.5.2010.

#### 1.4. Veljavne določbe na področju, na katerega se predlog nanaša

Ta predlog dopolnjuje regulativne in neregulativne pobude politike varnosti omrežij in informacij, ki so bile sprejete na ravni Unije, da se povečata varnost in odpornost IKT:

- Akcijski načrt, ki je bil uveden s Sporočilom o zaščiti kritične informacijske infrastrukture, določa ustanovitvev:
  - (1) Evropskega foruma za države članice (EFMS), ki naj bi pospešil razpravo o dobrih praksah in njihovo izmenjavo, s čimer naj bi se na področju varnosti in odpornosti infrastrukture IKT določili skupni cilji politik in prednostne naloge ter izkoristile neposredne koristi, ki jih agencija zagotavlja s svojim delom in podporo.
  - (2) Evropskega javno-zasebnega partnerstva za odpornost (EP3R) kot prožnega evropskega okvira za upravljanje odpornosti infrastrukture IKT, ki spodbuja sodelovanje med javnim in zasebnim sektorjem pri ciljih, temeljnih zahtevah, dobrih praksah in ukrepih na področju varnosti in odpornosti.
- Stockholmski program, ki ga je 11. decembra 2009 sprejel Evropski svet, podpira ukrepe, ki zagotavljajo varnost omrežij in pri kibernetških napadih v Uniji omogočajo hitrejše ukrepanje.
- Te pobude prispevajo k uresničevanju digitalne agende za Evropo. V delu strategije, ki se osredotoča na povečanje zaupanja in varnosti v informacijski družbi, imajo politike s področja varnosti omrežij in informacij osrednjo vlogo. Prav tako dopolnjujejo podporne ukrepe in politiko Komisije na področju zaščite zasebnosti (zlasti „vgrajene zasebnosti“) in varstva osebnih podatkov (ponovni pregled okvira), omrežje za sodelovanje na področju varstva potrošnikov (CPC), upravljanje identitete in program za varnejši internet.

#### 1.1. 1.5. Razvoj trenutne politike varnosti omrežij in informacij, ki se nanaša na predlog

Podpora in strokovno znanje ENISA koristita trenutnemu razvoju politike NIS na več področjih, zlasti razvoju v okviru digitalne agende za Evropo, tj.:

- krepiti sodelovanje na področju politike NIS z okrepitevijo dejavnosti **Evropskega foruma držav članic (EFMS)**, ki bo z neposredno podporo ENISA pomagal:
  - opredeliti načine za vzpostavitev učinkovite evropske mreže s čezmejnimi sodelovanjem med nacionalnimi/vladnimi skupinami za odzivanje na računalniške grožnje (CERT);
  - opredeliti dolgoročne cilje in prednostne naloge vseevropskih obsežnih vaj za incidente NIS;
  - poostriti minimalne zahteve za javno naročanje, da se povečata varnost in odpornost javnih sistemov in omrežij;
  - opredeliti gospodarske in regulativne pobude za varnost in odpornost;
  - oceniti trenutno stanje NIS v Evropi.

- podpirati **evropsko javno-zasebno partnerstvo za odpornost (EP3R)** ter tako spodbujati sodelovanje in ustanavljanje partnerstev med javnim in zasebnim sektorjem. ENISA ima pri srečanjih in dejavnostih EP3R vedno pomembnejšo vlogo. Faze v okviru EP3R bodo obsegale:
  - razprave o inovativnih ukrepih in instrumentih za izboljšanje varnosti in odpornosti, npr.:
    - (1) o temeljnih zahtevah za varnost in odpornost, zlasti pri javnem naročanju izdelkov ali storitev IKT, da se zagotovijo enaki pogoji in hkrati ustreznost pripravljenosti in preprečevanja;
    - (2) o vprašanjih o odgovornosti gospodarskih subjektov, npr. pri uvedbi minimalnih varnostnih zahtev;
    - (3) o gospodarskih pobudah za razvoj in uvedbo praks za obvladovanje tveganja, varnostnih procesov in izdelkov;
    - (4) o shemah za ocenjevanje in obvladovanje tveganja pri večjih incidentih na podlagi skupnega razumevanja;
    - (5) o sodelovanju med zasebnim in javnim sektorjem pri obsežnih incidentih;
    - (6) o organizaciji **gospodarskega vrha** na temo gospodarskih ovir in gonilnih sil varnosti in odpornosti.
- uporabljati varnostne zahteve regulativnega paketa o elektronskih komunikacijah v praksi, za kar sta potrebna strokovno znanje in podpora ENISA;
  - države članice in Komisijo podpirati pri določanju okvira pravil in postopkov za izvajanje določb o obveščanju pri kršitvah varnosti (člen 13(a) revidirane okvirne direktive) ter pri tem po potrebi upoštevati mnenje zasebnega sektorja;
  - ustanoviti letni forum za nacionalne organe/nacionalne regulativne organe, pristojne za NIS, ter zainteresirane strani iz zasebnega sektorja, na katerem se bo razpravljalo o pridobljenih izkušnjah in izmenjevalo dobrih praks uporabe regulativnih ukrepov za NIS.
- poenostaviti **pripravljalne vaje za kibernetiko po vsej EU** s pomočjo Komisije in sodelovanjem ENISA, da bi se take vaje pozneje lahko razširile na mednarodno raven;
- **ustanoviti CERT (skupine za odzivanje na računalniške grožnje) za institucije EU.** Šesti ključni ukrep digitalne agende za Evropo je, da bo Komisija predstavila „ukrepe, katerih cilj je okrepljena politika varnosti omrežij in informacij na visoki ravni, vključno z [...] ukrepi, ki omogočajo hitrejše odzivanje na kibernetične napade, vključno s skupinami CERT za institucije EU<sup>8</sup>. V ta namen bodo morale Komisije in ostale institucije Unije

---

<sup>8</sup> Svet je v resoluciji z dne 18. decembra 2009 o skupnem evropskem pristopu do varnosti omrežij in informacij prav tako potrdil, da: „Svet [...] priznava [...], da je za ustanovitev skupin za odzivanje na računalniške grožnje v okviru institucij EU treba preučiti strateške učinke, tveganja in možnosti ter opredeliti možno prihodnjo vlogo ENISA na tem področju.“

analizirati in ustanoviti skupino za odzivanje na računalniške grožnje, ENISA pa ji bo lahko zagotovila tehnično podporo in strokovno znanje.

- mobilizirati države članice in jih podpirati pri izpopolnitvi in po potrebi pri ustanovitvi **nacionalnih/vladnih CERT, da se vzpostavi dobro delujoča mreža CERT, ki bo pokrivala vso Evropo**. S to dejavnostjo bo mogoče nadalje razviti evropski sistem za souporabo informacij in opozarjanje (EISAS) za državljane in MSP, ki naj bi bil do konca leta 2012 ustanovljen z nacionalnimi viri in zmogljivostmi.
- **ozaveščati** o izzivih NIS, kar bo obsegalo:
  - sodelovanje Komisije z ENISA pri pripravi osnutka smernic za spodbujanje standardov, dobrih praks in kulture upravljanja tveganja na področju NIS. Pripravljen bo prvi primer smernic.
  - ENISA bo v sodelovanju z državami članicami organizirala **evropski mesec varnosti omrežij in informacij za vse**, v katerem bodo potekala nacionalna/evropska tekmovanja o kibernetiski varnosti.

## 1.6. Usklajenost z drugimi politikami in cilji Unije

Predlog je v skladu z veljavnimi politikami in cilji Evropske unije ter v celoti v skladu s ciljem, da se z izboljšanjem pripravljenosti in odzivnosti na izzive, povezane z varnostjo omrežij in informacij, prispeva k nemotenemu delovanju notranjega trga.

## 2. REZULTATI POSVETOVANJ IN OCENA UČINKA

### 2.1. Posvetovanje z zainteresiranimi stranmi

Ta pobuda politike je rezultat širše razprave, ki je sledila vključujočemu pristopu, pri katerem so se upoštevala načela sodelovanja, odprtosti, odgovornosti, učinkovitosti in medsebojne skladnosti. Širši proces je obsegal tudi ocenjevanje agencije v letu 2006/2007, temu pa so sledila priporočila upravnega odbora ENISA, dve javni posvetovanji (leta 2007 in leta 2008–2009) ter vrsta delavnic o vprašanjih, ki se nanašajo na NIS.

Prvo javno posvetovanje je bilo organizirano v povezavi s Sporočilom Komisije o srednjeročni oceni ENISA. Osredotočalo se je na prihodnost agencije, potekalo pa je od 13. junija do 7. septembra 2007. Na njem je bilo zbranih 44 spletnih in dva pisna prispevka. Odgovore so pripravile zainteresirane strani in zainteresirana javnost, med drugim tudi ministrstva držav članic, regulativni organi, gospodarska združenja in združenja potrošnikov, znanstvene ustanove, podjetja in posamezniki.

V odgovorih so izpostavili vrsto zanimivih vprašanj, ki so se nanašala na pripravo scenarija ogroženosti, potrebo po jasnejši in prožnejši uredbi, ki bi ENISA omogočala, da se prilagodi na izzive, na pomen učinkovitega sodelovanja z zainteresiranimi stranmi in na možnost omejenega povečanja njenih virov.

Na drugem javnem posvetovanju, ki je potekalo od 7. novembra 2008 do 9. januarja 2009, naj bi se opredelili prednostni cilji za okrepljeno politiko NIS na evropski ravni ter sredstva za doseg te ciljev. Organi držav članic, znanstvene/raziskovalne ustanove, gospodarska združenja, zasebna podjetja in druge zainteresirane strani (npr. organizacije in svetovalnice za varstvo podatkov) ter posamezniki so poslali skoraj 600 prispevkov.

Velika večina je v odgovorih<sup>9</sup> podprla podaljšanje mandata agencije ter se zavzela za večjo vlogo agencije pri usklajevanju dejavnosti NIS na evropski ravni ter za povečanje njenih sredstev. Glavne prednostne naloge so bile bolj usklajeno obravnavanje kibernetских napadov v Evropi, mednacionalno sodelovanje pri odzivanju na obsežne kibernetске napade, vzpostavljanje zaupanja in boljša izmenjava informacij med zainteresiranimi stranmi.

V zvezi s predlogom se je septembra 2009 začela opravljati ocena učinka, ki je temeljila na pripravljani študiji zunanjega izvajalca. Pri študiji je sodelovalo več različnih zainteresiranih strani in strokovnjakov. Prispevke so pripravili organi držav članic, pristojni za NIS, nacionalni regulativni organi, telekomunikacijski operaterji, ponudniki internetnih storitev ter ustrezna sektorska združenja, združenja potrošnikov, proizvajalci IKT, skupine za odzivanje na računalniške grožnje (CERT) ter znanstveniki in poslovni uporabniki. V procesu ocene učinka je sodelovala tudi v ta namen ustanovljena medresorska usklajevalna skupina, ki so jo sestavljali predstavniki ustreznih generalnih direktoratsv Komisije.

## 2.2. Ocena učinka

Ohranitev agencije je bila opredeljena kot ustrezna rešitev za doseganje ciljev evropske politike<sup>10</sup>. Po predhodnem pregledu je bilo za nadaljnjo analizo izbranih pet možnosti politik:

- 1. možnost – brez ukrepov;
- 2. možnost – brez sprememb, tj. nadaljevanje s podobnim mandatom in enakimi sredstvi;
- 3. možnost – razširitev nalog ENISA z vključitvijo organov pregona in organov za zaščito zasebnosti kot enakopravnih akterjev;
- 4. možnost – preprečevanje kibernetских napadov in odzivanje na kibernetске incidente kot novi nalogi agencije;
- 5. možnost – pomoč organom pregona in pravosodnim organom pri preprečevanju kibernetskega kriminala kot nova naloga agencije.

Po primerjalni analizi stroškov in koristi je bila tretja možnost opredeljena kot najbolj stroškovno učinkovita in uspešna za doseganje ciljev politike.

Tretja možnost predvideva razširitev vloge ENISE:

- vzpostaviti in vzdrževati povezovalno mrežo med zainteresiranimi stranmi in mrežo znanja, s čimer se bo zagotovilo, da bo ENISA dovolj dobro obveščena o evropskem stanju NIS;
- biti center za podporo NIS pri oblikovanju politike in njenem izvajanju (zlasti na področju e-zasebnosti, e-znaka, e-osebne izkaznice in standardov za javno naročanje za NIS);
- spodbujati politiko Unije na področju zaščite in odpornosti kritične informacijske infrastrukture (vaje, EP3R, evropski sistem za izmenjavo informacij in opozarjanje itn.);
- vzpostaviti okvir Unije za zbiranje podatkov o NIS, vključno s pripravo metod in praks za pravno poročanje in izmenjavo;

---

<sup>9</sup> Glej prilogo XI ocene učinka.

<sup>10</sup> Glej prilogo IV ocene učinka.



- preučevati gospodarske vidike NIS;
- spodbujati sodelovanje s tretjimi državami in mednarodnimi organizacijami, da se izoblikuje skupen svetovni pristop do NIS in vpliva na mednarodne pobude na visoki ravni v Evropi;
- opravljati neoperativne naloge, ki se nanašajo na vidike NIS pri izvrševanju zakonodaje o kibernetnem kriminalu in pravosodnem sodelovanju.

### 3. PRAVNI ELEMENTI PREDLOGA

#### 3.1. Povzetek predlaganega predloga

Predlagana uredba naj bi okrepila in posodobila Evropsko agencijo za varnost omrežij in informacij (ENISA) ter njen mandat podaljšala na pet let.

Predlog vsebuje v primerjavi s prvotno uredbo nekatere bistvene spremembe:

- (1) **Večja prožnost, prilagodljivost in sposobnost za osredotočanje.** Naloge se posodobijo in široko preoblikujejo, da se dejavnostim agencije zagotovi večje področje delovanja; opredelijo se dovolj natančno, da se lahko določijo sredstva, potrebna za doseg ciljev. Tako je poslanstvo agencije bolj opredeljeno, njena sposobnost za doseganje ciljev je večja, naloge, s katerimi podpira izvajanje politike Unije, pa so okrepljene.
- (2) **Boljša prilagoditev agencije politiki in regulativnem postopku Unije.** Agencija lahko pomaga in svetuje evropskim institucijam in organom. To je v skladu s političnim in regulativnim razvojem: Svet agencijo že naslavlja neposredno v resolucijah, Evropski parlament in Svet pa sta agenciji v regulativnem okviru za elektronske komunikacije že dodelila naloge, ki se nanašajo na varnost omrežij in informacij.
- (3) **Vmesnik pri preprečevanju kibernetnega kriminala.** Pri doseganju ciljev agencija upošteva boj proti kibernetnemu kriminalu. Organi pregona in organi za zaščito zasebnosti postanejo enakopravni akterji agencije, zlasti v stalni skupini zainteresiranih strani.
- (4) **Okrepljena upravna struktura.** Predlog določa, da ima upravni odbor agencije, v katerem so zastopane države članice in Komisija, nadzorno funkcijo. Upravni odbor lahko npr. poda splošne usmeritve za kadrovske zadeve, kar je bilo prej v izključni pristojnosti izvršnega direktorja. Lahko ustanovi tudi delovna telesa, ki mu pomagajo pri opravljanju nalog, med drugim tudi pri izvajanju njegovih sklepov.
- (5) **Poenostavitev postopkov.** Postopki, ki so se izkazali za nepotrebno obremenilne, se poenostavijo. Na primer: (a) poenostavljen postopek za sprejetje statuta upravnega odbora, (b) mnenje o programu dela ENISA predložijo službe Komisije, namesto da ga Komisija sprejme s sklepom. Upravnemu odboru se zagotovijo tudi ustrezna sredstva, da lahko po potrebi sprejme izvedbene sklepe in jih izvaja (npr. uslužbenec vložiti pritožbo zoper izvršnega direktorja ali upravni odbor).
- (6) **Postopno povečanje sredstev.** Da bo agencija lahko izpolnila okrepljene evropske prednostne naloge in se odzvala na vedno večje izzive, je treba ne glede na predlog

Komisije za naslednji večletni finančni okvir finančne in kadrovske vire agencije med leti 2012 in 2016 postopno povečevati. Na podlagi predloga uredbe o večletnem finančnem okviru po letu 2013 in ob upoštevanju sklepnih ugotovitev ocene učinka bo Komisija predložila spremenjeno oceno finančnih posledic.

- (7) **Možnost podaljšanja mandata izvršnega direktorja.** Upravni odbor lahko mandat izvršnega direktorja podaljša za tri leta.

### 3.2. Pravna podlaga

Ta predlog temelji na členu 114 Pogodbe o delovanju Evropske unije<sup>11</sup> (PDEU).

Pred začetkom veljavnosti Lizbonske pogodbe je bil v skladu s sodbo Evropskega sodišča<sup>12</sup> **člen 95 Pogodbe ES** ustrezna pravna podlaga za ustanovitev organa, ki naj bi v Uniji zagotavljal visoko in učinkovito raven NIS. Avtorji pogodbe so v členu 95 z izrazom „ukrepi za približevanje“ želeli zakonodajnemu telesu Unije prepustiti diskrecijo pri izbiri ustreznih ukrepov za doseganje zelenega rezultata. Večja varnost in odpornost infrastruktur IKT sta torej pomembni prvini, ki prispevata k nemotenemu delovanju notranjega trga.

Lizbonska pogodba v **členu 114 PDEU**<sup>13</sup> skoraj enako določa pristojnost na področju notranjega trga. Zaradi navedenih razlogov bo to še naprej veljavna pravna podlaga za sprejemanje ukrepov za izboljšanje NIS. Na področju notranjega trga si Unija in države članice delijo pristojnost (člen 4(2)(a) PDEU). To pomeni, da lahko Unija in države članice sprejemajo (zavezujoče) ukrepe in da države članice izvajajo svojo pristojnost, kolikor Unija svoje pristojnosti ne izvaja ali se je odločila, da jo bo prenehala izvajati (člen 2(2) PDEU).

Ukrepi, ki so v pristojnosti notranjega trga, se bodo sprejemali po rednem zakonodajnem postopku (člena 289 in 294 PDEU), ki je podoben<sup>14</sup> prejšnjemu postopku soodločanja (člen 251 Pogodbe ES).

Lizbonska pogodba je odpravila prejšnje razlikovanje med stebri. Preprečevanje in boj proti kriminalu je zdaj v deljeni pristojnosti Unije. S tem je ENISA dobila priložnost, da deluje kot platforma za vidike NIS v boju proti kibernetickemu kriminalu ter da izmenjuje mnenja in najboljše prakse z organi za kibernetično obrambo, izvrševanje zakonodaje in zaščito zasebnosti.

### 3.3. Načelo subsidiarnosti

Predlog je v skladu z načelom subsidiarnosti. Politika NIS zahteva skupen pristop, ciljev predloga pa države članice ne morejo doseči same.

S popolnoma neintervencijsko politiko Unije in nacionalnimi politikami držav članic bi bile naloge prepuščene državam članicam, jasna medsebojna odvisnost obstoječih informacijskih sistemov pa pri tem ne bi bila upoštevana. Ukrep, ki predvideva ustrezno usklajevanje med državami članicami ter tako zagotavlja dobro obvladovanje tveganj NIS v čezmejnem

---

<sup>11</sup> UL C 115, 9.5.2008, str. 94.

<sup>12</sup> Sodišče Evropskih skupnosti, 2.5.2006, C-217/04, Združeno kraljestvo Velika Britanija in Severna Irska proti Parlamentu in Svetu Evropske unije.

<sup>13</sup> Glej zgoraj.

<sup>14</sup> Redni zakonodajni postopek se razlikuje predvsem v večini, ki se zahteva v Svetu in Evropskem parlamentu.

kontekstu, v katerem se pojavljajo, je v skladu z načelom subsidiarnosti. Poleg tega bi evropski ukrep izboljšal učinkovitost obstoječih nacionalnih politik in tako zagotovil dodano vrednost.

Poleg tega bi uvedba usklajene in skupne politike NIS pozitivno vplivala na zaščito temeljnih pravic, zlasti pravico do varstva osebnih podatkov in zasebnosti. Varstvo podatkov je trenutno izredno pomembno, saj evropski državljani podatke vedno – po lastni izbiri ali ker se od njih tako zahteva – vedno pogosteje zaupajo kompleksnim informacijskim sistemom, ne da bi pri tem pravilno ocenili tveganje, ki s tem nastane za varstvo podatkov. Ob incidentih se zato ne bodo mogli ustrezno odzvati. Prav tako ni gotovo, da se bodo države članice brez evropskega usklajevanja NIS lahko učinkovito odzvale na mednarodne incidente.

### **3.4. Načelo sorazmernosti**

Predlog je v skladu z načelom sorazmernosti, saj ne presega tistega, kar je potrebno za doseg cilja.

### **3.5. Izbira instrumentov**

Predlagani instrument: ki se uporablja neposredno v vseh državah članicah.

## **4. POSLEDICE ZA PRORAČUN**

Predlog bo vplival na proračun Unije.

Ker so naloge, ki spadajo v novi mandat ENISA, določene, se predpostavlja, da bo agencija prejela sredstva, ki jih potrebuje za zadovoljivo opravljanje teh nalog. Iz ocene agencije, širšega posvetovanja z zainteresiranimi stranmi na vseh ravneh in ocene učinka je splošno razvidno, da je velikost agencije pod kritično maso in da je treba njena sredstva povečati. Posledice in učinki, ki bi jih imelo povečanje kadrov in proračuna agencije, so analizirani v oceni učinka, ki je priložena predlogu.

Financiranje EU po letu 2013 bo preučeno v razpravi znotraj Komisije o vseh predlogih za obdobje po letu 2013.

## **5. DODATNE OPOMBE**

### **5.1. Veljavnost**

Uredba naj bi veljala pet let.

### **5.2. Klavzula ponovnega pregleda**

Uredba določa, da je treba agencijo oceniti v obdobju, ki presega obdobje zadnje ocene iz leta 2007. Ocenila se bo učinkovitost agencije pri doseganju ciljev iz uredbe, ali še vedno predstavlja učinkovit instrument in ali bi bilo treba trajanje agencije nadalje podaljšati. Na podlagi ugotovitev bo upravni odbor Komisiji predložil priporočila glede sprememb te uredbe, agencije in njenih delovnih praks. Da bi lahko Komisija pravočasno predložila morebitni predlog o podaljšanju mandata, mora biti ocena opravljena do konca drugega leta mandata, ki ga določa uredba.

### **5.3. Začasen ukrep**

Komisija se zaveda, da lahko zakonodajni postopek v Evropskem parlamentu in Svetu pri tem predlogu zahteva veliko časa za razpravo in da obstaja tveganje pravne praznine, če novi mandat agencije ne bo sprejet pravočasno, tj. pred iztekom sedanjega mandata. Zato skupaj s predlogom predlaga še eno uredbo, ki bi sedanji mandat agencije podaljšala za 18 mesecev, kar bi zagotovilo dovolj časa za razpravo in postopek.

**Predlog**

**UREDBA EVROPSKEGA PARLAMENTA IN SVETA**

**o Evropski agenciji za varnost omrežij in informacij (ENISA)**

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

ob upoštevanju Pogodbe o delovanju Evropske unije, zlasti člena 114 Pogodbe,

ob upoštevanju predloga Evropske komisije,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora<sup>15</sup>,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora<sup>16</sup>,

po predložitvi predloga nacionalnim parlamentom,

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

- (1) Elektronske komunikacije, infrastruktura in storitve so bistven dejavnik gospodarskega in družbenega razvoja. Imajo ključno vlogo za družbo in so tako kot oskrba z električno energijo ali vodo postale nepogrešljive. Njihove motnje lahko povzročijo veliko gospodarsko škodo, zaradi česar so ukrepi za povečanje zaščite in odpornosti, ki naj bi zagotovili neprekinjenost kritičnih storitev, še toliko pomembnejši. Varnost elektronskih komunikacij, infrastrukture in storitev, zlasti njihova celovitost in razpoložljivost, je izpostavljena vedno večjim izzivom. Za družbo je vedno pomembnejša, navsezadnje tudi zato, ker lahko zaradi kompleksnosti sistemov, nesreč, napak in napadov nastanejo težave, ki imajo lahko posledice za fizično infrastrukturo, prek katere se evropskim državljanom zagotavljajo storitve v njihovo dobrobit.
- (2) Nevarnosti se neprestano spreminjajo in varnostni incidenti lahko ogrozijo zaupanje uporabnika. Medtem ko lahko resne motnje v elektronskih komunikacijah, infrastrukturi in storitvah močno vplivajo na gospodarstvo in družbo, lahko tudi vsakodnevne kršitve varnosti, težave in neprijetnosti zmanjšajo zaupanje javnosti v tehnologijo, omrežja in storitve.
- (3) Za oblikovalce politike, stroko in uporabnike je zato pomembno, da se varnost omrežij in informacij v Evropi redno ocenjuje z zanesljivimi evropskimi podatki.

---

<sup>15</sup> UL C „, str. ...

<sup>16</sup> UL C „, str. ..

- (4) Predstavniki držav članic so na zasedanju Evropskega sveta 13. decembra 2003 sprejeli sklep, da bo sedež Evropske agencije za varnost omrežij in informacij (ENISA), ki naj bi bila ustanovljena na podlagi predloga Komisije, v grškem mestu, ki ga bo določila grška vlada.
- (5) Leta 2004 sta Evropski parlament in Svet sprejela Uredbo (ES) št. 460/2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij<sup>17</sup>, da bi prispevala k ciljema, da se zagotovi visoka raven varnosti omrežij in informacij v Uniji ter razvije kultura varnosti omrežij in informacij v korist državljanov, potrošnikov, podjetij in javnih uprav. Leta 2008 sta Evropski parlament in Svet sprejela Uredbo (ES) št. 1007/2008<sup>18</sup>, s katero sta mandat agencije podaljšala do marca 2012.
- (6) Po ustanovitvi agencije so se s tehnološkim, tržnim in družbeno-gospodarskim razvojem spremenili izzivi, povezani z varnostjo omrežij in informacij, zato se jih je nadalje preučevalo in o njih razpravljalo. Kot odgovor na spreminjajoče se izzive je Unija prednostne naloge politike na področju varnosti omrežij in informacij posodobila z vrsto dokumentov, med drugim tudi s sporočilom Komisije iz leta 2006 z naslovom Strategija za varno informacijsko družbo – dialog, partnerstvo ter povečanje vpliva in moči<sup>19</sup>, resolucijo Sveta iz leta 2007 z naslovom Strategija za varno informacijsko družbo v Evropi<sup>20</sup>, sporočilom Komisije iz leta 2009 z naslovom O zaščiti kritične informacijske infrastrukture – Kako zaščititi Evropo pred obsežnimi kibernetскими napadi in prekinitvami: izboljšati pripravljenost, varnost in odpornost<sup>21</sup>, sklepi predsedstva ministrske konference o zaščiti kritične informacijske infrastrukture, resolucijo Sveta iz leta 2009 o skupnem evropskem pristopu do varnosti omrežij in informacij<sup>22</sup>. Ugotovljeno je bilo, da je treba agencijo posodobiti in okrepiti, da bo lahko uspešno prispevala k prizadevanjem evropskih institucij in držav članic, da razvijejo evropsko sposobnost za odzivanje na izzive, ki jih prinaša varnost omrežij in informacij. Komisija je pred kratkim sprejela digitalno agendo za Evropo<sup>23</sup> kot eno vodilnih pobud strategije Evropa 2020. S to celovito agendo naj bi se izkoristil in povečal potencial IKT, ki se bo nato pretvoril v trajnostno rast in inovacije. Večje zaupanje v informacijsko družbo je eden ključnih ciljev te celovite agende, v kateri je Komisija za to področje napovedala vrsto ukrepov, vključno s tem predlogom.
- (7) Ukrepi na notranjem trgu na področju varnosti elektronskih komunikacij ter varnosti omrežij in informacij na splošno zahtevajo, da jih države članice in Komisija tehnično in organizacijsko različno izvajajo. Različno izvajanje teh zahtev lahko povzroči neučinkovitost in na notranjem trgu ustvari ovire. Zato je treba na evropski ravni ustanoviti strokovni center, ki bo države članice in evropske institucije usmerjal, jim svetoval in na zahtevo pomagal pri vprašanjih, ki se nanašajo na varnost omrežij in informacij, ter na katerega se bodo te lahko zanesle. Agencija lahko te potrebe zadovolji, če bo razvila in ohranila visoko raven strokovnega znanja in izkušenj ter državam članicam, Komisiji in s tem tudi gospodarski skupnosti pomagala pri

---

<sup>17</sup> UL L 77, 13.3.2004, str. 1.

<sup>18</sup> UL L 293, 31.10.2008, str. 1.

<sup>19</sup> COM(2006) 251, 31.5.2006.

<sup>20</sup> Resolucija Sveta z dne 22. marca 2007 o strategiji za varno informacijsko družbo v Evropi (UL C 68, 24.3.2007, str. 1).

<sup>21</sup> COM(2009) 149, 30.3.2009.

<sup>22</sup> Resolucija Sveta z dne 18. decembra 2009 o skupnem evropskem pristopu do varnosti omrežij in informacij (UL C 321, 29.12.2009, str. 1).

<sup>23</sup> COM(2010)245, 19.5.2010

izpolnjevanju pravnih in regulativnih zahtev, ki veljajo za varnost omrežij in informacij, ter tako prispevala k nemotenemu delovanju notranjega trga.

- (8) Agencija mora opravljati naloge, ki so bile nanjo prenesene z veljavno zakonodajo Unije o elektronskih komunikacijah, ter z nudenjem strokovnega znanja in izkušenj, svetovanjem in spodbujanjem izmenjave dobrih praks na splošno prispevati k večji varnosti elektronskih komunikacij.
- (9) Direktiva 2002/21/ES Evropskega parlamenta in Sveta z dne 7. marca 2002 o skupnem regulativnem okviru za elektronska komunikacijska omrežja in storitve 2002/21/ES (okvirna direktiva)<sup>24</sup> tudi določa, da ponudniki javnih elektronskih komunikacijskih omrežij ali javnosti dostopnih elektronskih komunikacijskih storitev sprejmejo ustrezne ukrepe, s katerimi zavarujejo integriteto in varnost, ter uvaja zahteve za obveščanje o kršitvah varnosti in izgubah integritete. Agencijo morajo po potrebi obveščati tudi nacionalni regulativni organi, ki morajo Komisiji in agenciji predložiti povzetek letnega poročila o prejetih obvestilih in sprejetih ukrepih. Direktiva 2002/21/ES tudi določa, da agencija z mnenji prispeva k usklajevanju ustreznih tehničnih in organizacijskih varnostnih ukrepov.
- (10) Direktiva 2002/58/ES Evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (direktiva o zasebnosti in elektronskih komunikacijah)<sup>25</sup> določa, da ponudnik javno razpoložljive elektronske komunikacijske storitve sprejme ustrezne tehnične in organizacijske ukrepe, s katerimi zagotovi varnost svojih storitev, ter da so sporočila in s tem povezani podatki o prometu zaupni. Direktiva 2002/58/ES za ponudnike elektronskih komunikacijskih storitev uvaja zahteve glede informacij in obvestil o kršitvah varstva osebnih podatkov. Prav tako določa, da se Komisija pri vseh tehničnih izvedbenih ukrepih, ki jih namerava sprejeti, posvetuje z agencijo o njihovih okoliščinah, obliki in postopkih, ki se uporabljajo za zahteve za obveščanje in sporočanje. Države članice morajo v skladu z Direktivo 95/46/ES Evropskega parlamenta in Sveta z dne 24. oktobra 1995 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov<sup>26</sup> zagotoviti, da upravljavec izvaja ustrezne tehnične in organizacijske ukrepe, s katerimi osebne podatke zavaruje pred slučajnim ali nezakonitim uničenjem ali slučajno izgubo, predelavo, nepooblaščenim posredovanjem ali dostopom, predvsem kadar obdelava vključuje prenos podatkov po omrežju, ter ukrepe proti vsem drugim nezakonitim oblikam obdelave.
- (11) Agencija mora prispevati k visoki ravni varnosti omrežij in informacij v Uniji in razvoju kulture varnosti omrežij in informacij v korist državljanov, potrošnikov, podjetij in organizacij javnega sektorja v Evropski uniji ter tako prispevati k nemotenemu delovanju notranjega trga.
- (12) Nabor nalog mora določati, kako naj agencija doseže svoje cilje, ter ji hkrati dopuščati dovolj prožnosti pri njenem delovanju. Med naloge agencije mora spadati zbiranje ustreznih informacij in podatkov, da se lahko opravijo analize tveganj za varnost in odpornost elektronskih komunikacij, infrastrukture in storitev, ter v sodelovanju z

---

<sup>24</sup> UL L 108, 24.4.2002, str. 33.

<sup>25</sup> UL L 201, 31.7.2002, str. 37.

<sup>26</sup> UL L 281, 23.11.1995, str. 31.

državami članicami oceni stanje varnosti omrežij in podatkov v Evropi. Agencija mora zagotoviti sodelovanje z državami članicami in izboljšati sodelovanje med zainteresiranimi stranmi v Evropi tako, da v svoje dejavnosti vključi zlasti pristojne nacionalne organe in strokovnjake s področja varnosti omrežij in informacij iz zasebnega sektorja. Agencija mora Komisijo in države članice podpirati v dialogu s stroko, da se pri izdelkih strojne in programske opreme odpravijo varnostne težave ter tako prispeva k sodelovalnemu pristopu do varnosti omrežij in informacij.

- (13) Agencija mora delovati kot referenčna točka in s svojo neodvisnostjo, ponujenim kakovostnim svetovanjem, informacijami, ki jih razširja, preglednostjo postopkov in načinom delovanja ter skrbnostjo pri izvajanju dodeljenih nalog ustvarjati zaupanje. Na podlagi nacionalnih prizadevanj in prizadevanj Unije mora naloge opravljati v popolnem sodelovanju z državami članicami ter biti odprta za stike s stroko in drugimi ustreznimi zainteresiranimi stranmi. Poleg tega se mora opirati na prispevke zasebnega sektorja in njegovo sodelovanje, saj ima ta pomembno vlogo pri varovanju elektronskih komunikacij, infrastrukture in storitev.
- (14) Komisija je uvedla evropsko javno-zasebno partnerstvo za odpornost kot prožen evropski upravni okvir za odpornost infrastrukture IKT, pri katerem naj bi agencija olajšala povezovanje med zainteresiranimi stranmi iz javnega in zasebnega sektorja ter tako odprla razpravo o prednostnih nalogah javne politike, gospodarskih in tržnih razsežnostih izzivov in ukrepov za odpornost infrastrukture IKT ter opredelila njihove pristojnosti.
- (15) Agencija mora Komisiji na zahtevo ali lastno pobudo svetovati z mnenji ter tehničnimi in družbeno-ekonomskimi analizami ter ji tako pomagati pri razvoju politike na področju varnosti omrežij in informacij. Države članice ter evropske institucije in organe mora na zahtevo podpreti v njihovih prizadevanjih, da za področje varnosti omrežij in informacij razvijejo politiko ter sposobnost.
- (16) Agencija mora države članice in evropske institucije podpreti v prizadevanjih za vzpostavitev in povečanje čezmejnih sposobnosti in pripravljenosti za preprečevanje, odkrivanje ter boljše odzivanje na težave v zvezi z varnostjo omrežij in informacij ter incidenti; pri tem mora olajšati sodelovanje med državami članicami ter državami članicami in Komisijo. V ta namen mora aktivno podpirati države članice v stalnih prizadevanjih, da izboljšajo odzivno sposobnost ter organizirajo in izvajajo nacionalne in evropske vaje za varnostne incidente.
- (17) Direktiva 95/46/ES ureja obdelovanje osebnih podatkov, ki se opravlja na podlagi te uredbe.
- (18) Da bi agencija bolje razumela izzive na področju varnosti omrežij in informacij, mora analizirati trenutna in nastajajoča tveganja. V ta namen mora v sodelovanju z državami članicami in po potrebi s statističnimi uradi zbrati ustrezne informacije. Prav tako mora države članice ter evropske institucije in organe podpreti v prizadevanjih, da zbirajo, analizirajo in razširjajo varnostne podatke.
- (19) Pri opravljanju spremljanja v Uniji mora agencija olajšati sodelovanje med Unijo in državami članicami pri ocenjevanju stanja varnosti omrežja in informacij v Evropi ter v sodelovanju z državami članicami prispevati k ocenjevanju.



- (20) Agencija mora olajšati sodelovanje med pristojnimi javnimi organi držav članic, zlasti podpirati razvoj in izmenjavo dobrih praks in standardov za izobraževalne programe in programe ozaveščanja. Take ukrepe bi poenostavila boljša izmenjava informacij med državami članicami. Agencija mora podpirati tudi sodelovanje med javnimi in zasebnimi akterji na ravni Unije, med drugim tudi tako, da spodbuja izmenjavo informacij, kampanje za ozaveščanje, izobraževalne programe in programe usposabljanja.
- (21) Učinkoviti varnostni ukrepi morajo v javnem kot tudi zasebnem sektorju temeljiti na dobro razvitih metodah za ocenjevanje tveganja. Metode in postopki za ocenjevanje tveganj se uporabljajo na različnih ravneh, skupne prakse za učinkovito izvajanje ni. Spodbujanje in razvoj najboljših praks za ocenjevanje tveganj ter medobratovalnih rešitev za obvladovanje tveganj v javnih in zasebnih organizacijah bosta povečala varnost omrežnih in informacijskih sistemov v Evropi. V ta namen mora agencija spodbujati sodelovanje med javnimi in zasebnimi akterji na ravni Unije ter jih podpreti v prizadevanjih, da se razvijejo in uvedejo standardi za obvladovanje tveganja in merljivo varnost elektronskih izdelkov, sistemov, omrežij in storitev.
- (22) Agencija mora pri svojem delu upoštevati trenutne raziskave ter dejavnosti, s katerimi se ocenjujejo razvoj in tehnologije, zlasti dejavnosti, ki se opravljajo v okviru različnih raziskovalnih pobud Evropske unije.
- (23) Agencija mora z organi in agencijami, ustanovljenimi po pravu Evropske unije, ki se ukvarjajo z varnostjo omrežij in informacij, deliti izkušnje in splošne informacije, če je to v skladu z njenimi pristojnostmi, cilji in nalogami.
- (24) Pri stikih z organi pregona, ki se nanašajo na varnostne vidike kibernetnega kriminala, uporablja obstoječe informacijske kanale in ustanovljena omrežja, npr. kontaktne točke iz predloga Direktive Evropskega parlamenta in Sveta o napadih na informacijske sisteme, ki naj bi razveljavil okvirno direktivo 2005/222/PNZ, ali Europolove vodje projektnih skupin za preprečevanje visokotehnološkega kriminala.
- (25) Da bi agencija cilje dosegla v celoti, mora navezati stike z organi pregona in organi za zaščito zasebnosti, da bi lahko v boju proti kibernetnemu kriminalu izpostavila in ustrezno obravnavala varnostne vidike omrežij in informacij. Predstavniki teh organov morajo postati enakopravni akterji agencije in biti zastopani v stalni skupini zainteresiranih strani agencije.
- (26) Težave z varnostjo omrežij in informacij imajo svetovno razsežnost. Da se izboljšajo varnostni standardi in izmenjava informacij ter spodbuja skupen globalni pristop do vprašanj, ki se nanašajo na varnost omrežij in informacij, je potrebno tesnejše mednarodno sodelovanje. V ta namen mora agencija podpirati sodelovanje s tretjimi državami in mednarodnimi organizacijami ter pri tem po potrebi sodelovati z EEAS.
- (27) Pri opravljanju nalog agencija ne sme posegati v pristojnosti oziroma okrniti pooblastil in nalog naslednjih organov, jih ovirati ali se z njimi prekrivati: nacionalnih regulativnih organov iz direktiv o elektronskih komunikacijskih omrežjih in storitvah, Organa evropskih regulatornih organov za elektronske komunikacije (BEREC), ki je bil ustanovljen z Uredbo Evropskega parlamenta in Sveta št. 1211/2009<sup>27</sup>, Odbora za

---

<sup>27</sup> UL L 337, 18.12.2009, str. 1.

komunikacije iz Direktive 2002/21/ES, evropskih in nacionalnih inštitutov za standardizacijo, stalnega odbora iz Direktive 98/34/ES Evropskega parlamenta in Sveta z dne 22. junija 1998 o določitvi postopka za zbiranje informacij na področju tehničnih standardov in tehničnih predpisov o storitvah informacijske družbe<sup>28</sup> ter nadzornih organov držav članic na področju zaščite fizičnih oseb pri obdelovanju osebnih podatkov in prostem pretoku takšnih podatkov.

- (28) Da se zagotovi učinkovitost agencije, morajo biti države članice in Komisija zastopane v upravnem odboru, ki določa glavno usmeritev njenih dejavnosti in zagotovi, da ta naloge opravlja v skladu s to uredbo. Na odbor je treba prenesti ustrezna pooblastila, da lahko pripravi proračun in preveri njegovo izvajanje, sprejme ustrezna finančna pravila, uvede pregledne postopke za sprejemanje odločitev agencije, sprejme program dela, poslovnik in statut agencije, imenuje izvršnega direktorja ter odloča o podaljšanju ali koncu njegovega mandata. Upravni odbor mora imeti možnost, da ustanovi delovne organe, ki mu pomagajo pri njegovih nalogah; taki organi bi lahko npr. pripravili osnutek njegovih sklepov ali spremljali njihovo izvajanje.
- (29) Da bi agencija delovala nemoteno, je treba njenega izvršnega direktorja imenovati na podlagi zaslug ter upravnih in vodstvenih sposobnosti, ki jih izkaže z dokazili, ustreznih usposobljenosti in izkušenj s področja varnosti omrežij in informacij, svoje naloge pa mora opravljati popolnoma neodvisno od organiziranosti notranjega delovanja agencije. V ta namen mora izvršni direktor po posvetovanju s službami Komisije pripraviti predlog programa dela agencije ter sprejeti vse potrebne ukrepe, da zagotovi njegovo nemoteno izvajanje. Vsako leto mora pripraviti osnutek splošnega poročila in ga predložiti upravnemu odboru, pripraviti osnutek predloga o načrtovanih prihodkih in odhodkih agencije ter izvrševati proračun.
- (30) Izvršni direktor mora imeti možnost, da ustanovi ad hoc delovne skupine, ki preučujejo posebne znanstvene, tehnološke, pravne ali družbeno-gospodarske zadeve. Pri ustanavljanju ad hoc delovnih skupin si mora izvršni direktor prizadevati, da v njih sodelujejo ustrezni zunanji strokovnjaki, ter se opirati na njihovo znanje, s čimer agenciji zagotovi dostop do najbolj ažurnih informacij o varnostnih izzivih, povezanih z razvojem informacijske družbe. Agencija mora zagotoviti, da člane ad hoc delovnih skupin izbira v skladu z najvišjimi strokovnimi standardi ter glede na posamezno zadevo po potrebi zagotovi ravnovesje med predstavniki javnih uprav držav članic in zasebnega sektorja, vključno s stroko, uporabniki in znanstveniki s področja varnosti informacij in omrežij. Agencija lahko v posameznih primerih po potrebi povabi priznane strokovnjake z zadevnega področja, da sodelujejo v postopkih delovnih skupin. Njihove stroške mora kriti agencija v skladu s statutom in veljavnimi finančnimi uredbami.
- (31) Agencija mora imeti skupino stalnih zainteresiranih strani, ki deluje kot svetovalni organ, da zagotovi redni dialog z zasebnim sektorjem, združenji potrošnikov in drugimi ustreznimi zainteresiranimi stranmi. Skupina stalnih zainteresiranih strani, ki jo na predlog izvršnega direktorja ustanovi upravni odbor, mora obravnavati zadeve, ki so pomembne za vse zainteresirane strani, ter o njih obvestiti agencijo. Izvršni direktor lahko v skladu z dnevnim redom sej na seje skupine po potrebi povabi predstavnike Evropskega parlamenta in drugih ustreznih organov.

---

<sup>28</sup> UL L 204, 21.7.1998, str. 37.

- (32) Agencija deluje v skladu z (i) načelom subsidiarnosti, pri čemer med državami članicami zagotavlja ustrezno raven sodelovanja, izboljšuje učinkovitost nacionalnih politik ter jim tako dodaja vrednost, ter (ii) načelom sorazmernosti, pri čemer ne presega tistega, kar je potrebno za doseganje ciljev iz te uredbe.
- (33) Agencija mora uporabljati ustrezno zakonodajo Unije o dostopu javnosti do dokumentov, ki ga ureja Uredba (ES) št. 1049/2001 Evropskega parlamenta in Sveta<sup>29</sup>, ter o varstvu posameznikov pri obdelavi osebnih podatkov, ki ga ureja Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov<sup>30</sup>.
- (34) Pri pristojnostih, ciljnih in nalogah mora agencija spoštovati določbe o ravnanju z občutljivimi dokumenti, ki se uporabljajo za evropske institucije, ter ustrezno nacionalno zakonodajo. Upravni odbor mora biti pooblaščen, da sprejme sklep, s katerim agencijo pooblasti za ravnanje s tajnimi podatki.
- (35) Da se agenciji zagotovita popolna samostojnost in neodvisnost, ji je treba dodeliti lastna proračunska sredstva, ki se večinoma zagotovijo s prispevkom Unije in prispevki tretjih držav, ki sodelujejo pri delu agencije. Država članica gostiteljica ali vsaka druga država članica lahko prostovoljno prispeva k prihodkom agencije. Za nepovratna sredstva v breme splošnega proračuna Evropske unije se uporablja postopek za sprejemanje proračuna Unije. Revizijo opravi Računsko sodišče.
- (36) Agencija naj bi nadomestila ENISA, ki je bila ustanovljena z Uredbo št. 460/2004. Glede na sklep, ki so ga predstavniki držav članic sprejeli na zasedanju Evropskega sveta 13. decembra 2003, mora država članica gostiteljica ohraniti in oblikovati praktične podrobnosti za nemoteno in učinkovito delovanje agencije, zlasti kar zadeva sodelovanje agencije s Komisijo, državami članicami in pristojnimi organi, ostalimi institucijami in organi Unije ter zainteresiranimi stranmi iz javnega in zasebnega sektorja po vsej Evropi ter pomoč, ki jim jo zagotavlja.
- (37) Agencija se ustanovi za določen čas. Njene dejavnosti je treba oceniti glede na njihovo učinkovitost pri doseganju ciljev in njene delovne prakse, da se ugotovi, ali so cilji agencije še vedno veljavni oziroma ali je treba delovanje agencije podaljšati.

SPREJELA NASLEDNJO UREDBO:

## **ODDELEK 1 PODROČJE UPORABE, CILJI IN NALOGE**

### *Člen 1*

#### **Vsebina in področje uporabe**

1. S to uredbo se ustanavlja Agencija za varnost omrežij in informacij (v nadaljnjem besedilu: agencija), ki naj bi prispevala k visoki ravni varnosti omrežij in informacij v Uniji, ozaveščala

---

<sup>29</sup> Uredba (ES) št. 1049/2001 Evropskega parlamenta in Sveta z dne 30. maja 2001 o dostopu javnosti do dokumentov Evropskega parlamenta, Sveta in Komisije (UL L 145, 31.5.2001, str. 43).

<sup>30</sup> Uredba (ES) št. 45/2001 Evropskega parlamenta in Sveta z dne 18. decembra 2000 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah in organih Skupnosti in o prostem pretoku takih podatkov (UL L 8, 12.1.2001, str. 1).

ter razvila kulturo varnosti omrežij in informacij v družbi v korist državljanov, potrošnikov, podjetij in organizacij javnega sektorja Unije ter tako prispevala k nemotenemu delovanju notranjega trga.

2. Cilji in naloge agencije ne posegajo v pristojnosti držav članic na področju varnosti omrežij in informacij in nikakor ne v dejavnosti, ki se nanašajo na javno varnost, obrambo, državno varnost (vključno z gospodarsko blaginjo države, če se zadeva nanaša na državno varnost), ter v dejavnosti države na področju kazenskega prava.

3. V tej uredbi pomeni „varnost omrežij in informacij“ zmožnost omrežja ali informacijskega sistema, da na določeni ravni zaupanja prepreči slučajne dogodke in nezakonita ali zlonamerna dejanja, ki ogrožajo razpoložljivost, verodostojnost, celovitost in zaupnost shranjenih ali prenesenih podatkov ter s tem povezanih storitev, ki se prek teh omrežij zagotavljajo oziroma so prek njih dostopni.

## *Člen 2* **Cilji**

1. Agenciji pri izpolnjevanju pravnih in regulativnih zahtev v skladu z veljavno in prihodnjo zakonodajo Unije, ki se nanašajo na varnost omrežij in informacij, pomagajo Komisija in države članice, ki tako prispevajo k nemotenemu delovanju notranjega trga.

2. Agencija povečuje sposobnost in pripravljenost Unije in držav članic, da preprečijo, odkrivajo ter se odzovejo na težave in incidente na področju varnosti omrežij in informacij.

3. Agencija razvija in vzdržuje visoko raven strokovnega znanja in izkušenj ter z njim spodbuja širše sodelovanje med zainteresiranimi stranmi iz javnega in zasebnega sektorja.

## *Člen 3* **Naloge**

1. Za namen iz člena 1 agencija opravlja naslednje naloge:

(a) na zahtevo ali lastno pobudo pomaga Komisiji z nasveti, mnenji, tehničnimi in družbeno-gospodarskimi analizami ter pripravami na razvoj in posodobitev zakonodaje Unije o varnosti omrežij in informacij oblikovati politiko varnosti omrežij in informacij;

(b) olajšuje sodelovanje med državami članicami ter državami članicami in Komisijo pri čezmejnih prizadevanjih za preprečevanje in odkrivanje incidentov na področju varnosti omrežij in informacij ter za odzivanje nanje;

(c) podpira države članice ter evropske institucije in organe v prizadevanjih, da zbirajo, analizirajo in razširjajo podatke o varnosti omrežij in informacij;

(d) v sodelovanju z državami članicami in evropskimi institucijami redno ocenjuje stanje varnosti omrežij in informacij v Evropi;

(e) podpira sodelovanje med pristojnimi evropskimi javnimi organi, zlasti pri prizadevanjih za razvoj ter izmenjavo dobrih praks in standardov;

- (f) Uniji in državam članicam pomaga spodbujati uporabo dobrih praks in standardov za obvladovanje tveganj pri elektronskih izdelkih, sistemih in storitvah ter za njihovo varnost;
- (g) spodbuja sodelovanje med zainteresiranimi stranmi iz javnega in zasebnega sektorja na ravni Unije tako, da spodbuja izmenjavo informacij in ozaveščanje ter podpira prizadevanja za pripravo in uvedbo standardov za upravljanje tveganj ter varnost elektronskih izdelkov, omrežij in storitev;
- (h) med zainteresiranimi stranmi iz javnega in zasebnega sektorja olajšuje dialog in izmenjavo dobrih praks s področja varnosti omrežij in informacij, vključno z vidiki, povezanimi z bojem proti kibernetickemu kriminalu, ter Komisiji pomaga oblikovati politiko, pri kateri se upoštevajo vidiki varnosti omrežij in informacij v boju pri kibernetickemu kriminalu;
- (i) na zahtevo držav članic ter evropskih institucij in organov podpira prizadevanja, da se razvije sposobnost za odkrivanje, analiziranje in odzivanje na področju varnosti omrežij in informacij;
- (j) po potrebi v sodelovanju z EEAS podpira dialog in sodelovanje Unije s tretjimi državami in mednarodnimi organizacijami ter tako spodbuja mednarodno sodelovanje in skupen globalni pristop do zadev, ki se nanašajo na varnost omrežij in informacij;
- (k) opravlja naloge, ki so bile nanjo prenesene s pravnimi akti Unije.

## **ODDELEK 2 ORGANIZACIJA**

### *Člen 4* **Sestava agencije**

Agencijo sestavljajo:

- (a) upravni odbor,
- (b) izvršni direktor in osebje ter
- (c) stalna skupina zainteresiranih strani.

### *Člen 5* **Upravni odbor**

1. Upravni odbor določi splošno usmeritev delovanja agencije in zagotovi, da agencija deluje v skladu s pravili in načeli iz te uredbe. Prav tako zagotovi, da je delo agencije v skladu z dejavnostmi držav članic in Unije.
2. Upravni odbor sprejme poslovnik v soglasju z ustreznimi službami Komisije.
3. Upravni odbor sprejme statut v soglasju z ustreznimi službami Komisije. Statut tudi objavi.
4. Upravni odbor imenuje izvršnega direktorja v skladu s členom 10(2) in ga lahko razreši. Izvršni direktor je disciplinsko odgovoren upravnemu odboru.

5. Upravni odbor sprejme program dela agencije v skladu s členom 13(3) in splošno poročilo o dejavnostih agencije v lanskem letu v skladu s členom 14(2).

6. Upravni odbor sprejme pravilnik o finančnem poslovanju agencije. Pravilnik lahko odstopa od Uredbe Komisije (ES, Euratom) št. 2343/2002 z dne 19. novembra 2002 o okvirni finančni uredbi za organe iz člena 185 Uredbe Sveta (ES, Euratom) št. 1605/2002 o finančni uredbi za splošni proračun Evropskih skupnosti<sup>31</sup> samo, če se tako odstopanje izrecno zahteva za delovanje Agencije in je Komisija dala zanj predhodno soglasje.

7. Upravni odbor v soglasju s Komisijo in v skladu s členom 110 Kadrovskih predpisov sprejme ustrezna izvedbena pravila.

8. Upravni odbor lahko ustanovi delovna telesa, sestavljena iz njegovih članov, ki mu pomagajo pri opravljanju nalog, vključno s pripravo osnutkov sklepov in spremljanjem njihovega izvajanja.

9. Upravni odbor lahko, potem ko se je posvetoval s službami Komisije in o tem ustrezno obvestil proračunski organ, sprejme večletni načrt kadrovske politike.

#### *Člen 6*

#### **Sestava upravnega odbora**

1. Upravni odbor sestavljajo po en predstavnik vsake države članice, trije predstavniki, ki jih imenuje Komisija, in trije predstavniki brez pravice do glasovanja, ki jih imenuje Komisija, vsak od članov pa zastopa naslednje skupine:

(a) stroko informacijskih in komunikacijskih tehnologij;

(b) skupine potrošnikov;

(c) znanstvene strokovnjake s področja varnosti omrežij in informacij.

2. Člani uprave in njihovi namestniki so imenovani na podlagi ustreznih izkušenj in strokovnega znanja s področja varnosti omrežij in informacij.

3. Mandat predstavnikov skupin iz odstavka 1(a), (b) in (c) traja štiri leta. Mandat se lahko enkrat podaljša. Če predstavnik zapusti ustrezno interesno skupino, Komisija imenuje njegovega namestnika.

#### *Člen 7*

#### **Predsednik upravnega odbora**

Upravni odbor izmed svojih članov izvoli predsednika in njegovega namestnika za tri leta z možnostjo ponovne izvolitve. Namestnik po uradni dolžnosti nadomešča predsednika, kadar ta ne more opravljati svojih dolžnosti.

---

<sup>31</sup> UL L 357, 31.12.2002, str. 72.

*Člen 8*  
**Seje**

1. Seje upravnega odbora skliče predsednik.
2. Upravni odbor se redno sestane dvakrat letno. Na zahtevo predsednika ali najmanj tretjine članov, ki imajo pravico do glasovanja, se sestane tudi na izrednih sejah.
3. Izvršni direktor se udeležuje sej upravnega odbora, vendar nima glasovalne pravice.

*Člen 9*  
**Glasovanje**

1. Upravni odbor sprejema sklepe z večino glasov članov z glasovalno pravico.
2. Za sprejetje poslovnika, statuta agencije, proračuna, letnega programa dela ter za imenovanje, razrešitev izvršnega direktorja in podaljšanje njegovega mandata je potrebna dvotretjinska večina glasov članov upravnega odbora s pravico do glasovanja.

*Člen 10*  
**Izvršni direktor**

1. Agencijo vodi izvršni direktor, ki svoje dolžnosti opravlja neodvisno.
2. Izvršnega direktorja imenuje in razreši upravni odbor. Imenuje ga za pet let na podlagi njegovih zaslug ter upravnih in vodstvenih sposobnosti, ki jih izkaže z dokazili, ter ustrezne usposobljenosti in izkušenj s seznama kandidatov, ki ga predlaga Komisija. Kandidata, ki ga izbere upravni odbor, lahko pristojni odbor Evropskega parlamenta pred imenovanjem pozove, da poda izjavo in odgovarja na vprašanja njegovih članov.
3. V zadnjih devetih mesecih pred iztekom tega obdobja Komisija opravi ocenjevanje. Pri tem oceni zlasti:
  - uspešnost izvršnega direktorja;
  - dolžnosti agencije in zahteve v prihodnjih letih.
4. Upravni odbor lahko na predlog Komisije, pri čemer mora upoštevati poročilo o oceni, in samo, če dolžnosti in zahteve Agencije to upravičujejo, mandat izvršnega direktorja enkrat podaljša za največ tri leta.
5. Upravni odbor obvesti Evropski parlament, da namerava podaljšati mandat izvršnega direktorja. Direktorja lahko v mesecu pred podaljšanjem mandata pristojni odbor Evropskega parlamenta pozove, da poda izjavo in odgovarja na vprašanja njegovih članov.
6. Če se mandat izvršnega direktorja ne podaljša, ta funkcijo opravlja do imenovanja njegovega naslednika.
7. Izvršni direktor je odgovoren za:
  - (a) dnevno upravljanje agencije;

- (b) izvajanje programa dela in sklepe, ki jih sprejme upravni odbor;
- (c) da agencija naloge opravlja v skladu z zahtevami uporabnikov njenih storitev, predvsem kar zadeva ustreznost zagotovljenih storitev;
- (d) vse posebne kadrovske zadeve, pri čemer zagotavlja skladnost s splošnimi usmeritvami upravnega odbora in njegovimi splošnimi sklepi;
- (e) vzpostavljanje in vzdrževanje stikov z evropskimi institucijami in organi;
- (f) vzpostavljanje in ohranjanje stika z gospodarstvom in združenji potrošnikov, pri čemer zagotavlja reden dialog z ustreznimi zainteresiranimi stranmi;
- (g) druge naloge, ki so mu dodeljene s to uredbo.

8. Izvršni direktor lahko po potrebi in če je to v skladu s cilji in nalogami agencije, ustanovi ad hoc delovne skupine, ki jo sestavljajo strokovnjaki. O tem vnaprej obvesti upravni odbor. Postopki, ki se nanašajo predvsem na sestavo, imenovanje strokovnjakov s strani izvršnega direktorja in delovanje ad hoc delovnih skupin se določijo v statutu agencije.

9. Izvršni direktor upravnemu odboru zagotovi podporne upravne kadre in po potrebi druge vire.

#### *Člen 11*

#### **Stalna skupina zainteresiranih strani**

1. Na predlog izvršnega direktorja upravni odbor ustanovi stalno skupino zainteresiranih strani, ki jo sestavljajo strokovnjaki, ki zastopajo ustrezne zainteresirane strani, npr. stroko informacijskih in komunikacijskih tehnologij, skupine potrošnikov, znanstvenike s področja varnosti omrežij in informacij, organe pregona in organe za zaščito zasebnosti.
2. Postopki, ki se nanašajo predvsem na število, sestavo, imenovanje članov s strani izvršnega direktorja in delovanje skupine, predlog izvršnega direktorja in delovanje skupine, se določijo v statutu agencije in objavijo.
3. Skupini predseduje izvršni direktor.
4. Mandat članov skupine traja dve leti in pol. Člani upravnega odbora ne smejo biti člani skupine. Osebe Komisije ima pravico biti prisotno na sejah skupine in sodelovati pri njenem delu.
5. Skupina agenciji svetuje v zvezi z opravljanjem dejavnosti. Še zlasti svetuje izvršnemu direktorju pri pripravi osnutka predloga programa dela agencije in komuniciranju z ustreznimi zainteresiranimi stranmi o zadevah, ki se nanašajo na program dela.



## **ODDELEK 3 DELOVANJE**

### *Člen 12*

#### **Program dela**

1. Agencija deluje v skladu s programom dela, ki vsebuje vse načrtovane dejavnosti. Program dela ne izključuje, da bi agencija v okviru svojega proračuna opravljala nepredvidene dejavnosti, ki so v skladu z njenimi cilji in nalogami. O dejavnostih agencije, ki niso določene v programu dela, izvršni direktor obvesti upravni odbor.
2. Izvršni direktor je odgovoren za pripravo programa dela agencije, o katerem se mora prej posvetovati s službami Komisije. Izvršni direktor vsako leto do 15. marca upravnemu odboru predloži osnutek programa dela za naslednjo leto.
3. Upravni odbor vsako leto do 30. novembra po posvetovanju s službami Komisije sprejme program dela agencije za naslednje leto. Program vsebuje večletne napovedi. Upravni odbor zagotovi, da je program dela v skladu s cilji agencije ter prednostnimi nalogami zakonodaje in politike Unije na področju varnosti omrežij in informacij.
4. Program dela se pripravi v skladu z načelom upravljanja na podlagi dejavnosti. Program je v skladu s poročilom o načrtovanih prihodkih in odhodkih agencije ter proračunom agencije za isto proračunsko leto.
5. Potem ko upravni odbor sprejme program dela, ga izvršni direktor predloži Evropskemu parlamentu, Svetu, Komisiji in državam članicam ter ga objavi.

### *Člen 13*

#### **Splošno poročilo**

1. Izvršni direktor vsako leto upravnemu odboru predloži osnutek splošnega poročila, v katerem so zajete vse dejavnosti agencije iz prejšnjega leta.
2. Upravni odbor vsako leto do 31. marca sprejme splošno poročilo o dejavnostih agencije v prejšnjem letu.
3. Potem ko upravni odbor sprejme splošno poročilo agencije, ga izvršni direktor predloži Evropskemu parlamentu, Svetu, Komisiji, Računskemu sodišču, Evropskemu ekonomsko-socialnemu odboru in Odboru regij ter ga objavi.

### *Člen 14*

#### **Zahtevki, naslovljeni na agencijo**

1. Zahtevki za svetovanje in pomoč, ki spadajo med cilje in naloge agencije, se naslovijo na izvršnega direktorja, priložiti pa jim je treba osnovne informacije, ki pojasnjujejo vprašanje, ki ga je treba obravnavati. Izvršni direktor obvesti upravni odbor o prejetih zahtevkih in pravočasno o nadaljnjih ukrepih v zvezi z zahtevki. Če agencija zahtevke zavrne, to obrazloži.
2. Zahtevke iz prvega odstavka lahko vložijo:

(a) Evropski parlament;

(b) Svet;

(c) Komisija;

(d) vsi pristojni organi, ki jih imenuje država članica, npr. nacionalni regulativni organi iz člena 2 Direktive 2002/21/ES.

3. Praktične podrobnosti za uporabo prvega in drugega odstavka, zlasti glede vložitve, določitve prednosti, nadaljnjih ukrepov kot tudi obveščanja upravnega odbora o zahtevkih, naslovljenih na agencijo, določi upravni odbor v statutu agencije.

#### *Člen 15*

#### **Izjava o interesu**

1. Izvršni direktor in iz držav članic začasno napoteni uradniki podpišejo izjavo o zavezi in izjavo o interesu, v katerih navedejo, da nimajo neposrednih ali posrednih interesov, ki bi lahko ogrozili njihovo neodvisnost.

2. Zunanji strokovnjaki, ki sodelujejo v ad hoc delovnih skupinah, na vsaki seji dajo izjavo o interesih, ki bi lahko ogrozili njihovo neodvisnost pri obravnavi točk dnevnega reda.

#### *Člen 16*

#### **Preglednost**

1. Agencija zagotovi, da dejavnosti opravlja pregledno ter v skladu s členoma 13 in 14.

2. Agencija zagotovi, da imajo javnost in vse zainteresirane strani objektivne, zanesljive in lahko dostopne informacije, po potrebi zlasti o rezultatih njenega dela. Objavi tudi izjave o interesu, ki jih dajo izvršni direktor in iz držav članic začasno napoteni uradniki, kot tudi izjave o interesu, ki jih dajo strokovnjaki na sejah ad hoc skupin pri obravnavi točk dnevnega reda.

3. Upravni odbor lahko na predlog izvršnega direktorja dovoli, da zainteresirane osebe pri določenih dejavnostih agencije sodelujejo kot opazovalci.

4. Agencija v statutu določi praktične podrobnosti za uporabo pravil o preglednosti iz prvega in drugega odstavka.

#### *Člen 17*

#### **Zaupnost**

1. Ne glede na člen 14 agencija tretjim osebam ne sme razkriti informacij, ki jih obdeluje ali prejme in za katere je bilo zahtevano, da se z njimi ravna zaupno.

2. Člani upravnega odbora, izvršni direktor, člani stalne skupine zainteresiranih strani, zunanji strokovnjaki, ki sodelujejo v ad hoc delovnih skupinah, in osebje agencije, vključno z iz držav članic začasno napoteni uradniki, spoštujejo zahteve glede zaupnosti v skladu s členom 339 Pogodbe tudi po izteku dolžnosti.

3. Agencija v statutu določi praktične podrobnosti za uporabo pravil o zaupnosti iz prvega in drugega odstavka.

4. Upravni odbor lahko agenciji dovoli, da ravna z zaupnimi informacijami. Pri tem upravni odbor v soglasju z ustreznimi službami Komisije sprejme statut, pri čemer uporabi varnostna načela iz Sklepa Komisije 2001/844/ES, ESPJ, Euratom z dne 29. novembra 2001 o spremembah njenega poslovnika<sup>32</sup>. To med drugim vključuje tudi določbe o izmenjavi, obdelavi in hrambi tajnih podatkov.

#### *Člen 18*

#### **Dostop do dokumentov**

1. Za dokumente agencije se uporablja Uredba (ES) št. 1049/2001.

2. Upravni odbor v šestih mesecih po ustanovitvi agencije sprejme ukrepe za izvajanje Uredbe (ES) št. 1049/2001.

3. Zoper sklepe, ki jih agencija sprejme v skladu s členom 8 Uredbe (ES) št. 1049/2001, je v skladu s členom 228 oziroma 263 Pogodbe možna pritožba pri varuhu človekovih pravic oziroma Sodišču Evropske unije.

### **ODDELEK 4 FINANČNE DOLOČBE**

#### *Člen 19*

#### **Sprejetje proračuna**

1. Prihodke agencije sestavljajo prispevek iz proračuna Evropske unije, prispevki tretjih držav, ki v skladu s členom 29 sodelujejo pri delu agencije, ter prispevki držav članic.

2. Odhodke agencije predstavljajo odhodki za osebje, upravno in tehnično podporo, infrastrukturo, odhodki, ki nastanejo pri poslovanju, ter odhodki, ki izhajajo iz pogodb, sklenjenih s tretjimi osebami.

3. Izvršni direktor vsako leto do 1. marca pripravi osnutek poročila o načrtovanih prihodkih in odhodkih agencije za naslednje proračunsko leto in ga skupaj z osnutkom načrta delovnih mest predloži upravnemu odboru.

4. Prihodki in odhodki so uravnoteženi.

5. Upravni odbor na podlagi osnutka poročila o načrtovanih prihodkih in odhodkih, ki ga pripravi izvršni direktor, vsako leto pripravi poročilo o načrtovanih prihodkih in odhodkih agencije za naslednje proračunsko leto.

6. Upravni odbor to poročilo o načrtovanih prihodkih in odhodkih, ki vsebuje osnutek načrta delovnih mest in programa dela, najpozneje do 31. marca pošlje Komisiji in državam, s katerimi je Evropska unija sklenila sporazume v skladu s členom 24.

---

<sup>32</sup> UL L 317, 3.12.2001, str. 1.

7. To poročilo Komisija predloži Evropskemu parlamentu in Svetu (v nadaljnjem besedilu: proračunski organ) skupaj z osnutkom splošnega proračuna Evropske unije.

8. Na podlagi poročila Komisija v osnutek splošnega proračuna Evropske unije, ki ga predloži proračunskemu organu v skladu s členom 314 Pogodbe, vnese potrebne predvidene odhodke in prihodke, ki jih po njenem mnenju zahteva načrt delovnih mest, in znesek nepovratnih sredstev, za katerega se bo bremenil splošni proračun.

9. Proračunski organ odobri proračunska sredstva za nepovratna sredstva agencije.

10. Proračunski organ sprejme načrt delovnih mest agencije.

11. Upravni odbor skupaj s programom dela sprejme proračun agencije. Proračun je dokončen, ko je dokončno sprejet splošni proračun Evropske unije. Upravni odbor po potrebi prilagodi proračun in program dela agencije v skladu s splošnim proračunom Evropske unije. Nemudoma ga predloži Komisiji in proračunskemu organu.

## *Člen 20*

### **Boj proti goljufijam**

1. Za boj proti goljufijam, korupciji in drugim nezakonitim dejanjem se brez omejitev uporabljajo določbe Uredbe (ES) št. 1073/1999 Evropskega parlamenta in Sveta z dne 25. maja 1999 o preiskavah, ki jih izvaja Evropski urad za boj proti goljufijam (OLAF)<sup>33</sup>.

2. Agencija pristopi k Medinstitucionalnemu sporazumu z dne 25. maja 1999 med Evropskim parlamentom in Svetom Evropske unije ter Komisijo Evropskih skupnosti o notranjih preiskavah Evropskega urada za boj proti goljufijam (OLAF)<sup>34</sup> in nemudoma izda ustrezne določbe, ki se uporabljajo za vse zaposlene agencije.

## *Člen 21*

### **Izvrševanje proračuna**

1. Proračun agencije izvršuje izvršni direktor.

2. Notranji revizor Komisije ima za agencijo enaka pooblastila kot za oddelke Komisije.

3. Računovodja agencije najpozneje do 1. marca v letu po proračunskem letu računovodji Komisije pošlječasne računovodske izkaze ter poročilo o izvrševanju proračuna in finančnem upravljanju za navedeno proračunsko leto. Računovodja Komisiječasne računovodske izkaze institucij in decentraliziranih organov združi v skladu s členom 128 Uredbe Sveta (ES, Euratom) št. 1605/2002 z dne 25. junija 2002 o finančni uredbi, ki se uporablja za splošni proračun Evropskih skupnosti<sup>35</sup> (v nadaljnjem besedilu: finančna uredba).

4. Računovodja Komisije najpozneje do 31. marca v letu po proračunskemu letu Računskemu sodišču pošlječasne računovodske izkaze agencije ter poročilo o izvrševanju proračuna in

---

<sup>33</sup> UL L 136, 31.5.1999, str. 1.

<sup>34</sup> UL L 136, 31.5.1999, str. 15.

<sup>35</sup> UL L 248, 16.9.2002, str. 1.

finančnem poslovanju za navedeno proračunsko leto. To poročilo pošlje tudi proračunskemu organu.

5. Po prejemu ugotovitev Računskega sodišča o začasnih računovodskih izkazih agencije v skladu s členom 129 splošne finančne uredbe izvršni direktor na lastno odgovornost pripravi dokončne računovodske izkaze agencije in jih predloži upravnemu odboru v mnenje.

6. Upravni odbor predloži mnenje o zaključnem računu agencije.

7. Izvršni direktor najpozneje do 1. julija v letu po proračunskem letu Evropskemu parlamentu, Svetu, Komisiji in Računskemu sodišču predloži končne računovodske izkaze in mnenje upravnega odbora.

8. Izvršni direktor objavi zaključni račun.

9. Izvršni direktor Računskemu sodišču najpozneje do 30. septembra pošlje odgovor na njegove ugotovitve. Odgovor pošlje tudi upravnemu odboru.

10. Na zahtevo Evropskega parlamenta izvršni direktor Evropskemu parlamentu v skladu s členom 146(3) splošne finančne uredbe predloži vse informacije, ki jih ta potrebuje za nemoten potek postopka razrešnice za zaključni račun za zadevno proračunsko leto.

11. Na priporočilo Sveta da Evropski parlament izvršnemu direktorju do 30. aprila leta N+2 razrešnico za izvrševanje proračuna za leto N.

## **ODDELEK 5 SPLOŠNE DOLOČBE**

### *Člen 22*

#### **Pravni položaj**

1. Agencija je organ Skupnosti. Je pravna oseba.

2. Agencija ima v vsaki državi članici največjo pravno sposobnost, ki jo njeni zakoni določajo za pravne osebe. Zlasti lahko pridobiva premočnine in nepremičnine ter je lahko stranka v pravnih postopkih.

3. Agencijo zastopa izvršni direktor.

### *Člen 23*

#### **Osebj**

1. Za osebj agencije, vključno z izvršnim direktorjem, se uporabljajo pravila in predpisi, ki se uporabljajo za uradnike in drugo osebj Evropske unije.

2. V zvezi z izvršnim direktorjem upravni odbor izvaja pooblastila, ki so bili na organ za imenovanje preneseni s Kadrovskimi predpisi in na pooblaščen organ za sklepanje pogodb s pogoji za zaposlitev.

3. V zvezi z osebjem agencije izvršni direktor izvaja pooblastila, ki so bili na organ za imenovanje preneseni s Kadrovski predpisi in na pooblaščen organ za sklepanje pogodb s pogoji za zaposlitev.

4. Agencija lahko zaposli nacionalne strokovnjake, ki jih napotijo države članice. Agencija v statutu določi praktične podrobnosti v zvezi s tem.

#### *Člen 24*

### **Privilegiji in imunitete**

Za agencijo in njeno osebje se uporablja Protokol o privilegijih in imunitetah Evropskih skupnosti.

#### *Člen 25*

### **Odgovornost**

1. Pogodbeno odgovornost agencije ureja pravo, ki se uporablja za posamezno pogodbo.

Za odločitve na podlagi arbitražnih klavzul iz pogodb, ki jih sklene agencija, je pristojno Sodišče Evropske unije.

2. Pri nepogodbeni odgovornosti agencija nadomesti vsakršno škodo, ki jo pri opravljanju nalog povzroči sama ali njeni uslužbenci, v skladu s splošnimi načeli, ki so skupni zakonom držav članic.

Sodišče je pristojno za odločanje v vseh sporih o odškodninah.

3. Osebno odgovornost uslužbencev do agencije urejajo ustrezni pogoji za osebje agencije.

#### *Člen 26*

### **Jeziki**

1. Za organ se uporabljajo določbe Uredbe št. 1 z dne 15. aprila 1958 o določitvi jezikov, ki se uporabljajo v Evropski gospodarski skupnosti<sup>36</sup>. Države članice in drugi organi, ki jih te imenujejo, lahko pišejo agenciji in prejmejo odgovor v jeziku Evropske unije, ki ga izberejo.

2. Prevajalske storitve, potrebne za delovanje agencije, zagotavlja Prevajalski center organov Evropske unije.

#### *Člen 27*

### **Varstvo osebnih podatkov**

Pri obdelavi podatkov o posameznikih veljajo za agencijo določbe iz Uredbe (ES) št. 45/2001.

---

<sup>36</sup> UL 17, 6.10.1958, str. 385/58. Uredba, ki je bila nazadnje spremenjena z Aktom o pristopu iz leta 1994.

*Člen 28*  
**Udeležba tretjih držav**

1. Z agencijo lahko sodelujejo tretje države, ki so z Evropsko unijo sklenile sporazum, s katerim so sprejele ali uporabile zakonodajo Unije s področja uporabe te uredbe.
2. Na podlagi ustreznih določb teh sporazumov se določi ureditev, ki določa predvsem vrsto, obseg in način sodelovanja teh držav pri delu agencije, vključno z določbami o sodelovanju pri pobudah agencije, finančnih prispevkih in osebju.

**ODDELEK 6 FINANČNE DOLOČBE**

*Člen 29*  
**Klavzula ponovnega pregleda**

1. Komisija najpozneje v treh letih od dneva ustanovitve iz člena 34 opravi ocenjevanje na podlagi pristojnosti, dogovorjenih z upravnim odborom, pri čemer upošteva mnenja vseh ustreznih zainteresiranih strani. Ocena vsebuje oceno učinka in učinkovitosti agencije pri doseganju ciljev iz člena 2 ter njenih delovnih praksah. Komisija opravi ocenjevanje zlasti zato, da bi lahko določila, ali agencija še vedno predstavlja učinkovit instrument in ali bi bilo treba trajanje agencije po obdobju iz člena 34 nadalje podaljšati.
2. Ugotovitve, pridobljene med ocenjevanjem, Komisija predloži Evropskemu parlamentu in Svetu ter jih objavi.
3. Upravni odbor prejme oceno in Komisiji izda priporočila glede sprememb te uredbe, agencije in njenih delovnih praks. Upravni odbor in izvršni direktor upoštevata rezultate te ocene pri večletnem načrtovanju agencije.

*Člen 30*  
**Sodelovanje države članice gostiteljice**

Država članica, ki je gostiteljica agencije, zagotovi najboljše možne pogoje za njeno nemoteno in učinkovito delovanje.

*Člen 31*  
**Upravni nadzor**

Delovanje agencije nadzoruje varuh človekovih pravic v skladu s členom 228 Pogodbe.

*Člen 32*  
**Razveljavitev in nasledstvo**

1. Uredba (ES) št. 460/2004 se razveljavi.

Sklici na Uredbo (ES) št. 460/2004 oziroma na ENISA se štejejo za sklice na to uredbo oziroma agencijo.

2. Agencija je pravna naslednica agencije, ustanovljene z Uredbo (ES) št. 460/2004, kar zadeva lastništvo, ureditev, pravne obveznosti, pogodbe o zaposlitvi, finančne obveznosti in odgovornosti.

*Člen 33*  
**Trajanje**

Agencija se ustanovi [...] za pet let.

*Člen 34*  
**Začetek veljavnosti**

Ta uredba začne veljati na dan po objavi v Uradnem listu Evropske unije ter se uporablja od 14. marca 2012 ali dan po objavi, če je ta datum poznejši.

Ta uredba je zavezujoča v celoti in se neposredno uporablja v vseh državah članicah.

V [...],

*Za Evropski parlament*  
*Predsednik*

*Za Svet*  
*Predsednik*



## OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

### 1. OKVIR PREDLOGA/POBUDE

#### 1.1. Naslov predloga/pobude

Predlog uredbe Evropskega parlamenta in Sveta o Evropski agenciji za varnost omrežij in informacij (ENISA)

#### 1.2. Področja politike v strukturi ABM/ABB<sup>37</sup>

Informacijska družba in mediji.  
Regulativni okvir za digitalno agendo

#### 1.3. Vrsta predloga/pobude

- Predlog/pobuda se nanaša na **nov ukrep**
- Predlog/pobuda se nanaša na **nov ukrep, ki sledi pilotnemu projektu / pripravljalnemu ukrepu**<sup>38</sup>
- Predlog/pobuda se nanaša na **podaljšanje obstoječega ukrepa**
- Predlog/pobuda se nanaša na **nadaljevanje obstoječega ukrepa z novo usmeritvijo**

#### 1.4. Cilji

##### 1.4.1. Večletni strateški cilji Komisije, ki jih obravnava predlog/pobuda

**Skladnost regulativnih pristopov** – Komisiji in državam članicam zagotoviti smernice in jim svetovati pri posodobitvi in razvoju enotnega normativnega okvira na področju NIS.

**Preprečevanje, odkrivanje in odzivanje** – prispevati k evropski sposobnosti za zgodnje opozarjanje in odzivanje na incidente ter k vseevropskim kriznim načrtom in vajam ter tako izboljšati pripravljenost

**Izboljšati znanje oblikovalcev politik** – Komisiji in državam članicam zagotavljati pomoč in jim svetovati, da se doseže visoka raven znanja o zadevah NIS po vsej Uniji in njihova uporaba pri zainteresiranih straneh iz stroke. To obsega tudi zbiranje, analiziranje in zagotavljanje razpoložljivosti podatkov o gospodarskih vidikih in kršitvah NIS, spodbude za naložbe v ukrepe NIS za zainteresirane strani, ugotavljanje tveganj, kazalnikov stanja NIS v Uniji itn.

**Izboljšanje položaja zainteresiranih strani** – razviti kulturo upravljanja varnosti in tveganj s spodbujanjem izmenjave informacij in širšega sodelovanja med akterji iz javnega in zasebnega

<sup>37</sup> ABM: upravljanje na podlagi dejavnosti (Activity-Based Management) – ABB: oblikovanje proračuna na podlagi dejavnosti (Activity-Based Budgeting).

<sup>38</sup> Po členu 49(6)(a) ali (b) finančne uredbe.

sektorja, kar naj bi neposredno koristilo tudi državljanom, razvila pa naj bi se tudi kultura ozavešanja o NIS.

**Zaščititi Evropo pred mednarodnimi nevarnostmi** – doseči visoko stopnjo sodelovanja s tretjimi državami in mednarodnimi organizacijami, da se spodbudi skupen globalni pristop do NIS in vpliva na mednarodne pobude na visoki ravni v Evropi.

**Za skupno izvajanje** – olajšati sodelovanje pri izvajanju politik NIS.

**Boj proti kibernetškemu kriminalu** – v razprave in izmenjave dobrih praks med javnimi in zasebnimi akterji vključiti vidike NIS v boju proti kibernetškemu kriminalu, zlasti s sodelovanjem z organi (nekdanjega) drugega in tretjega stebra, npr. z Europolom.

#### 1.4.2. *Posebni cilji in zadevne dejavnosti ABM/ABB*

Posebni cilj št. ...

Povečati varnost omrežij in informacij (NIS), razviti kulturo varnosti omrežij in informacij v korist državljanov, potrošnikov, podjetij in organizacij v javnem sektorju ter opredeliti izzive politike, ki so povezani z prihodnjimi omrežji in internetom

Zadevne dejavnosti AMB/ABB

Politika elektronskih komunikacij in varnosti omrežij

#### 1.4.3. Pričakovani rezultati in učinek

Pobuda naj bi imela naslednje učinke na gospodarstvo:

- večja razpoložljivost informacij o trenutnih in prihodnjih izzivih in tveganjih na področju varnosti in odpornosti
- nepodvajanje prizadevanj posameznih držav članic pri zbiranju ustreznih informacij o tveganjih, nevarnostih in ranljivostih
- boljša obveščenost oblikovalcev politik pri sprejemanju odločitev
- kakovostnejše določbe politike NIS v državah članicah zaradi širjenja najboljših praks
- ekonomije obsega pri odzivanju na incidente na ravni EU
- več naložb zaradi skupnih ciljev politike ter standardov za varnost in odpornost na ravni EU
- manjša operativna tveganja za podjetja zaradi visoke stopnje varnosti in odpornosti
- bolj usklajeni ukrepi v boju proti kibernetickemu kriminalu.

Pobuda naj bi imela naslednje učinke na družbo:

- večje zaupanje uporabnikov v storitve in sisteme informacijske družbe
- večje zaupanje v delovanje notranjega trga EU z doseganjem boljše zaščite potrošnikov
- večja izmenjava informacij in znanja z državami nečlanicami EU;
- boljše varovanje temeljnih človekovih pravic EU zaradi zagotavljanja enakega varstva osebnih podatkov in zasebnosti državljanov EU.

Pričakovani učinki na okolje so minimalni:

- zmanjšan učinek emisij CO<sub>2</sub> npr. zaradi manj potovanj kot posledice pogostejše uporabe sistemov in storitev IKT ter manjše porabe energije zaradi ekonomij obsega pri izvajanju varnostnih obveznosti.

#### 1.4.4. Kazalniki rezultatov in učinka

Kazalniki spremljanja posameznih ciljev so naslednji:

##### **Skladnost regulativnih pristopov:**

- vrsta držav članic je v procesu oblikovanja politike upoštevala priporočila agencije
- vrsta študij, ki naj bi opredelile vrzeli in neskladnosti pri standardih za NIS
- manj razhajanj pri pristopih držav članic do NIS.

##### **Preprečevanje, odkrivanje in odzivanje:**

- število organiziranih usposabljanj o varnosti omrežij
- razpoložljivost sistema za zgodnje opozarjanje na nova tveganja in napade
- število vaj za NIS na ravni EU, ki jih usklajuje agencija

##### **Povečanje znanja za oblikovalce politike:**

- število študij za zbiranje informacij o trenutnih in predvidenih tveganjih za NIS in tehnologijah za njihovo preprečevanje

- število posvetovanj z javnimi organi, ki se ukvarjajo z NIS
- razpoložljivost evropskega okvira, prek katerega se organizira zbiranje podatkov o NIS

#### **Izboljšanje položaja zainteresiranih strani:**

- število opredeljenih dobrih praks za stroko
- višina naložb zasebnih zainteresiranih strani v varnostne ukrepe

#### **Zaščita Evrope pred mednarodnimi nevarnostmi:**

- število konferenc/srečanj med državami članicami EU, da se opredelijo skupno dogovorjeni cilji za NIS
- vrsta srečanj med evropskimi in mednarodnimi strokovnjaki s področja NIS

#### **Skupen pristop**

- število ocen regulativne skladnosti
- število praks NIS, ki se izvajajo po vsej EU

#### **Boj proti kibernetickemu kriminalu:**

- redne interakcije med agencijami nekdanjega drugega in tretjega stebra
- število primerov, pri katerih je bilo pri kriminalističnih preiskavah zagotovljeno strokovno znanje

## **1.5. Utemeljitev predloga/pobude**

### *1.5.1. Zahteve, ki jih je treba izpolniti kratkoročno ali dolgoročno*

ENISA je bila prvotno ustanovljena leta 2004, obravnavala pa naj bi nevarnosti in z njimi povezane morebitne kršitve NIS. Od takrat so se izzivi, ki se nanašajo na varnost omrežij in informacij, s tehnološkim in tržnim razvojem spremenili, zato se jih je nadalje preučevalo in o njih razpravljalo, kar danes omogoča posodobitev in podrobnejši opis ugotovljenih težav in načina njihovega vpliva spreminjajoče se okolje NIS.

### *1.5.2. Dodana vrednost pri posredovanju EU*

Težave, ki se nanašajo na NIS, ne sledijo nacionalnim mejam, zato jih na nacionalni ravni ni mogoče učinkovito odpraviti. Hkrati javni organi v različnih državah članicah te težave različno obravnavajo. Te razlike lahko predstavljajo veliko oviro pri izvajanju ustreznih mehanizmov Unije za povečanje NIS v Evropi. Ker so infrastrukture IKT med seboj povezane, na učinkovitost ukrepov na nacionalni ravni v eni državi članici še vedno močno vplivata nizka stopnja ukrepov v drugi državi članici ter pomanjkanje sistematskega čezmejnega sodelovanja. Če v eni državi članici zaradi nezadostnih ukrepov NIS pride do incidenta, lahko to povzroči motenje storitev v drugih državah članicah.

Poleg tega povečanje varnostnih zahtev pomeni stroškovno oviro za podjetja, ki delujejo na ravni Evropske unije, ter na evropskem notranjem trgu povzroča razdrobljenost in pomanjkanje konkurenčnosti.

Medtem ko se odvisnost od omrežnih in informacijskih sistemov povečuje, je pripravljenost na incidente nezadostna.

Trenutni nacionalni sistemi za zgodnje opozarjanje in obravnavanje incidentov so zelo pomanjkljivi. Vendar se postopki in prakse spremljanja varnostnih incidentov v omrežjih in njihovega poročanja med posameznimi državami članicami zelo razlikujejo. V nekaterih državah procesi niso dovolj formalizirani, medtem ko druge države nimajo pristojnega organa za sprejemanje in obdelovanje poročil o incidentih. Skupnih evropskih sistemov ni. Incidenti NIS bi lahko bistveno onemogočili zagotavljanje osnovnih potrebščin, zato je treba pripraviti ustrezne odzivne ukrepe. Komisija je v sporočilu o zaščiti kritične informacijske infrastrukture tudi poudarila, da je potrebna evropska sposobnost za zgodnje opozarjanje in odzivanje na incidente, ki bi jo podprli z vajami na evropski ravni.

Nujno so potrebni instrumenti politike, ki naj bi proaktivno opredelili tveganja in ranljivosti NIS, uvedli ustrezne mehanizme za odzivanje (npr. z opredelitvijo in širjenjem dobrih praks) ter zagotovili, da mehanizme za odzivanje poznajo in uporabljajo zainteresirane strani.

*1.5.3. Podobne izkušnje v preteklosti*

*Glej točki 1.5.1 in 1.5.2.*

*1.5.4. Skladnost in morebitne sinergije z drugimi zadevnimi instrumenti*

Pobuda je v celoti skladna s splošno razpravo o NIS in drugimi pobudami politike, ki se osredotočajo na prihodnost NIS. Je ena glavnih prvin digitalne agende za Evropo, ki je med vodilnimi pobudami v okviru strategije Evropa 2020.

## 1.6. Trajanje in finančni učinek

Časovno omejen predlog/pobuda

- Petletno podaljšanje se bo začelo s 14. marcem 2012 ali na dan začetka veljavnosti nove uredbe, če je ta datum poznejši.
- Finančne posledice med letoma 2012 in 2017

Časovno omejen predlog/pobuda

- Izvedba s poskusnim obdobjem od leta LLLL do leta LLLL,
- ki mu sledi popolno izvajanje.

## 1.7. Predvideni načini upravljanja<sup>39</sup>

Neposredno centralizirano upravljanje s strani Komisije

Posredno centralizirano upravljanje s prenosom izvrševanja na:

- izvajalske agencije
- organe, ki jih ustanovijo Skupnosti<sup>40</sup>
- nacionalne javne organe/organe, ki opravljajo javne storitve
- osebe, ki se jim zaupa izvedba določenih ukrepov v skladu z naslovom V Pogodbe o Evropski uniji in ki so določene v zadevnem temeljnem aktu po členu 49 finančne uredbe

Deljeno upravljanje z državami članicami

Decentralizirano upravljanje s tretjimi državami

Skupno upravljanje z mednarodnimi organizacijami (*navedite*)

---

<sup>39</sup> Pojasnila o načinih upravljanja in sklici na finančno uredbo so na voljo na spletni strani za proračun: [http://www.cc.cec/budg/man/budgmanag/budgmanag\\_en.html](http://www.cc.cec/budg/man/budgmanag/budgmanag_en.html)

<sup>40</sup> Po členu 185 finančne uredbe.

## 2. UPRAVLJALNI UKREPI

### 2.1. Pravila o spremljanju in poročanju

Izvršni direktor je odgovoren za učinkovit nadzor in ocenjevanje uspešnosti dela Agencije glede na njene cilje. Izvršni direktor letno poroča upravnemu odboru.

Izvršni direktor pripravi osnutek splošnega poročila o vseh dejavnostih agencije v preteklem letu, v katerem primerja zlasti dosežene rezultate s cilji letnega programa dela. Potem ko upravni odbor sprejme poročilo, ga pošlje Evropskemu parlamentu, Svetu, Komisiji, Računskemu sodišču, Evropskemu ekonomsko-socialnemu odboru in Odboru regij ter ga objavi.

### 2.2. Sistem upravljanja in nadzora

#### 2.2.1. Ugotovljena tveganja

Od ustanovitve leta 2004 je bila ENISA zunanje in notranje ocenjevana.

V skladu s členom 25 uredbe o ENISA je bila prva faza v tem procesu neodvisno ocenjevanje ENISA, ki ga je opravil zunanji odbor strokovnjakov v letu 2006/2007. Odbor<sup>41</sup> je v poročilu potrdil, da so prvotni politični cilji za ustanovitev ENISA in njeni prvotni cilji še vedno veljavni, opozoril pa je tudi na nekatere zadeve, ki jih je treba izboljšati.

Komisija je marca 2007 poročala o oceni za upravni odbor, ki je nato predložil svoja priporočila glede prihodnosti agencije in spremembah uredbe o ENISA<sup>42</sup>.

Junija 2007 je Komisija v sporočilu Evropskemu parlamentu in Svetu<sup>43</sup> predložila lastno oceno rezultatov zunanje ocene in priporočila upravnega odbora. S sporočilom, ki je vsebovalo tudi seznam vprašanj za nadaljnjo usmeritev razprav, je Komisija odprla tudi javno razpravo, na kateri je evropske zainteresirane strani pozvala k oddaji prispevkov<sup>44</sup>.

#### 2.2.2. Predvidene nadzorne metode

Glej točki 2.1 in 2.2.1.

### 2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

Plačila zahtevanih storitev ali študij pred izplačilom preveri osebje agencije, pri čemer upošteva pogodbene obveznosti, gospodarska načela ter dobro finančno prakso in dobro

<sup>41</sup> [http://ec.europa.eu/dgs/information\\_society/evaluation/studies/index\\_en.htm](http://ec.europa.eu/dgs/information_society/evaluation/studies/index_en.htm).

<sup>42</sup> Po členu 25 uredbe o ENISA. Celotno besedilo s pripombami, ki ga je sprejel upravni odbor ENISA, je na voljo na spletni strani: [http://enisa.europa.eu/pages/03\\_02.htm](http://enisa.europa.eu/pages/03_02.htm).

<sup>43</sup> Sporočilo Komisije Evropskemu parlamentu in Svetu o oceni Evropske agencije za varnost omrežij in informacij (ENISA), COM(2007) 285 konč., 1.6.2007: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52007DC0285:EN:NOT>.

<sup>44</sup> <http://ec.europa.eu/yourvoice/ipm/forms/dispatch?form=EnisaFuture&lang=en>.

prakso upravljanja. Določbe o preprečevanju goljufij (nadzor, zahteve za poročanje itn.) se vključijo v vse sporazume in pogodbe, ki jih sklenejo agencija in prejemniki plačil.



### 3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE\*

#### 3.1. Razdelek večletnega finančnega okvira in proračunske vrstice na strani odhodkov

- Obstoječe proračunske vrstice na strani odhodkov

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodka	Prispevek			
	Število / opis	dif./nedif. (45)	države EFTA <sup>46</sup>	države kandidatke <sup>47</sup>	tretje države	po členu 18(1)(aa) finančne uredbe
1.a Konkurenčnost za rast in zaposlovanje	09 02 03 01 Evropska agencija za varnost omrežij in informacij – subvencija iz naslovov 1 in 2	dif.	DA	NE	NE	NE
	09 02 03 02 Evropska agencija za varnost omrežij in informacij – subvencija iz naslova 3	dif.	DA	NE	NE	NE
5 Upravni odhodki	09 01 01 Odhodki za aktivno zaposlene na področju Informacijska družba in mediji	nedif.	NE	NE	NE	NE
	09 01 02 11 Odhodki za ostalo upravljanje	nedif.	NE	NE	NE	NE

\* Ta ocena učinka zakonodajnega predloga ne zajema ocenjenega finančnega učinka predloga za obdobje po veljavnem finančnem načrtu 2007–2013. Na podlagi Komisijinega predloga uredbe o večletnem finančnem okviru za obdobje po letu 2013 in ob upoštevanju sklepnih ugotovitev ocene učinka bo Komisija predložila spremenjeno oceno finančnega učinka.

<sup>45</sup> dif. = diferencirana sredstva, nedif. = nediferencirana sredstva

<sup>46</sup> EFTA: Evropsko združenje za prosto trgovino.

<sup>47</sup> Države kandidatke in, če je ustrezno, potencialne države kandidatke Zahodnega Balkana.

### 3.2. Ocenjeni učinek na odhodke

#### 3.2.1. Povzetek ocenjenega učinka na odhodke

v mio EUR (na tri decimalna mesta natančno)

<b>Razdelek večletnega finančnega okvira</b>	1.a	Konkurenčnost za rast in zaposlovanje
--	-----	---------------------------------------

ENISA			1. januar– 13. marec 2012	14. marec–31. december 2012	leto 2013	leto 2014	leto 2015	leto 2016	1. januar–13. marec 2017	<b>SKUPAJ 14. marec 2012–13. marec 2017</b>
Odobritve za poslovanje										
09 02 03 02 Evropska agencija za varnost omrežij in informacij – subvencija iz naslova 3	Obveznosti	(1)	0,454	1,976	2,470					
	Plačila	(2)	0,454	1,976	2,470					
Upravna sredstva										
09 02 03 01 Evropska agencija za varnost omrežij in informacij – subvencija iz naslovov 1 in 2		(3)	1,293	4,697	6,120					
<b>Odobritve za RAZDELEK 1a SKUPAJ</b>	Obveznosti	=1 +3	1,747	6,673	8,590					
	Plačila	=2+3	1,747	6,673	8,590					
Odobritve za	Obveznosti	(4)	0,454	1,976	2,470					

poslovanje SKUPAJ	Plačila	(5)	0,454	1,976	2,470					
Odobritve za upravne zadeve, ki se financirajo iz sredstev nekaterih programov, SKUPAJ		(6)	1,293	4,697	6,120					
<b>Odobritve v razdelku 1.a</b> okvirnega programa SKUPAJ	Obveznosti	=4+ 6	1,747	6,673	8,590					
	Plačila	=5+ 6	1,747	6,673	8,590					

v mio EUR (na tri decimalna mesta natančno)

<b>Razdelek večletnega finančnega okvira</b>	5	Upravni odhodki
--	---	-----------------

		1. januar– 13. marec 2012	14. marec–31. december 2012	leto 2013	leto 2014	leto 2015	leto 2016	1. januar–13. marec 2017	Skupaj
Človeški viri		0,085	0,342	0,427					
Drugi upravni dohodki		0,002	0,013	0,015					
SKUPAJ GD INFSO	Odobritve	0,087	0,355	0,442					

<b>Odobritve v RAZDELKU 5</b> večletnega finančnega okvira SKUPAJ	(obveznosti skupaj = plačila skupaj)	0,087	0,355	0,442					
---	--	-------	-------	-------	--	--	--	--	--

		1. januar– 13. marec 2012	14. marec– 31. decem ber 2012	leto 2013	leto 2014	leto 2015	leto 2016	1. januar– 13. marec 2017	Skupaj
<b>Odobritve v RAZDELKU 1 do 5</b> večletnega finančnega okvira SKUPAJ	Obveznosti	1,834	7,028	9,032					
	Plačila	1,834	7,028	9,032					

### 3.2.2. Ocenjeni učinek na odobritve za poslovanje

- Predlog/pobuda ne zahteva uporabe odobritev za poslovanje.
- Predlog/pobuda zahteva porabo odobritev za poslovanje, kot je pojasnjeno v nadaljevanju:

odobritve za prevzem obveznosti v mio EUR (na tri decimalna mesta natančno)

Cilji in njihova realizacija ↓	1. januar– 13. marec 2012	14. marec– 31. december 2012	leto 2013	leto 2014	leto 2015	leto 2016	1. januar– 13. marec 2017	14. marec 2012– 13. marec 2017 SKUPAJ
Skladnost regulativnih pristopov	0,114	0,494	0,620					
Preprečevanje, odkrivanje in odzivanje	0,114	0,494	0,620					
Povečanje znanja za oblikovalce politike	0,068	0,297	0,370					
Izboljšanje položaja zainteresiranih strani	0,050	0,218	0,270					
Zaščita Evrope pred mednarodnimi nevarnostmi	0,023	0,099	0,120					
Skupen pristop	0,064	0,276	0,340					
Boj proti kibernetickemu kriminalu	0,023	0,098	0,120					
<b>STROŠKI SKUPAJ</b>	0,454	1,976	2,460					

### 3.2.3. Ocenjeni učinek na odobritve za upravne zadeve<sup>48</sup>

#### 3.2.3.1. Povzetek

- Predlog/pobuda ne zahteva uporabe odobritev za poslovanje.
- Predlog/pobuda zahteva porabo odobritev za poslovanje, kot je pojasnjeno v nadaljevanju:

#### a) Upravni odhodki v razdelku 5 večletnega finančnega okvira

v mio EUR (na tri decimalna mesta natančno)

<b>RAZDELEK 5 večletnega finančnega okvira</b>	1. januar– 13. marec 2012	14. marec– 31. decem ber 2012	leto 2013	leto 2014	leto 2015	leto 2016	1. januar– 13. marec 2017	<b>14. marec 2012–13. marec 2017 SKUPAJ</b>
--	---------------------------------	--	-----------	--------------	--------------	--------------	---------------------------------	---

Človeški viri	0,085	0,342	0,427					
Drugi upravni dohodki	0,002	0,013	0,015					

<b>SKUPAJ</b>	<b>0,087</b>	<b>0,355</b>	<b>0,442</b>					
---------------	--------------	--------------	--------------	--	--	--	--	--

#### b) Upravni odhodki za ENISA – vsebovani v proračunski vrstici „09.020301 Varnost omrežij in informacij v Evropi: Naslov 1 – Osebj e in Naslov 2 – Delovanje agencije“.

v mio EUR (na tri decimalna mesta natančno)

	1. januar– 13. marec 2012	14. marec– 31. decem ber 2012	leto 2013	leto 2014	leto 2015	leto 2016	1. januar– 13. marec 2017	<b>14. marec 2012–13. marec 2017 SKUPAJ</b>
--	---------------------------------	--	-----------	--------------	--------------	--------------	---------------------------------	---

Človeški viri – naslov 1 – osebj e	1,153	4,329	5,607					
Drugi upravni dohodki Naslov 2 – delovanje agencije.	0,140	0,368	0,513					

<b>SKUPAJ</b>	<b>1,293</b>	<b>4,697</b>	<b>6,120</b>					
---------------	--------------	--------------	--------------	--	--	--	--	--

<sup>48</sup> Priloga ocene finančnih posledic predloga ni izpolnjena, ker se za trenutni predlog ne uporablja.

### 3.2.3.2. Ocenjene potrebe po človeških virih

Vsako leto se načrt delovnih mest agencije obrazloži in upraviči v t.i. načrtu kadrovske politike, ki se predloži proračunskemu organu.

- Predlog/pobuda ne zahteva uporabe odobritev za človeške vire.
- Predlog/pobuda zahteva porabo odobritev za človeške vire, kot je pojasnjeno v nadaljevanju:

#### a) Človeški viri Komisije

	1. januar– 13. marec 2012	14. marec– 31. decem ber 2012	leto 2013	leto 2014	leto 2015	leto 2016	1. januar– 13. marec 2017
<b>Načrt delovnih mest (za uradnike in začasno osebje)</b>							
XX 01 01 01 (sedeži in predstavništva Komisije)	3,5	3,5	3,5				
<b>SKUPAJ</b>	<b>3,5</b>	<b>3,5</b>	<b>3,5</b>				

#### b) Človeški viri ENISA

	1. januar– 13. marec 2012	14. marec– 31. decem ber 2012	leto 2013	leto 2014	leto 2015	leto 2016	1. januar– 13. marec 2017
<b>Načrt delovnih mest za ENISA (v ekvivalentih polnega delovnega časa)</b>							
Uradniki ali začasno osebje	AD	29	31	31			
	AST	15	16	16			
Uradniki ali začasno osebje <b>SKUPAJ</b>	<b>44</b>	<b>47</b>	<b>47</b>				
<b>Drugo osebje (v ekvivalentih polnega delovnega časa)</b>							
Pogodbeno osebje	13	14	14				
Napoteni nacionalni strokovnjaki	5	5	5				
Skupaj ostalo osebje	18	19	19				
<b>SKUPAJ</b>	<b>62</b>	<b>66</b>	<b>66</b>				

Opis nalog, ki jih opravlja osebje agencije:

Uradniki in začasni uslužbenci	<p>Agencija bo še naprej:</p> <ul style="list-style-type: none"> <li>– imela svetovalno in usklajevalno funkcijo, s katero bo <b>pridobivala in analizirala podatke</b> o varnosti informacij. Danes zbirajo podatke o incidentih IT in druge podatke o varnosti informacij javne in zasebne organizacije z različnimi cilji. Na evropski ravni ni centralnega organa, ki bi celovito zbral in analiziral podatke ter podajal mnenja in nasvete, s katerimi bi podprl politike Unije na področju varnosti omrežij in informacij;</li> <li>– <b>imela vlogo strokovnega centra</b>, pri katerem lahko države članice in evropske institucije dobijo <b>mnenja in nasvete glede tehničnih vprašanj</b> v zvezi z varnostjo;</li> <li>– prispevala k <b>širokemu sodelovanju med različnimi akterji</b> na področju varnosti informacij, npr. pomagala pri nadaljnjih dejavnostih pri podpori varnega e-poslovanja. Takšno sodelovanje je nujen predpogoj za varno delovanje omrežij in informacijskih sistemov v Evropi. Potrebna sta sodelovanje in udeležba vseh zainteresiranih strani;</li> <li>– prispevala k usklajenemu pristopu do varnosti informacij, tako da bo <b>podpirala države članice</b>, npr. pri <b>spodbujanju ocenjevanja tveganj</b> in dejavnosti ozaveščanja;</li> <li>– zagotavljala <b>medobratovalnost omrežij in informacijskih sistemov</b>, če države članice <b>uporabljajo</b> tehnične zahteve, ki vplivajo na varnost;</li> <li>– ugotavljala potrebe po <b>ustrezni standardizaciji</b> ter ocenjevala obstoječe varnostne standarde in sisteme potrjevanja ter spodbujala njihovo čim širšo uporabo v evropski zakonodaji;</li> <li>– podpirala <b>mednarodno sodelovanje</b> na tem vedno pomembnejšem področju, saj so vprašanja varnosti omrežij in informacij globalna.</li> </ul>
Zunanji sodelavci	Glej zgoraj



### 3.2.4. Skladnost z veljavnim večletnim finančnim okvirom

- Predlog/pobuda je skladna z veljavnim večletnim finančnim okvirom.
- – • Predlog/pobuda zahteva spremembo ustreznega razdelka večletnega finančnega okvira.
- – • Predlog/pobuda zahteva uporabo instrumenta prilagodljivosti ali spremembo večletnega finančnega okvira<sup>49</sup>.

Financiranje EU po letu 2013 bo preučeno v razpravi znotraj Komisije o vseh predlogih za obdobje po letu 2013. To pomeni, da ko bo Komisija skupaj s predlogom za naslednji večletni finančni okvir predložila tudi spremenjeno oceno učinka zakonodajnega predloga, pri čemer bo upoštevala sklepne ugotovitve ocene učinka.

### 3.2.5. Prispevki tretjih oseb

- Predlog/pobuda ne določa sofinanciranja tretjih oseb.
- Predlog/pobuda določa sofinanciranje, kot je ocenjeno v nadaljevanju:

Okvirne odobritve za prevzem obveznosti v mio EUR (na tri decimalna mesta natančno)

	1. januar– 13. marec 2012	14. marec– 31. decem ber 2012	leto 2013	leto 2014	leto 2015	leto 2016	1. januar– 13. marec 2017	<b>14. marec 2012–13. marec 2017 SKUPAJ</b>
EFTA	0,042	0,160	0,206					

### 3.3. Ocenjeni učinek na odhodke

- Predlog/pobuda nima finančnih posledic za prihodke.
- Predlog/pobuda ima naslednje finančne posledice:
  - na lastna sredstva
  - na druga sredstva

<sup>49</sup> Glej točki 19 in 24 medinstitucionalnega sporazuma.