EVROPSKA
KOMISIJA

Bruselj, 22.2.2018
COM(2017) 477 final/3

2017/0225 (COD)

CORRIGENDUM

This document corrects document COM(2017)477 final of 04.10.2017

Concerns all language versions.

Correction of errors of a clerical nature, correction of some references and adding the title of an article.

The text shall read as follows:

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti)

(Besedilo velja za EGP)

{SWD(2017) 500 final} - {SWD(2017) 501 final} - {SWD(2017) 502 final}

OBRAZLOŽITVENI MEMORANDUM

1. OZADJE PREDLOGA

• Razlogi za predlog in njegovi cilji

Evropska unija je sprejela številne ukrepe, da bi bila na področju kibernetske varnosti odpornejša in bolje pripravljena. V svoji prvi strategiji za kibernetsko varnost[1], sprejeti leta 2013, je EU določila strateške cilje in konkretne ukrepe, da bi dosegla odpornost, zmanjšala kibernetsko kriminaliteto, oblikovala politiko in razvila zmogljivosti kibernetske obrambe, razvila industrijske in tehnološke vire ter oblikovala skladno mednarodno politiko kibernetskega prostora za EU. Od tedaj so se na tem področju zvrstili pomembni dogodki, zlasti začetek drugega mandata Agencije Evropske unije za varnost omrežij in informacij (v nadaljnjem besedilu: agencija ENISA)[2] in sprejetje **direktive o varnosti omrežij in informacij**[3], na kateri temelji ta predlog.

Poleg tega je **Evropska komisija leta 2016 sprejela sporočilo o krepitvi odpornosti evropskega sistema kibernetske varnosti ter spodbujanju konkurenčne in inovativne industrije kibernetske varnosti**[4], v katerem je napovedala nadaljnje ukrepe za okrepitev sodelovanja ter izmenjavo znanja in informacij kot tudi za povečanje odpornosti in pripravljenosti EU, pri čemer je bila upoštevana tudi možnost velikih incidentov in morebitne vseevropske kibernetske krize. V tem okviru je Komisija napovedala zgodnejšo **oceno** in **revizijo** Uredbe (EU) št. 526/2013 Evropskega parlamenta in Sveta o agenciji Evropske unije za varnost omrežij in informacij (ENISA) in razveljavitvi Uredbe (ES) št. 460/2004 (v nadaljnjem besedilu: uredba o agenciji ENISA). Postopek ocenjevanja bi lahko vodil k morebitni reformi Agencije ter izboljšanju njenih zmožnosti in zmogljivosti za trajnostno podporo držav članic. Agenciji bi torej dal bolj operativno in osrednjo vlogo pri doseganju kibernetske odpornosti ter bi v njenem novem mandatu priznal nove pristojnosti Agencije v skladu z direktivo o varnosti omrežij in informacij.

Direktiva o varnosti omrežij in informacij je z uvedbo varnostnih zahtev kot pravnih obveznosti za ključne gospodarske akterje, zlasti izvajalce, ki zagotavljajo bistvene storitve (izvajalci bistvenih storitev – OBS), in dobavitelje nekaterih ključnih digitalnih storitev (ponudniki digitalnih storitev – PDS), prvi bistveni korak za spodbujanje kulture obvladovanja tveganj. Glede na varnostne zahteve, ki so dojemane kot bistvene za zaščito koristi razvijajoče se digitalizacije družbe, in glede na hitro širjenje povezanih naprav (internet stvari) je Komisija v sporočilu iz leta 2016 predložila tudi zamisel o vzpostavitvi okvira za varnostno certificiranje izdelkov in storitev IKT, da bi se povečala zaupanje in varnost na enotnem digitalnem trgu. Certificiranje kibernetske varnosti IKT je še posebej pomembno zaradi večje uporabe tehnologij, ki zahtevajo visoko raven kibernetske varnosti, kot so povezani in avtomatizirani avtomobili, elektronsko zdravje ali nadzorni sistemi industrijske avtomatizacije (IACS).

---

1 Skupno sporočilo Evropske komisije in Evropske službe za zunanje delovanje: Strategija Evropske unije za kibernetsko varnost: Odprt, varen in zanesljiv kibernetski prostor – JOIN(2013).

2 Uredba (EU) št. 526/2013 o agenciji Evropske unije za varnost omrežij in informacij (ENISA) in razveljavitvi Uredbe (ES) št. 460/2004.

3 Direktiva (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji.

4 Sporočilo Komisije „Krepitev odpornosti evropskega sistema kibernetske varnosti ter spodbujanje konkurenčne in inovativne industrije kibernetske varnosti“, COM/2016/0410 final.

Te ukrepe in napovedi politike so še dodatno podkrepili **sklepi Sveta** iz leta 2016, v katerih je bilo priznano, da se „pojavljajo [...] nove in še nevarnejše kibernetske grožnje ter šibke točke, zato bo treba nenehno in še tesneje sodelovati, zlasti pri obvladovanju velikih čezmejnih kibernetskih incidentov“. Svet je v sklepih potrdil, da je „Uredba o Agenciji Evropske unije za varnost omrežij in informacij (ENISA) [... eden izmed] osrednji[h] element[ov] okvira EU za odpornost kibernetske varnosti“[5] in pozval Komisijo, naj sprejme nadaljnje ukrepe za obravnavanje vprašanja certificiranja na evropski ravni.

Vzpostavitev sistema certificiranja bi zahtevala vzpostavitev ustreznega sistema upravljanja na ravni EU, vključno s temeljitim strokovnim znanjem, ki bi ga zagotavljala neodvisna agencija EU. V zvezi s tem ta predlog opredeljuje agencijo ENISA kot naraven organ na ravni EU, pristojen za kibernetsko varnost, ki bi moral prevzeti takšno vlogo za združevanje in usklajevanje dela nacionalnih pristojnih organov na področju certificiranja.

V svojem sporočilu o **vmesnem pregledu strategije za enotni digitalni trg maja 2017** je Komisija nadalje pojasnila, da bo do septembra 2017 revidirala mandat agencije ENISA. To bo storila, da bi opredelila njeno vlogo v spreminjajočem se ekosistemu kibernetske varnosti in oblikovala ukrepe glede standardov, certificiranja in označevanja kibernetske varnosti, s čimer bo poskrbela, da bodo sistemi, ki temeljijo na IKT, vključno s povezanimi predmeti, kibernetsko varnejši[6]. **Evropski svet je v sklepih** iz junija 2017[7] pozdravil namen Komisije, da septembra revidira strategijo za kibernetsko varnost in do konca leta 2017 predlaga nadaljnje ciljno usmerjene ukrepe.

Predlagana uredba določa celovit sklop ukrepov, ki temeljijo na prejšnjih ukrepih, in spodbuja posebne cilje, ki se vzajemno krepijo:

- povečanje **zmogljivosti in pripravljenosti** držav članic in podjetij;
- boljše **sodelovanje in usklajevanje** med državami članicami ter institucijami, agencijami in organi EU;
- povečanje **zmogljivosti na ravni EU, da se dopolni ukrepanje držav članic**, zlasti v primeru čezmejnih kibernetskih kriz;
- povečanje **ozaveščenosti** državljanov in podjetij o vprašanjih kibernetske varnosti;
- povečanje splošne **preglednosti zagotovil**[8] izdelkov in storitev IKT glede kibernetske varnosti za krepitev zaupanja v enotni digitalni trg in digitalne inovacije ter
- preprečevanje **razdrobljenosti certifikacijskih shem** v EU ter povezanih varnostnih zahtev in meril za ocenjevanje v različnih državah članicah in sektorjih.

Naslednji del obrazložitvenega memoranduma podrobneje pojasnjuje razloge za pobudo v zvezi s predlaganimi ukrepi za agencijo ENISA in certificiranje kibernetske varnosti.

---

5 Sklepi Sveta o krepitvi odpornosti evropskega sistema kibernetske varnosti ter spodbujanju konkurenčne in inovativne industrije kibernetske varnosti, 15. novembra 2016.

6 Sporočilo Komisije o vmesnem pregledu izvajanja strategije za enotni digitalni trg – COM(2017) 228.

7 Zasedanje Evropskega sveta (22. in 23. junija 2017) – sklepi EUCO 8/17.

8 Preglednost zagotovil kibernetske varnosti pomeni, da se uporabnikom zagotovi dovolj informacij o lastnostih kibernetske varnosti, ki jim omogočajo, da objektivno določijo raven varnosti zadevnega izdelka, storitve ali procesa IKT.

Agencija ENISA

Agencija ENISA deluje kot strokovno središče, namenjeno povečanju varnosti omrežij in informacij v Uniji ter podpiranju krepitve zmogljivosti držav članic.

Agencija ENISA je bila ustanovljena leta 2004[9], da bi prispevala k splošnemu cilju zagotavljanja visoke ravni varnosti omrežij in informacij v EU. Leta 2013 je bil z Uredbo (EU) št. 526/2013 vzpostavljen nov mandat Agencije za obdobje sedmih let, do leta 2020. Agencija ima prostore v Grčiji, in sicer upravni sedež v Heraklionu na Kreti in jedrne dejavnosti v Atenah.

Agencija ENISA je v primerjavi z drugimi agencijami EU majhna agencija z nizkim proračunom in majhnim številom zaposlenih. Ima mandat za določen čas.

Agencija ENISA podpira Evropske institucije, države članice in poslovno skupnost pri **obravnavanju težav v zvezi z varnostjo omrežij in informacij, odzivanju nanje ter zlasti njihovemu preprečevanju**. To počne z vrsto dejavnosti na petih področjih, opredeljenih v njeni strategiji[10]:

- strokovno znanje: zagotavljanje informacij in strokovnega znanja o ključnih vprašanjih varnosti omrežij in informacij;
- politika: podpora oblikovanju in izvajanju politik v Uniji;
- zmogljivost: podpora krepitvi zmogljivosti po vsej Uniji (npr. prek usposabljanj, priporočil, dejavnosti ozaveščanja);
- skupnost: spodbujanje skupnosti za varnost omrežij in informacij (npr. podpora skupinam za odzivanje na računalniške grožnje (CERT), usklajevanje vseevropskih kibernetskih vaj);
- omogočanje (npr. sodelovanja z zainteresiranimi stranmi in mednarodnih odnosov).

Med pogajanji o direktivi o varnosti omrežij in informacij sta se sozakonodajalca EU odločila, da agenciji ENISA dodelita pomembne vloge pri izvajanju navedene direktive. Agencija zlasti zagotavlja sekretariat za mrežo skupin CSIRT (vzpostavljeno za spodbujanje hitrega in učinkovitega operativnega sodelovanja med državami članicami v zvezi s posebnimi incidenti na področju kibernetske varnosti in za izmenjavo informacij o tveganjih), poklicana pa je tudi k pomoči skupini za sodelovanje pri izvrševanju njenih nalog. Poleg tega direktiva od agencije ENISA zahteva, da državam članicam in Komisiji pomaga s strokovnim znanjem in nasveti ter olajševanjem izmenjave najboljših praks.

V skladu z uredbo o agenciji ENISA je Komisija izvedla oceno Agencije, ki vključuje neodvisno študijo in javno posvetovanje. Ocena je ocenjevala ustreznost, učinek, uspešnost, učinkovitost, skladnost in dodano vrednost EU Agencije v zvezi z njenim delovanjem, upravljanjem, notranjo organizacijsko strukturo in delovnimi praksami v obdobju 2013–2016.

---

9 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.

10 https://www.enisa.europa.eu/publications/corporate/enisa-strategy

Večina anketirancev[11] (74 %) je v javnem posvetovanju pozitivno ocenila splošno delovanje agencije ENISA. Poleg tega je večina anketirancev menila, da agencija ENISA dosega svoje različne cilje (najmanj 63 % za vsak cilj). Storitve in izdelke agencije ENISA redno (vsak mesec ali pogosteje) uporablja skoraj polovica anketirancev (46 %) in so cenjeni, ker izvirajo iz organa na ravni EU (83 %) in ker so kakovostni (62 %).

Vendar je velika večina (88 %) anketirancev menila, da so zdajšnji instrumenti in mehanizmi, ki so na voljo na ravni EU, neustrezni ali le delno ustrezni za odzivanje na trenutne izzive v zvezi s kibernetsko varnostjo. Velika večina anketirancev (98 %) je navedla, da bi moral te potrebe obravnavati organ EU, in 99 % anketirancev je menilo, da je agencija ENISA ustrezna organizacija za ta namen. Poleg tega je 67,5 % anketirancev izrazilo stališče, da bi agencija ENISA lahko imela vlogo pri vzpostavitvi harmoniziranega okvira za varnostno certificiranje izdelkov in storitev IT.

S splošno oceno (ki ne temelji le na javnem posvetovanju, ampak tudi na številnih individualnih razgovorih, dodatnih ciljnih raziskavah in delavnicah) so bili doseženi naslednji sklepi:

- Cilji Agencije ENISA so še vedno ustrezni. Zaradi hitrega tehnološkega razvoja in spreminjajočih se groženj ter naraščajočih tveganj v zvezi s kibernetsko varnostjo v EU glede vprašanj kibernetske varnosti obstaja jasna potreba po spodbujanju in nadaljnji krepitvi tehničnega strokovnega znanja na visoki ravni. V državah članicah je treba okrepiti zmogljivosti za razumevanje in odzivanje na grožnje, zainteresirane strani pa morajo sodelovati na različnih tematskih področjih in medinstitucionalno.
- Kljub skromnemu proračunu je bila Agencija operativno učinkovita pri uporabi virov in izvajanju nalog. Vendar je delitev na lokaciji v Atenah in Heraklionu povzročila tudi dodatne upravne stroške.
- Kar zadeva uspešnost, je agencija ENISA delno dosegla svoje cilje. Agencija je uspešno prispevala k izboljšanju varnosti omrežij in informacij v Evropi z zagotavljanjem krepitve zmogljivosti v 28 državah članicah[12], izboljšanjem sodelovanja med državami članicami ter zainteresiranimi stranmi s področja varnosti omrežij in informacij kot tudi zagotavljanjem strokovnega znanja, oblikovanja skupnosti in podpore pri oblikovanju politik. Na splošno se je agencija ENISA skrbno osredotočala na izvajanje svojega delovnega programa in delovala kot zaupanja vreden partner za svoje zainteresirane strani na področju, ki mu je bil tako velik čezmejni pomen priznan šele pred kratkim.

---

[11] Na posvetovanje se je odzvalo 90 zainteresiranih strani iz 19 držav članic (88 odgovorov in 2 dokumenta o stališču), vključno z nacionalnimi organi iz 15 držav članic in 8 krovnimi organizacijami, ki predstavljajo znatno število evropskih podjetij.

[12] Anketiranci javnega posvetovanja so bili povprašani, kateri so po njihovem mnenju glavni dosežki agencije ENISA v obdobju 2013–2016. Anketiranci iz vseh skupin (skupaj 55, in sicer 13 iz nacionalnih organov, 20 iz zasebnega sektorja in 22 iz „drugo“) so kot glavne dosežke agencije ENISA navedli naslednje: 1) usklajevanje vaj na področju kibernetske varnosti Cyber Europe; 2) zagotavljanje podpore za skupine CERT/CSIRT z usposabljanjem in delavnicami za spodbujanje usklajevanja in izmenjave; 3) publikacije agencije ENISA (smernice in priporočila, poročila o naravi groženj, strategije za poročanje o incidentih ter krizno upravljanje itd.), ki se štejejo za koristne pri pripravi in posodobitvi nacionalnih varnostnih okvirov, pa tudi kot referenca za oblikovalce politik in strokovnjake iz prakse; 4) pomoč pri promociji direktive o varnosti omrežij in informacij; 5) prizadevanja za večjo ozaveščenost glede kibernetske varnosti z mesecem kibernetske varnosti.

- Agenciji ENISA je uspelo vsaj deloma pustiti pečat na obsežnem področju varnosti omrežij in informacij, vendar ji ni v celoti uspelo razviti močne blagovne znamke ter pridobiti zadostne prepoznavnosti, da bi postala priznana kot glavno strokovno središče v Evropi. Razlog za to je v širokem mandatu agencije ENISA, ki pa ni imela sorazmerno zadostnih virov. Poleg tega agencija ENISA ostaja edina agencija EU z mandatom za določen čas, kar omejuje njeno zmožnost razvoja dolgoročne vizije in trajnostne podpore zainteresiranih strani. To je v nasprotju z določbami direktive o varnosti omrežij in informacij, ki agenciji ENISA podeljuje naloge brez končnega roka. Poleg tega je bilo z oceno ugotovljeno, da se ta omejena uspešnost lahko delno pojasni z visoko odvisnostjo od zunanjega strokovnega znanja v primerjavi z notranjim in s težavami pri zaposlovanju in ohranitvi specializiranega osebja.
- Nenazadnje je bilo v oceni sklenjeno, da je dodana vrednost agencije ENISA zlasti v njeni zmožnosti, da izboljša sodelovanje predvsem med državami članicami in zlasti s povezanimi skupnostmi za varnost omrežij in informacij (zlasti med skupinami CSIRT). Na ravni EU ni nobenega drugega akterja, ki bi podpiral tako različne zainteresirane strani s področja varnosti omrežij in informacij. Vendar zaradi potrebe po strogem določanju prednostnih dejavnosti delovni program agencije ENISA večinoma usmerjajo potrebe držav članic. Zato ne obravnava v zadostni meri potreb drugih zainteresiranih strani, zlasti industrije. Poleg tega pa je iz istega razloga Agencija začela izpolnjevati potrebe svojih ključnih zainteresiranih strani, kar ji preprečuje, da bi dosegla večji učinek. Zato je dodana vrednost Agencije nihala glede na različne potrebe njenih zainteresiranih strani in obseg, v katerem se je nanje lahko odzvala (npr. velike in majhne države članice, države članice in industrija).

Če povzamemo, z rezultati posvetovanj z zainteresiranimi stranmi in oceno se je pokazalo, da je treba prilagoditi mandat in vire agencije ENISA, da bo lahko imela ustrezno vlogo pri odzivanju na sedanje in prihodnje izzive.

Glede na te ugotovitve se s tem predlogom revidira zdajšnji mandat agencije ENISA in določa prenovljen sklop nalog in funkcij, da bi uspešno in učinkovito podprla države članice, institucije EU in druge zainteresirane strani pri njihovih prizadevanjih za zagotovitev varnega kibernetskega prostora v Evropski uniji. Z novim predlaganim mandatom naj bi se Agenciji podelila močnejša in osrednejša vloga, zlasti s podporo državam članicam pri izvajanju direktive o varnosti omrežij in informacij ter dejavnejšim preprečevanjem posameznih groženj (operativna zmogljivost) in s tem, da postane strokovno središče v podporo državam članicam in Komisiji na področju certificiranja kibernetske varnosti. V okviru tega predloga:

- Agenciji ENISA bi bil podeljen stalni mandat, s čimer bi imela trdno podlago za prihodnost. Mandat, cilji in naloge bi se morali še vedno redno revidirati.
- Predlagani mandat dodatno pojasnjuje vlogo agencije ENISA kot agencije EU za kibernetsko varnost in kot referenčne točke v ekosistemu EU za kibernetsko varnost, ki deluje v tesnem sodelovanju z vsemi drugimi ustreznimi organi takega ekosistema.
- Organizacija in upravljanje Agencije, ki sta bila v oceni pozitivno ocenjena, bi bila zmerno revidirana, zlasti da se zagotovi, da so potrebe širše skupnosti zainteresiranih strani bolje upoštevane v delu Agencije.
- Predlagani obseg mandata je natančno določen, pri čemer so okrepljena področja, na katerih se je pokazalo, da ima Agencija jasno dodano vrednost, in dodana so nova področja, na katerih je potrebna podpora glede na nove prednostne naloge politik in instrumente, zlasti direktivo o varnosti omrežij in informacij, revizijo strategije EU

za kibernetsko varnost, prihodnji načrt EU za kibernetsko varnost na področju sodelovanja ob kibernetskih krizah in varnostno certificiranje IKT:

- **Oblikovanje in izvajanje politik EU:** Agenciji ENISA bi bila naložena naloga proaktivno prispevati k oblikovanju politik na področju varnosti omrežij in informacij ter drugih pobud politike z elementi kibernetske varnosti v različnih sektorjih (npr. energetiki, prometu in financah). V ta namen bi imela pomembno svetovalno vlogo, ki bi jo lahko izpolnila z zagotavljanjem neodvisnih mnenj in pripravljalnega dela za oblikovanje in posodobitev politike in prava. Agencija ENISA bi prav tako podpirala politiko in pravo EU na področjih elektronskih komunikacij, elektronske identifikacije in storitev zaupanja, da bi spodbujala višjo raven kibernetske varnosti. V fazi izvajanja, zlasti v okviru skupine za sodelovanje glede varnosti omrežij in informacij, bi agencija ENISA državam članicam pomagala pri doseganju doslednega pristopa k izvajanju direktive o varnosti omrežij in informacij v različnih državah in sektorjih ter drugih zadevnih politik in zakonodaje. V podporo rednemu pregledu politik in zakonodaje na področju kibernetske varnosti bi agencija ENISA zagotovila tudi redno poročanje o stanju izvajanja pravnega okvira EU.
- **Krepitev zmogljivosti:** Agencija ENISA bi prispevala k izboljšanju zmogljivosti in strokovnega znanja evropskih in nacionalnih javnih organov, tudi glede odzivanja na incidente in nadzora nad regulativnimi ukrepi, povezanimi s kibernetsko varnostjo. Od Agencije bi se prav tako zahtevalo, da z zagotavljanjem najboljših praks in smernic o razpoložljivih orodjih in postopkih ter ustreznim obravnavanjem regulativnih vprašanj, povezanih z izmenjavo informacij, prispeva k vzpostavitvi centrov za izmenjavo in analizo informacij (ISAC) v različnih sektorjih.
- **Znanje in obveščanje, ozaveščanje:** Agencija ENISA bi postala informacijsko vozlišče EU. To bi pomenilo promocijo in izmenjavo najboljših praks in pobud po vsej EU z združevanjem informacij o kibernetski varnosti, ki izvirajo iz institucij, agencij in organov na ravni EU in nacionalni ravni. Agencija bi prav tako nudila svetovanje, smernice in najboljše prakse o varnosti kritičnih infrastruktur. Po večjih čezmejnih kibernetskih incidentih bi agencija ENISA poleg tega pripravljala poročila, da bi zagotovila smernice za podjetja in državljane po vsej EU. Ta del nalog bi prav tako vključeval redno organizacijo dejavnosti ozaveščanja, usklajenih z organi držav članic.
- **S trgom povezane naloge (standardizacija, certificiranje kibernetske varnosti):** Agencija ENISA bi opravljala številne funkcije, ki posebej podpirajo notranji trg in zajemajo „tržni observatorij“ kibernetske varnosti, saj bi analizirala ustrezne trende na trgu kibernetske varnosti, s čimer bi se bolje usklajevala ponudba in povpraševanje, ter podpirala oblikovanje politike EU na področju standardizacije in certificiranja kibernetske varnosti izdelkov in storitev IKT. Zlasti v zvezi s standardizacijo bi olajšala vzpostavitev in uporabo standardov kibernetske varnosti. Agencija ENISA bi prav tako izvajala naloge, predvidene v okviru prihodnjega okvira za certificiranje (glej spodnji razdelek).
- **Raziskave in inovacije:** Agencija ENISA bi prispevala svoje strokovno znanje s svetovanjem organom EU in nacionalnim organom o določanju prednostnih nalog pri raziskavah in razvoju, vključno v okviru pogodbenega javno-

zasebnega partnerstva za kibernetsko varnost. Nasvete agencije ENISA glede raziskav bi uporabil novi evropski raziskovalni in strokovni center za kibernetsko varnost v naslednjem večletnem finančnem okviru. Agencija ENISA bi bila na zahtevo Komisije vključena tudi v izvajanje programov EU za financiranje raziskav in inovacij.

- **Operativno sodelovanje in krizno upravljanje:** Ta del nalog bi moral temeljiti na krepitvi obstoječih operativnih zmogljivosti preprečevanja, zlasti z nadgradnjo vseevropskih vaj na področju kibernetske varnosti (Cyber Europe), tako da se organizirajo letno, in s podporno vlogo pri operativnem sodelovanju kot sekretariat mreže skupin CSIRT (v skladu z določbami direktive o varnosti omrežij in informacij), pri čemer se med drugim zagotovi dobro delovanje informacijske infrastrukture in komunikacijskih kanalov navedene mreže. V tem okviru bi bilo potrebno strukturirano sodelovanje s skupino CERT-EU, Evropskim centrom za boj proti kibernetski kriminaliteti (EC3) in drugimi zadevnimi organi EU. Poleg tega bi moralo strukturirano sodelovanje s skupino CERT-EU v neposredni fizični bližini omogočiti zagotavljanje tehnične pomoči v primeru večjih incidentov in podpore pri analizi incidentov. Države članice, ki bi za to zaprosile, bi prejele pomoč za obvladovanje incidentov in podporo za analizo šibkih točk, artefaktov in incidentov, da si okrepijo lastne zmogljivosti preprečevanja in odzivanja.
- ENISA bi prav tako imela vlogo v **načrtu EU za kibernetsko varnost**, ki je predstavljen v tem svežnju in izraža priporočilo Komisije državam članicam za usklajen odziv na velike čezmejne kibernetske incidente in krize na ravni EU[13]. Agencija ENISA bi olajšala sodelovanje med posameznimi državami članicami pri odzivanju v izrednih razmerah z analizo in združevanjem nacionalnih poročil o stanju na podlagi informacij, ki so jih države članice in drugi subjekti prostovoljno dali na razpolago Agenciji.

- **Certificiranje izdelkov in storitev IKT glede kibernetske varnosti**

Za vzpostavitev in ohranitev zaupanja in varnosti, je treba v izdelke in storitve IKT neposredno vključiti varnostne lastnosti v zgodnjih fazah njihove tehnične zasnove in razvoja (vgrajena varnost). Poleg tega je treba omogočiti, da stranke in uporabniki lahko ugotovijo stopnjo zagotovila varnosti izdelkov in storitev, ki jih naročajo ali kupujejo.

Certificiranje, ki vsebuje formalno oceno izdelkov, storitev in postopkov s strani neodvisnega in akreditiranega organa glede na opredeljen sklop standardnih meril in izdajo certifikata o skladnosti, ima pomembno vlogo pri krepitvi zaupanja in varnosti izdelkov in storitev. Medtem ko so varnostne ocene dokaj tehnično področje, je namen certificiranja obveščati kupce in uporabnike ter jim dati zagotovila o varnostnih lastnostih izdelkov in storitev IKT, ki jih kupijo ali uporabljajo. Kot navedeno, je to zlasti pomembno za nove sisteme, ki obsežno uporabljajo digitalne tehnologije in zahtevajo visoko raven varnosti, kot so povezani in

[13] Ta načrt se bo uporabljal za kibernetske incidente, ki povzročijo obsežnejše motnje, kot bi jih lahko katera koli država članica obvladala sama, ali ki prizadenejo vsaj dve državi članici v tako veliki meri in s tako pomembnim učinkom ali političnim pomenom, da zahtevajo pravočasno politično usklajevanje in odziv na politični ravni Unije.

avtomatizirani avtomobili, elektronsko zdravje, nadzorni sistemi industrijske avtomatizacije (IACS)[14] ali pametna omrežja.

Trenutno je področje certificiranja izdelkov in storitev IKT glede kibernetske varnosti v EU precej neenotno. Obstaja več mednarodnih pobud, kot so t. i. skupna merila za oceno varnosti informacijske tehnologije (ISO 15408), ki je mednarodni standard za ocenjevanje varnosti računalniških sistemov. Temelji na oceni tretje strani in predvideva sedem stopenj zagotovila ocen (EAL). Skupna merila in spremljajoča skupna metodologija za oceno varnosti informacijske tehnologije so tehnična podlaga za mednarodni sporazum, dogovor o priznavanju skupnih meril, ki zagotavlja, da certifikate s skupnimi merili priznavajo vsi podpisniki dogovora o priznavanju skupnih meril. Vendar se po zdajšnji različici dogovora o priznavanju skupnih meril vzajemno priznavajo samo ocene do EAL 2. Poleg tega je dogovor podpisalo samo 13 držav članic.

Certifikacijski organi iz 12 držav članic so sklenili sporazum o vzajemnem priznavanju v zvezi s certifikati, izdanimi v skladu z dogovorom na podlagi skupnih meril[15]. Poleg tega v državah članicah trenutno obstaja več pobud za certificiranje IKT ali pa se vzpostavljajo. Te pobude so sicer pomembne, vendar pomenijo tveganje, da bi lahko prišlo do razdrobljenosti trga in težav z interoperabilnostjo. Posledično bi podjetje morda moralo opraviti več postopkov certificiranja v različnih državah članicah, da bi svoj izdelek lahko ponujalo na več trgih. Primer: proizvajalec pametnih števcev, ki želi svoje izdelke prodajati v treh državah članicah, npr. v Nemčiji, Franciji in Združenem kraljestvu, mora trenutno zagotavljati skladnost s tremi različnimi certifikacijskimi shemami: CPA (*Commercial Product Assurance*) v Združenem kraljestvu, CSPN (*Certification de Sécurité de Premier Niveau*) v Franciji in poseben profil zaščite, ki temelji na skupnih merilih, v Nemčiji.

Ta položaj povzroča višje stroške in pomeni znatno upravno breme za podjetja, ki poslujejo v več državah članicah. Čeprav se strošek certificiranja lahko močno razlikuje glede na zadevni izdelek/storitev, želeno stopnjo zagotovila ocene in/ali druge sestavne dele, je običajno za podjetja precej občuten. Cena certifikata BSI *Smart Meter Gateway* na primer znaša več kot milijon EUR (najvišja raven preskušanja in najvišja stopnja zagotovila, zadeva ne le en izdelek, ampak celotno infrastrukturo, povezano z njim). Stroški certificiranja pametnih števcev v Združenem kraljestvu znašajo skoraj 150 000 EUR. V Franciji so stroški podobni kot v Združenem kraljestvu, približno 150 000 EUR ali več.

Ključne javne in zasebne zainteresirane strani so navedle, da se morajo podjetja zaradi odsotnosti vseevropske certifikacijske sheme za kibernetsko varnost v številnih primerih certificirati v vsaki državi članici posebej, kar povzroča razdrobljenost trga. Še pomembneje je, da bi lahko ob odsotnosti harmonizacijske zakonodaje EU za izdelke in storitve IKT zaradi razlik v standardih in praksah certificiranja kibernetske varnosti v državah članicah v praksi nastalo 28 ločenih trgov varnosti v EU, pri čemer bi imel vsak svoje tehnične zahteve, metodologije preskušanja in postopke certificiranja kibernetske varnosti. Ti različni pristopi na nacionalni ravni lahko – če se ne bi ustrezno ukrepalo na ravni EU – zadajo precejšen

---

[14] GD JRC je objavil poročilo, v katerem predlaga začetni sklop skupnih evropskih zahtev in splošne smernice v zvezi s certificiranjem sestavnih delov IACS glede kibernetske varnosti. Na voljo na: https://erncip-project.jrc.ec.europa.eu/documents/introduction-european-iacs-components-cybersecurity-certification-framework-iccf

[15] Skupina visokih uradnikov za varnost informacijskih sistemov (SOG-IS) vključuje 12 držav članic in Norveško ter je pripravila nekaj profilov zaščite za omejeno število izdelkov, kot so digitalni podpis, digitalni tahograf in pametne kartice. Udeleženci sodelujejo pri usklajevanju standardizacije profilov zaščite skupnih meril in usklajujejo razvoj profilov zaščite. Države članice pogosto zahtevajo certificiranje SOG-IS za nacionalne razpise pri javnih naročilih.

udarec doseganju enotnega digitalnega trga, saj upočasnjujejo ali preprečujejo povezane pozitivne učinke na rast in delovna mesta.

Na podlagi navedenih dejstev predlagana uredba vzpostavlja evropski certifikacijski okvir za kibernetsko varnost (v nadaljnjem besedilu: **okvir**) za izdelke in storitve IKT ter podrobno določa bistvene funkcije in naloge agencije ENISA na področju certificiranja kibernetske varnosti. Ta predlog določa splošen okvir pravil, ki urejajo evropske certifikacijske sheme za kibernetsko varnost. Predlog neposredno ne uvaja operativnih certifikacijskih shem, temveč vzpostavlja sistem (okvir) za določitev posebnih certifikacijskih shem za posebne izdelke/storitve IKT (v nadaljnjem besedilu: evropske certifikacijske sheme za kibernetsko varnost). Oblikovanje evropskih certifikacijskih shem za kibernetsko varnost v skladu z okvirom bo omogočilo, da bodo certifikati, izdani na podlagi navedenih shem, veljavni in priznani v vseh državah članicah, ter bo obravnavalo zdajšnjo razdrobljenost trga.

Splošni namen evropske certifikacijske sheme za kibernetsko varnost je potrditi, da izdelki in storitve IKT, ki so bili certificirani v skladu s tako shemo, izpolnjujejo določene zahteve glede kibernetske varnosti. To bi na primer vključevalo njihovo zmožnost za varovanje podatkov (shranjenih, prenesenih ali drugače obdelanih) pred naključno ali nepooblaščeno hrambo, obdelavo, dostopom, razkritjem, uničenjem, naključno izgubo ali spremembo. Evropske certifikacijske sheme za kibernetsko varnost bi uporabile obstoječe standarde glede tehničnih zahtev in postopkov ocenjevanja, ki jih morajo izdelki izpolnjevati in same ne bi razvijale tehničnih standardov[16]. Na primer: certificiranje na ravni celotne EU za izdelke, kot so pametne kartice, ki se zdaj preskušajo glede na mednarodne standarde skupnih meril v okviru večstranske sheme SOG-IS (opisane zgoraj), bi pomenilo, da bi ta shema postala veljavna po vsej EU.

Poleg opredelitve posebnega sklopa varnostnih ciljev, ki jih je treba upoštevati pri oblikovanju posebne evropske certifikacijske sheme za kibernetsko varnost, predlog določa, kakšna bi morala biti minimalna vsebina takih shem. Take sheme bodo morale med drugim opredeliti številne posebne elemente, ki določajo področje uporabe in predmet certificiranja kibernetske varnosti. To vključuje določitev kategorij zajetih izdelkov in storitev, podrobno specifikacijo zahtev glede kibernetske varnosti (npr. s sklicevanjem na ustrezne standarde ali tehnične specifikacije), posebna merila in metode za ocenjevanje ter stopnjo zagotovila, ki naj bi jo zagotavljali (tj. osnovno, znatno ali visoko).

Evropske certifikacijske sheme za kibernetsko varnost bo pripravila agencija ENISA s pomočjo, strokovnim svetovanjem in v tesnem sodelovanju z Evropsko certifikacijsko skupino za kibernetsko varnost (glej spodaj), sprejela pa jih bo Komisija z izvedbenimi akti. Kadar se ugotovi potreba po certifikacijski shemi za kibernetsko varnost, bo Komisija od agencije ENISA zahtevala pripravo sheme za posamezne izdelke ali storitve IKT. Agencija ENISA bo shemo pripravljala v tesnem sodelovanju z nacionalnimi organi za nadzor nad certificiranjem, zastopanimi v skupini. Države članice in skupina lahko Komisiji predlagajo, naj od agencije ENISA zahteva pripravo posebne sheme.

Certificiranje je lahko zelo drag postopek, kar bi lahko privedlo do višjih cen za stranke in potrošnike. Potreba po certificiranju je lahko zelo različna tudi glede na posebne okoliščine uporabe izdelkov in storitev ter hitrost tehnoloških sprememb. Uporaba evropskega certificiranja kibernetske varnosti bi zato morala ostati prostovoljna, razen če je v zakonodaji Unije, ki določa varnostne zahteve za izdelke in storitve IKT, določeno drugače.

[16] V primeru evropskih standardov to opravijo evropske organizacije za standardizacijo in potrdi Evropska komisija z objavo v *Uradnem listu* (glej Uredbo (EU) št. 1025/2012).

Da pa bi zagotovili harmonizacijo in se izognili razdrobljenosti, se bodo nacionalne certifikacijske sheme ali postopki za kibernetsko varnost za izdelke in storitve IKT, ki jih zajema evropska certifikacijska shema za kibernetsko varnost, prenehali uporabljati od datuma, določenega v izvedbenem aktu, s katerim se sprejme shema. Poleg tega države članice ne bi smele uvajati novih nacionalnih certifikacijskih shem za kibernetsko varnost za izdelke in storitve IKT, ki jih zajema obstoječa evropska certifikacijska shema za kibernetsko varnost.

Ko bo sprejeta evropska certifikacijska shema za kibernetsko varnost, bodo proizvajalci izdelkov IKT ali ponudniki storitev IKT lahko vložili vlogo za certificiranje svojih izdelkov ali storitev pri organu za ugotavljanje skladnosti po lastni izbiri. Organe za ugotavljanje skladnosti bi moral akreditirati akreditacijski organ, če izpolnjujejo določene zahteve. Akreditacija bo izdana za obdobje največ petih let in se lahko pod enakimi pogoji podaljša, če organ za ugotavljanje skladnosti izpolnjuje zahteve. Akreditacijski organi bodo preklicali akreditacijo organa za ugotavljanje skladnosti, če pogoji za akreditacijo niso ali niso več izpolnjeni ali če ukrepi, ki jih sprejme organ za ugotavljanje skladnosti, kršijo to uredbo.

V skladu s predlogom so naloge spremljanja, nadzora in izvrševanja predpisov v pristojnosti držav članic. Države članice bodo morale zagotoviti organ za nadzor nad certificiranjem. Ta organ bo zadolžen za nadzor nad skladnostjo organov za ugotavljanje skladnosti in certifikatov, ki so jih izdali organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, z zahtevami iz te uredbe in zadevnih evropskih certifikacijskih shem za kibernetsko varnost. Nacionalni organi za nadzor nad certificiranjem bodo pristojni za obravnavanje pritožb, ki jih vložijo fizične ali pravne osebe v zvezi s certifikati, ki jih izdajo organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju. V ustrezni meri bodo preiskali vsebino pritožbe in pritožnika v razumnem roku obvestili o napredku in izidih preiskave. Poleg tega bodo sodelovali z ostalimi organi za nadzor nad certificiranjem ali drugimi javnimi organi, npr. z izmenjavo informacij o morebitni neskladnosti izdelkov in storitev IKT z zahtevami iz te uredbe ali posebnih evropskih certifikacijskih shem za kibernetsko varnost.

Poleg tega predlog vzpostavlja Evropsko certifikacijsko skupino za kibernetsko varnost (v nadaljnjem besedilu: skupina), ki jo sestavljajo nacionalni organi za nadzor nad certificiranjem iz vseh držav članic. Glavna naloga skupine je svetovati Komisiji glede vprašanj v zvezi s politiko certificiranja kibernetske varnosti in sodelovati z agencijo ENISA pri razvoju osnutka evropskih certifikacijskih shem za kibernetsko varnost. Agencija ENISA bo Komisiji pomagala pri zagotavljanju sekretariata skupine in vzdrževala posodobljen javni seznam shem, odobrenih na podlagi evropskega certifikacijskega okvira za kibernetsko varnost. Agencija ENISA bi prav tako sodelovala z organi za standardizacijo, da se zagotovi ustreznost standardov, uporabljenih v odobrenih shemah, in določijo področja, za katera so potrebni standardi glede kibernetske varnosti.

Evropski certifikacijski okvir za kibernetsko varnost (v nadaljnjem besedilu: okvir) bo državljanom in podjetjem prinesel več koristi. Zlasti:

- Oblikovanje certifikacijskih shem za kibernetsko varnost na ravni celotne EU za posamezne izdelke ali storitve bo podjetjem zagotovilo enotno kontaktno točko za certificiranje kibernetske varnosti v EU. Taka podjetja bodo lahko svoj izdelek certificirala le enkrat in pridobila certifikat, veljaven v vseh državah članicah. Izdelkov jim ne bo treba ponovno certificirati pri različnih nacionalnih organih za certificiranje. To bo znatno znižalo stroške za podjetja, olajšalo čezmejno poslovanje ter posledično zmanjšalo in preprečilo razdrobljenost notranjega trga za zadevne izdelke.

- Okvir določa primat evropskih certifikacijskih shem za kibernetsko varnost nad nacionalnimi shemami: na podlagi tega pravila bo sprejetje evropske certifikacijske sheme za kibernetsko varnost nadomestilo vse obstoječe vzporedne nacionalne sheme za iste izdelke ali storitve IKT na dani stopnji zagotovila. To bo prineslo večjo jasnost, zmanjšalo zdajšnje širjenje prekrivajočih se in potencialno nasprotujočih si nacionalnih certifikacijskih shem za kibernetsko varnost.
- Predlog podpira in dopolnjuje izvajanje direktive o varnosti omrežij in informacij tako, da podjetjem, za katera velja direktiva, zagotavlja zelo uporabno orodje za dokazovanje skladnosti z zahtevami iz direktive o varnosti omrežij in informacij v celotni Uniji. Pri oblikovanju novih certifikacijskih shem za kibernetsko varnost bosta Komisija in agencija ENISA namenili posebno pozornost potrebi, da se zagotovi, da so zahteve iz direktive o varnosti omrežij in informacij izražene v certifikacijskih shemah za kibernetsko varnost.
- Predlog bo s harmonizacijo pogojev in vsebinskih zahtev glede certificiranja izdelkov in storitev IKT v EU v zvezi s kibernetsko varnostjo podpiral in olajšal oblikovanje evropske politike kibernetske varnosti. Evropske certifikacijske sheme za kibernetsko varnost se bodo sklicevale na skupne standarde ali merila za ocenjevanje in metodologije preskušanja. To bo znatno, čeprav posredno, prispevalo k uvajanju skupnih varnostnih rešitev v EU, kar bo odpravljalo tudi ovire za notranji trg.
- Okvir je zasnovan tako, da zagotavlja potrebno prožnost za certifikacijske sheme za kibernetsko varnost. Glede na posebne potrebe na področju kibernetske varnosti se izdelek ali storitev lahko certificira po višjih ali nižjih ravneh varnosti. Evropske certifikacijske sheme za kibernetsko varnost bodo zasnovane ob upoštevanju te prožnosti in bodo zato zagotavljale različne stopnje zagotovil (tj. osnovno, znatno ali visoko), da bi jih bilo mogoče uporabiti za različne namene ali v različnih okvirih.
- Zaradi vseh zgoraj navedenih elementov bo certificiranje kibernetske varnosti kot učinkovito sredstvo za sporočanje stopnje zagotovila izdelkov in storitev IKT glede kibernetske varnosti postalo privlačnejše za podjetja. Kolikor bo certificiranje kibernetske varnosti manj drago, učinkovitejše in komercialno privlačnejše, več spodbud bo za podjetja, da certificirajo svoje izdelke za tveganja v zvezi s kibernetsko varnostjo, kar bo prispevalo k širjenju boljših praks na področju kibernetske varnosti pri zasnovi izdelkov in storitev IKT (vgrajena kibernetska varnost).

- **Skladnost z veljavnimi predpisi s področja zadevne politike**

V skladu z direktivo o varnosti omrežij in informacij morajo izvajalci v sektorjih, ki so ključni za naše gospodarstvo in družbo, npr. energetika, promet, vodni sektor, bančništvo, infrastrukture finančnih trgov, zdravstvo in digitalna infrastruktura, ter ponudniki digitalnih storitev (tj. iskalniki, storitve računalništva v oblaku in spletne tržnice) sprejeti ukrepe za ustrezno obvladovanje varnostnih tveganj. Nova pravila iz tega predloga dopolnjujejo in zagotavljajo skladnost z določbami direktive o varnosti omrežij in informacij, da bi bila z boljšimi zmogljivostmi, sodelovanjem, obvladovanjem tveganj in kibernetsko ozaveščenostjo kibernetska odpornost EU še boljša.

Poleg tega pravila glede certificiranja kibernetske varnosti zagotavljajo bistveno orodje za podjetja, za katera se uporablja direktiva o varnosti omrežij in informacij, saj bodo svoje izdelke in storitve IKT lahko certificirala za tveganja v zvezi s kibernetsko varnostjo na

podlagi certifikacijskih shem za kibernetsko varnost, veljavnih in priznanih po vsej EU. Prav tako bodo dopolnjevala varnostne zahteve iz uredbe eIDAS[17] in direktive o radijski opremi[18].

- **Skladnost z drugimi politikami Unije**

Uredba (EU) 2016/679 (v nadaljnjem besedilu: **Splošna uredba o varstvu podatkov**)[19] vsebuje določbe za vzpostavitev certifikacijskih mehanizmov ter pečatov in označb za varstvo podatkov za namen dokazovanja, da so postopki obdelave, ki jih uporabljajo upravljavci in obdelovalci, skladni s to uredbo. Ta uredba ne posega v certificiranje postopkov obdelave podatkov na podlagi Splošne uredbe o varstvu podatkov, tudi kadar so taki postopki vgrajeni v izdelke in storitve.

Predlagana uredba bo zagotovila skladnost z Uredbo (ES) št. 765/2008 o zahtevah za akreditacijo in nadzor trga[20] s sklicevanjem na pravila navedenega okvira o nacionalnih akreditacijskih organih in organih za ugotavljanje skladnosti. Kar zadeva nadzorne organe, bo predlagana uredba od držav članic zahtevala, da imenujejo nacionalne organe za nadzor nad certificiranjem, ki so pristojni za nadzor, spremljanje in izvrševanje predpisov. Navedeni organi bodo še naprej ločeni od organov za ugotavljanje skladnosti, kot to določa Uredba (ES) št. 765/2008.

2. PRAVNA PODLAGA, SUBSIDIARNOST IN SORAZMERNOST

- **Pravna podlaga**

Pravna podlaga za ukrepe EU je člen 114 Pogodbe o delovanju Evropske unije (PDEU), ki se nanaša na približevanje zakonov držav članic za dosego ciljev iz člena 26 PDEU, in sicer pravilnega delovanja notranjega trga.

Pravno podlago notranjega trga za ustanovitev agencije ENISA je potrdilo Sodišče (v zadevi C-217/04 *Združeno kraljestvo proti Evropskemu parlamentu in Svetu*), nato jo je ponovno potrdila uredba iz leta 2013, ki je določila zdajšnji mandat Agencije. Poleg tega bi dejavnosti, ki bi izražale cilje okrepitve sodelovanja in usklajevanja med državami članicami, ter dejavnosti, ki bi povečale zmogljivosti EU za dopolnitev ukrepov držav članic, sodile v kategorijo „operativnega sodelovanja“. To je posebej določeno v direktivi o varnosti omrežij in informacij (katere pravna podlaga je člen 114 PDEU) kot cilj, ki ga je treba doseči v okviru mreže skupin CSIRT, pri čemer „ENISA zagotovi sekretariat in dejavno podpira sodelovanje“ (člen 12(2)). Člen 12(3)(f) zlasti dodatno določa nadaljnje oblike operativnega sodelovanja kot nalogo mreže skupin CSIRT, vključno v zvezi s: (i) kategorijami tveganj in incidentov, (ii) zgodnjimi opozorili, (iii) medsebojno pomočjo ter (iv) načeli in načini usklajevanja pri odzivanju držav članic na čezmejna tveganja in incidente.

---

17 Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES.

18 Direktiva 2014/53/EU Evropskega parlamenta in Sveta z dne 16. aprila 2014 o harmonizaciji zakonodaj držav članic v zvezi z dostopnostjo radijske opreme na trgu in razveljavitvi Direktive 1999/5/ES.

19 Uredba (EU) 2016/679 Evropskega parlamenta in Sveta z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov) (UL L 119, 4.5.2016, str. 1–88).

20 Uredba (ES) št. 765/2008 o določitvi zahtev za akreditacijo in nadzor trga v zvezi s trženjem proizvodov ter razveljavitvi Uredbe (EGS) št. 339/93.

- Zdajšnja razdrobljenost certifikacijskih shem za izdelke in storitve IKT je tudi posledica pomanjkanja skupnega pravno zavezujočega in učinkovitega okvira, ki se uporablja za države članice. To ovira vzpostavitev notranjega trga za izdelke in storitve IKT ter konkurenčnost evropske industrije v tem sektorju. Namen tega predloga je z zagotovitvijo skupnega okvira za vzpostavitev certifikacijskih shem za kibernetsko varnost, ki bi veljale po vsej EU, obravnavati obstoječo razdrobljenost in z njo povezane ovire za notranji trg.

Subsidiarnost (za neizključno pristojnost)

Načelo subsidiarnosti zahteva oceno nujnosti in dodane vrednosti ukrepanja EU. Upoštevanje subsidiarnosti na tem področju je bilo priznano že pri sprejetju zdajšnje uredbe o agenciji ENISA[21].

Kibernetska varnost je vprašanje skupnega interesa Unije. Medsebojna odvisnost omrežij in informacijskih sistemov je tolikšna, da se posamezni akterji (javni in zasebni, vključno z državljani) zelo pogosto ne morejo sami spopadati z grožnjami ter obvladovati tveganj in morebitnih posledic kibernetskih incidentov. Na eni strani je zaradi medsebojnih odvisnosti po državah članicah, tudi kar zadeva delovanje kritičnih infrastruktur (energetika, promet, vodni sektor, če omenimo le nekatere), javno posredovanje na evropski ravni ne le koristno, temveč tudi potrebno. Po drugi strani lahko ukrepanje EU prinese pozitiven učinek „prelivanja“ zaradi izmenjave dobrih praks med državami članicami, kar lahko izboljša kibernetsko varnost Unije.

Če povzamemo, se v trenutnih razmerah in zroč v prihodnje scenarije zdi, da za **povečanje kolektivne kibernetske odpornosti** Unije **ukrepi posameznih držav članic EU in razdrobljen pristop h kibernetski varnosti** ne bodo zadostovali.

Ukrepanje na ravni EU se prav tako šteje za potrebno za obravnavanje razdrobljenosti zdajšnjih certifikacijskih shem za kibernetsko varnost. To bi proizvajalcem omogočilo, da z znatnimi prihranki pri stroških preskušanja in preoblikovanja v celoti izkoristijo notranji trg. Čeprav so bili na primer z zdajšnjim sporazumom o vzajemnem priznavanju (MRA) skupine visokih uradnikov za varnost informacijskih sistemov (SOG-IS) v zvezi s tem doseženi pomembni rezultati, so se prav tako pokazale pomembne omejitve, ki ovirajo njegovo primernost za zagotavljanje dolgoročnejših trajnostnih rešitev pri polnem izkoriščanju notranjega trga.

Dodana vrednost ukrepanja na ravni EU, zlasti za boljše sodelovanje med državami članicami, a tudi med skupnostmi na področju varnosti omrežij in informacij, je bila priznana s sklepi Sveta iz leta 2016[22] in prav tako jasno izhaja iz ocene agencije ENISA.

- **Sorazmernost**

Predvideni ukrepi so strogo omejeni na to, kar je potrebno za dosego ciljev. Poleg tega obseg posredovanja EU ne ovira kakršnih koli dodatnih nacionalnih ukrepov na področju nacionalne varnosti. Ukrepanje EU je zato utemeljeno na podlagi subsidiarnosti in sorazmernosti.

---

[21] Uredba (EU) št. 526/2013 Evropskega parlamenta in Sveta z dne 21. maja 2013 o agenciji Evropske unije za varnost omrežij in informacij (ENISA) in razveljavitvi Uredbe (ES) št. 460/2004.

[22] Sklepi Sveta o krepitvi odpornosti evropskega sistema kibernetske varnosti ter spodbujanju konkurenčne in inovativne industrije kibernetske varnosti, 15. novembra 2016.

- **Izbira instrumenta**

Ta predlog pregleduje Uredbo (EU) št. 526/2013, ki določa zdajšnji mandat in naloge agencije ENISA. Glede na pomembno vlogo agencije ENISA pri vzpostavljanju in upravljanju certifikacijskega okvira EU za kibernetsko varnost, je nov mandat in navedeni okvir najbolje vzpostaviti z enim samim pravnim instrumentom, in sicer z uredbo.

3. REZULTATI NAKNADNIH OCEN, POSVETOVANJ Z ZAINTERESIRANIMI STRANMI IN OCEN UČINKA

Naknadne ocene/preverjanja ustreznosti obstoječe zakonodaje

Komisija je v skladu s časovnim načrtom ocenjevanja[23] ocenila **ustreznost, učinek, uspešnost, učinkovitost, skladnost in dodano vrednost** Agencije v zvezi z njenim delovanjem, upravljanjem, notranjo organizacijsko strukturo in delovnimi praksami v obdobju 2013–2016. Glavne ugotovitve je mogoče povzeti kot sledi (za več informacij glej delovni dokument služb Komisije o zadevi, ki je priložen oceni učinka).

- **Ustreznost:** Glede na tehnološki razvoj in spreminjajoče se grožnje ter upoštevajoč znatno potrebo po večji kibernetski varnosti v EU so se cilji agencije ENISA izkazali za ustrezne. Tudi dejansko so države članice in organi EU odvisni od njenega znatnega strokovnega znanja v zadevah na področju kibernetske varnosti. Poleg tega je v državah članicah treba vzpostaviti zmogljivosti za boljše razumevanje groženj in odzivanje nanje, zainteresirane strani pa morajo sodelovati na različnih tematskih področjih in medinstitucionalno. Kibernetska varnost je še vedno ključna politična prednostna naloga EU, na katero naj bi se agencija ENISA odzivala, vendar zasnova agencije ENISA kot agencije EU z mandatom za določen čas: (i) ne omogoča dolgoročnega načrtovanja in trajnostne podpore državam članicam in institucijam EU; (ii) lahko povzroči pravno praznino, ker so določbe direktive o varnosti omrežij in informacij, ki agenciji ENISA podeljujejo naloge, trajne narave[24]; (iii) ni dovolj usklajena z vizijo, ki povezuje agencijo ENISA z izboljšanim ekosistemom EU za kibernetsko varnost.
- **Uspešnost:** Agencija ENISA je na splošno dosegla svoje cilje in izvedla svoje naloge. S svojimi glavnimi dejavnostmi (krepitvijo zmogljivosti, zagotavljanjem strokovnega znanja, oblikovanjem skupnosti in podporo politiki) je prispevala k večji varnosti omrežij in informacij v Evropi. Vendar so glede vsake izmed njih možne izboljšave. V oceni je bilo ugotovljeno, da je agencija ENISA uspešno ustvarila trdna razmerja, polna zaupanja, z nekaterimi svojimi zainteresiranimi stranmi, zlasti z državami članicami in mrežo skupin CSIRT. Ukrepi na področju krepitve zmogljivosti so se zdeli učinkoviti zlasti za države članice z manj viri. Spodbujanje širokega sodelovanja je bil eden od glavnih dosežkov, pri čemer je bilo med zainteresiranimi stranmi široko soglasje o pozitivni vlogi, ki jo ima agencija ENISA pri združevanju ljudi. Vendar se je agencija ENISA spopadala s težavami pri puščanju velikega pečata na prostranem področju varnosti omrežij in informacij. To je tudi posledica dejstva, da je imela dokaj omejene človeške in finančne vire za uresničevanje zelo širokega mandata. V oceni je bilo ugotovljeno tudi, da je agencija ENISA delno izpolnila cilje zagotavljanja strokovnega znanja, kar je povezano s težavami pri zaposlovanju strokovnjakov (glej tudi spodnji razdelek o učinkovitosti).

[23] http://ec.europa.eu/smart-regulation/roadmaps/docs/2017_cnect_002_evaluation_enisa_en.pdf

[24] Sklici na člene 7, 9, 11, 12 in 19 direktive o varnosti omrežij in informacij.

- **Učinkovitost**: Kljub skromnemu proračunu – enemu najmanjših v primerjavi z drugimi agencijami EU – je Agencija lahko prispevala k usmerjenim ciljem, pri čemer je izkazovala splošno učinkovitost pri uporabi virov. Z oceno je bilo ugotovljeno, da so bili postopki na splošno učinkoviti in da je jasna razmejitev odgovornosti znotraj organizacije pripomogla k dobro opravljenemu delu. Eden glavnih izzivov glede učinkovitosti Agencije se nanaša na težave agencije ENISA pri zaposlovanju in ohranitvi visoko usposobljenih strokovnjakov. Ugotovitve kažejo, da je to mogoče razložiti s kombinacijo dejavnikov, vključno s splošnimi težavami v celotnem javnem sektorju, da tekmuje z zasebnim sektorjem pri prizadevanjih za zaposlovanje visoko specializiranih strokovnjakov, vrsto pogodb (za določen čas), ki jih Agencija pretežno lahko ponudi, ter nekoliko nižjo privlačnostjo, ki je povezana z lokacijo agencije ENISA, na primer zaradi težav, s katerimi se soočajo zakonci zaposlenih pri iskanju zaposlitve. Delitev na lokaciji v Atenah in Heraklionu je zahtevala dodatne napore glede usklajevanja in povzročila dodatne stroške, vendar je selitev jedrnih dejavnosti v Atene leta 2013 povečala operativno učinkovitost Agencije.
- **Skladnost**: Dejavnosti agencije ENISA so bile na splošno skladne s politikami in dejavnostmi njenih zainteresiranih strani na nacionalni ravni in ravni EU, vendar je potreben bolj usklajen pristop h kibernetski varnosti na ravni EU. Možnosti za sodelovanje med agencijo ENISA in drugimi organi EU niso bile v celoti izkoriščene. Z razvojem pravnega in političnega okolja EU je zdajšnji mandat danes manj skladen.
- **Dodana vrednost EU**: Dodana vrednost agencije ENISA je predvsem v njeni zmožnosti, da izboljša sodelovanje, predvsem med državami članicami, a tudi s povezanimi skupnostmi na področju varnosti omrežij in informacij. Na ravni EU ni nobenega drugega akterja, ki podpira sodelovanje tako različnih zainteresiranih strani glede varnosti omrežij in informacij. Dodana vrednost Agencije je bila različna glede na različne potrebe in vire zainteresiranih strani (npr. velike in majhne države članice, države članice in industrija) ter glede na potrebo, da Agencija opredeli svoje prednostne dejavnosti v skladu z delovnim programom. Sklep iz ocene je, da bi morebitno prenehanje delovanja agencije ENISA pomenilo zamujeno priložnost za vse države članice. Zagotoviti enako stopnjo oblikovanja skupnosti in sodelovanja med državami članicami na področju kibernetske varnosti ne bo mogoče. Brez bolj centralizirane agencije EU bi bila slika bolj razdrobljena, praznino, ki bi jo zapustila agencija ENISA pa bi začelo zapolnjevati bilateralno ali regionalno sodelovanje.

Konkretno, kar zadeva preteklo in prihodnjo delovanje agencije ENISA, so glavni trendi, ki izhajajo iz posvetovanja leta 2017, naslednji[25]:

- Splošno delovanje agencije ENISA v obdobju od 2013 do 2016 je pozitivno ocenila večina anketirancev (74 %). Poleg tega je večina anketirancev menila, da agencija ENISA dosega svoje različne cilje (najmanj 63 % za vsak cilj). Storitve in izdelke

[25] Na posvetovanje se je odzvalo 90 zainteresiranih strani iz 19 držav članic (88 odgovorov in 2 dokumenta o stališču), tudi nacionalni organi iz 15 držav članic, vključno s Francijo, Italijo, Irsko in Grčijo, ter 8 krovnih organizacij, ki zastopajo veliko število evropskih organizacij, npr. Združenje evropskih bank, digitalna Evropa (ki zastopa industrijo digitalne tehnologije v Evropi), Združenje evropskih operaterjev telekomunikacijskih omrežij (ETNO). Javno posvetovanje o agenciji ENISA je bilo dopolnjeno s številnimi drugimi viri, vključno s: (i) temeljitimi razgovori s približno 50 ključnimi akterji v skupnosti kibernetske varnosti; (ii) raziskavo o mreži skupin CSIRT; (iii) raziskavo o upravnem odboru, izvršnem odboru, stalni skupini zainteresiranih strani agencije ENISA.

agencije ENISA redno (vsak mesec ali pogosteje) uporablja skoraj polovica anketirancev (46 %) in so cenjeni, ker izvirajo iz organa na ravni EU (83 %) in ker so kakovostni (62 %).

- Anketiranci so navedli številne vrzeli in izzive za prihodnost kibernetske varnosti v EU, med prvimi petimi (na seznamu 16) so bili zlasti: sodelovanje med državami članicami; zmogljivosti za preprečevanje, odkrivanje in reševanje velikih kibernetskih napadov; sodelovanje med državami članicami v zadevah, povezanih s kibernetsko varnostjo; sodelovanje in izmenjava informacij med različnimi zainteresiranimi stranmi, vključno s sodelovanjem med javnim in zasebnim sektorjem; zaščita kritične infrastrukture pred kibernetskimi napadi.
- Vendar je velika večina (88 %) anketirancev menila, da so zdajšnji instrumenti in mehanizmi, ki so na voljo na ravni EU, nezadostni ali za reševanje navedenega le delno ustrezni. Velika večina anketirancev (98 %) je navedla, da bi se moral na te potrebe odzivati organ EU, in od teh jih je 99 % menilo, da je agencija ENISA ustrezna organizacija za ta namen.

Posvetovanja z zainteresiranimi stranmi

- Komisija je organizirala javno posvetovanje glede revizije agencije ENISA med 12. aprilom in 5. julijem 2016 ter prejela 421 odgovorov[26]. V skladu z rezultati je 67,5 % anketirancev izrazilo stališče, da bi agencija ENISA lahko imela vlogo pri vzpostavitvi harmoniziranega okvira za varnostno certificiranje izdelkov in storitev IT.

Rezultati posvetovanja iz leta 2016 o javno-zasebnem partnerstvu za kibernetsko varnost[27] v razdelku o certificiranju kažejo, da:

- 50,4 % (tj. 121 od 240) anketirancev ne ve, ali so nacionalne certifikacijske sheme vzajemno priznane v državah članicah EU. 25,8 % (62 od 240) jih je odgovorilo z „ne“, 23,8 % (57 od 240) pa z „da“;
- 37,9 % anketirancev (91 od 240) jih je menilo, da obstoječe certifikacijske sheme ne podpirajo potreb evropske industrije. Po drugi strani je 17,5 % (42 od 240) – predvsem globalnih podjetij, ki delujejo na evropskem trgu – izrazilo nasprotno mnenje;
- 49,6 % (119 od 240) anketirancev pravi, da ni lahko dokazati enakovrednosti standardov, certifikacijskih shem in oznak. 37,9 % (91 od 240) jih je odgovorilo z „ne vem“, medtem ko jih je le 12,5 % (30 od 240) odgovorilo z „da“.

Zbiranje in uporaba strokovnih mnenj

Komisija je upoštevala naslednje nasvete zunanjih strokovnjakov:

- Študija o oceni agencije ENISA (Ramboll/Carsa, 2017; SMART št. 2016/0077),

[26] 162 prispevkov državljanov, 33 iz civilne družbe in potrošniških organizacij; 186 iz industrije in 40 iz javnih organov, vključno s pristojnimi organi, ki izvršujejo Direktivo o zasebnosti in elektronskih komunikacijah.

[27] Na razdelek o certificiranju se je odzvalo 240 zainteresiranih strani iz nacionalnih javnih uprav, velikih podjetij, malih in srednjih podjetij, mikropodjetij in raziskovalnih organov.

- Študija o varnostnem certificiranju in označevanju IKT – Zbrani podatki in ocena učinka (PriceWaterhouseCoopers, 2017; SMART št. 2016/0029).

Ocena učinka

- V poročilu o oceni učinka te pobude so bile opredeljene naslednje glavne težave, ki jih je treba obravnavati:
- razdrobljenost politik in pristopov h kibernetski varnosti v državah članicah,
- razpršenost virov in razdrobljenost pristopov h kibernetski varnosti v institucijah, agencijah in organih EU ter
- nezadostna ozaveščenost in obveščenost državljanov in podjetij, skupaj z vse več različnimi nacionalnimi in sektorskimi certifikacijskimi shemami.

V poročilu so bile glede mandata agencije ENISA ocenjene naslednje možnosti:

- ohranitev sedanjega stanja, kar pomeni podaljšan, a časovno še vedno omejen mandat (osnovna možnost);
- zdajšnji mandat agencije ENISA poteče brez podaljšanja in ukinitev te agencije (brez posredovanja politike);
- „reformirana agencija ENISA“ ter
- Agencija EU za kibernetsko varnost s polnimi operativnimi zmogljivostmi.

V poročilu so bile glede certificiranja kibernetske varnosti ocenjene naslednje možnosti:

- brez posredovanja politike (osnovna možnost),
- nezakonodajni ukrepi (ukrepi „mehkega prava“),
- zakonodajni akt EU za vzpostavitev obveznega sistema za vse države članice na podlagi sistema SOG-IS in
- splošni certifikacijski okvir EU za kibernetsko varnost IKT.

Na podlagi analize je bilo sklenjeno, da je prednostna možnost „reformirana agencija ENISA“ v povezavi s splošnim certifikacijskim okvirom EU za kibernetsko varnost IKT.

Prednostna možnost je bila ocenjena kot najučinkovitejša za doseganje opredeljenih ciljev EU glede večjih zmogljivosti na področju kibernetske varnosti, pripravljenosti, sodelovanja, ozaveščanja, preglednosti in preprečevanja razdrobljenosti trga. Prav tako je bila ocenjena kot najbolj skladna s prednostnimi nalogami politike v zvezi s strategijo EU za kibernetsko varnost in z njo povezanimi politikami (npr. direktivo o varnosti omrežij in informacij) ter strategijo za enotni digitalni trg. Poleg tega se je v postopku posvetovanja izkazalo, da prednostna možnost uživa podporo večine zainteresiranih strani. Nadalje je analiza, izvedena v okviru ocene učinka, pokazala, da bi bili s prednostno možnostjo cilji doseženi z razumno uporabo virov.

Odbor Komisije za regulativni nadzor je najprej 24. julija podal negativno mnenje, nato pa ob ponovni predložitvi 25. avgusta 2017 pozitivno mnenje. V spremenjeno poročilo o oceni učinka so bili vključeni dodatni dokazi, končne ugotovitve ocene agencije ENISA ter dodatne razlage možnosti politike in njihovega učinka. Priloga 1 h končnemu poročilu o oceni učinka povzema, kako so bile v drugem mnenju obravnavane pripombe odbora. Poročilo je bilo zlasti posodobljeno, da bi podrobneje predstavilo okvir EU za kibernetsko varnost, vključno z

ukrepi, ki so vključeni v skupno sporočilo „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“ (Resilience, Deterrence and Defence: Building strong cybersecurity for the EU) (JOIN(2017) 450) in imajo poseben pomen za agencijo ENISA: načrt EU za kibernetsko varnost ter evropski raziskovalni in strokovni center za kibernetsko varnost, s katerim bi Agencija povezala svoja priporočila glede potreb EU po raziskovanju.

V poročilu je pojasnjeno, kako bi reforma Agencije, vključno z novimi nalogami, boljšimi pogoji zaposlovanja in strukturnim sodelovanjem z organi EU na tem področju, izboljšala njeno privlačnost kot delodajalca in pripomogla k reševanju težav, povezanih z zaposlovanjem strokovnjakov. V Prilogi 6 k poročilu je predstavljena tudi revidirana ocena stroškov, povezanih z možnostmi politike za agencijo ENISA. Poročilo je bilo v zvezi z vprašanjem certificiranja revidirano, da bi vsebovalo podrobnejšo razlago prednostne možnosti, vključno z grafično predstavitvijo, ter zajelo ocene stroškov za države članice in Komisijo, povezanih z novim certifikacijskim okvirom. Utemeljitev za izbiro agencije ENISA kot ključnega akterja v okviru je bila dodatno pojasnjena na podlagi njenega strokovnega znanja na področju in dejstva, da je edina agencija na ravni EU za področje kibernetske varnosti. Nazadnje, pregledani so bili razdelki o certificiranju, da se pojasnijo vidiki, povezani z razliko glede na zdajšnji sistem SOG-IS, koristi v zvezi z različnimi možnostmi politike ter dejstvo, da bo vrsta izdelkov in storitev IKT, ki jih zajema evropska certifikacijska shema, opredeljena v sami odobreni shemi.

Ustreznost in poenostavitev ureditve

Ni relevantno.

Vpliv na temeljne pravice

Kibernetska varnost ima ključno vlogo pri varovanju zasebnosti in osebnih podatkov posameznikov v skladu s členoma 7 in 8 Listine EU o temeljnih pravicah. V primeru kibernetskih incidentov sta zasebnost in varstvo osebnih podatkov zelo izpostavljena. Kibernetska varnost je zato nujen pogoj za spoštovanje zasebnosti in zaupnosti naših osebnih podatkov. S tega vidika predlog s prizadevanjem za krepitev kibernetske varnosti v Evropi pomembno dopolnjuje obstoječo zakonodajo, ki varuje temeljno pravico do zasebnosti in osebne podatke. Kibernetska varnost je prav tako bistvena za varstvo zaupnosti naših elektronskih komunikacij ter s tem za uresničevanje svobode izražanja in obveščanja kot tudi drugih povezanih pravic, kot je svoboda misli, vesti in vere.

4. PRORAČUNSKE POSLEDICE

Glej oceno finančnih posledic.

5. DRUGI ELEMENTI

- **Načrti za izvedbo ter ureditev spremljanja, ocenjevanja in poročanja**

Komisija bo spremljala uporabo Uredbe ter Evropskemu parlamentu, Svetu in Evropskemu ekonomsko-socialnemu odboru vsakih pet let predložila poročilo o oceni te uredbe. Ta poročila bodo javna in bodo podrobno pojasnjevala dejansko uporabo in izvrševanje te uredbe.

- **Natančnejša pojasnitev posameznih določb predloga**

Naslov I Uredbe vsebuje splošne določbe: področje urejanja (člen 1), opredelitev pojmov (člen 2), vključno s sklici na zadevne opredelitve iz drugih instrumentov EU, kot so Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (direktiva o varnosti omrežij in informacij), Uredba (ES) št. 765/2008 Evropskega parlamenta in Sveta o določitvi zahtev za akreditacijo in nadzor trga v zvezi s trženjem proizvodov ter razveljavitvi Uredbe (EGS) št. 339/93 in Uredba (EU) št. 1025/2012 Evropskega parlamenta in Sveta o evropski standardizaciji.

Naslov II Uredbe vsebuje ključne določbe v zvezi z Agencijo EU za kibernetsko varnost ENISA.

Poglavje I tega naslova določa mandat (člen 3), cilje (člen 4) in naloge Agencije (členi 5 do 11).

Poglavje II določa organizacijo agencije ENISA in vsebuje ključne določbe o njeni strukturi (člen 12). Obravnava sestavo, pravila glasovanja ter naloge upravnega odbora (oddelek 1, členi 13 do 17), izvršnega odbora (oddelek 2, člen 18) in izvršnega direktorja (oddelek 3, člen 19). Prav tako vključuje določbe o sestavi in vlogi stalne skupine zainteresiranih strani (oddelek 4, člen 20). Nenazadnje, razdelek 5 tega poglavja podrobno navaja operativna pravila za Agencijo, vključno v povezavi z načrtovanjem njenega delovanja, nasprotjem interesov, preglednostjo, zaupnostjo in dostopom do dokumentov (členi 21 do 25).

Poglavje III zadeva določitev in sestavo proračuna Agencije (člena 26 in 27) ter pravila za njegovo izvrševanje (člena 28 in 29). Prav tako vključuje določbe za lažji boj proti goljufijam, korupciji in drugim nezakonitim dejanjem (člen 30).

Poglavje IV obravnava osebje Agencije. Vključuje splošne določbe o kadrovskih predpisih in pogojih za zaposlitev ter pravila glede privilegijev in imunitete (člena 31 in 32). Podrobno določa tudi pravila glede zaposlitve in imenovanja izvršnega direktorja Agencije (člen 33). Nenazadnje vključuje določbe o zaposlitvi napotenih nacionalnih strokovnjakov ali drugega osebja, ki ga ne zaposli Agencija (člen 34).

Poglavje V vključuje splošne določbe v zvezi z Agencijo. Določa pravni status (člen 35) ter vključuje določbe, ki urejajo vprašanja odgovornosti, jezikovno ureditev in varstvo osebnih podatkov (členi 36 do 38), pa tudi varnostne predpise o varstvu tajnih podatkov in občutljivih netajnih podatkov (člen 40). Opisuje pravila glede sodelovanja Agencije s tretjimi državami in mednarodnimi organizacijami (člen 39). Nenazadnje vsebuje tudi določbe o sedežu Agencije in pogojih delovanja ter upravnem nadzoru s strani varuha človekovih pravic (člena 41 in 42).

Naslov III Uredbe določa evropski certifikacijski okvir za kibernetsko varnost (v nadaljnjem besedilu: **okvir**) za izdelke in storitve IKT kot *lex generalis* (člen 1). Opredeljuje splošni namen evropskih certifikacijskih shem za kibernetsko varnost, tj. zagotoviti, da izdelki in storitve IKT izpolnjujejo določene zahteve s področja kibernetske varnosti glede njihove zmožnosti za odpornost, na določeni stopnji zagotovila, na ukrepe, ki ogrožajo razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali z njimi povezanih funkcij ali storitev (člen 43). Poleg tega navaja varnostne cilje, ki jih evropske certifikacijske sheme za kibernetsko varnost želijo doseči (člen 45), med drugim zmožnost varovanja podatkov pred naključnim ali nepooblaščenim dostopom ali razkritjem, uničenjem ali spreminjanjem, in vsebino (tj. elemente) evropskih certifikacijskih shem za kibernetsko varnost, npr. podrobno specifikacijo njihovega področja uporabe, varnostne cilje, merila za ocenjevanje itd. (člen 47).

Naslov III določa tudi glavne pravne učinke evropskih certifikacijskih shem za kibernetsko varnost, in sicer (i) obveznost za izvajanje sheme na nacionalni ravni in prostovoljna narava

certificiranja ter (ii) razveljavitveni učinek evropskih certifikacijskih shem za kibernetsko varnost za nacionalne sheme pri istih izdelkih ali storitvah (člena 48 in 49).

Nadalje naslov III določa postopek za sprejetje evropskih certifikacijskih shem za kibernetsko varnost ter vloge Komisije, agencije ENISA in Evropske certifikacijske skupine za kibernetsko varnost (v nadaljnjem besedilu: skupina) (člen 44). Nenazadnje, naslov III vsebuje določbe, ki urejajo organe za ugotavljanje skladnosti, vključno z njihovimi zahtevami, pooblastili in nalogami, nacionalne organe za nadzor nad certificiranjem ter kazni.

Naslov III skupino ustanavlja kot bistveni organ, ki ga sestavljajo predstavniki nacionalnih organov za nadzor nad certificiranjem, katerih glavna naloga je sodelovati z agencijo ENISA pri pripravi evropskih certifikacijskih shem za kibernetsko varnost in svetovati Komisiji o splošnih ali posebnih vprašanjih, ki zadevajo politiko kibernetske varnosti.

Naslov IV Uredbe vključuje končne določbe, ki opisujejo izvajanje pooblastil, zahteve glede ocenjevanja, razveljavitev in nasledstvo ter začetek veljavnosti.

2017/0225 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti)

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

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

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[28],

ob upoštevanju mnenja Odbora regij[29],

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) Omrežja in informacijski sistemi ter telekomunikacijska omrežja in storitve imajo ključno vlogo v družbi ter so postali temelj gospodarske rasti. Informacijske in komunikacijske tehnologije so osnova za kompleksne sisteme, ki podpirajo družbene dejavnosti, omogočajo, da naša gospodarstva delujejo v ključnih sektorjih, kot so zdravstvo, energetika, finance in promet, ter zlasti podpirajo delovanje notranjega trga.

(2) Med posamezniki, podjetji in vladami po vsej Uniji prevladuje uporaba omrežij in informacijskih sistemov. Digitalizacija in povezljivost postajata poglavitni značilnosti vse večjega števila izdelkov in storitev, s prihodom interneta stvari (IoT) pa naj bi se v naslednjem desetletju po vsej EU začelo uporabljati na milijone, morda celo milijarde povezanih digitalnih naprav. Medtem ko je vse več naprav povezanih z internetom, v njihovo zasnovo nista zadostno vključeni varnost in odpornost, kar vodi v nezadostno kibernetsko varnost. Omejeno certificiranje zato pomeni nezadostne informacije za organizacijske in posamezne uporabnike o lastnostih izdelkov in storitev IKT glede kibernetske varnosti, kar spodkopava zaupanje v digitalne rešitve.

(3) Večja digitalizacija in povezljivost vodita v večja tveganja na področju kibernetske varnosti, zaradi česar je družba na splošno bolj ranljiva za kibernetske grožnje, nevarnosti, s katerimi se srečujejo posamezniki, vključno z ranljivimi osebami, kot so otroci, pa so večje. Da bi ublažili tovrstno tveganje za družbo, je treba sprejeti vse potrebne ukrepe, da bi izboljšali kibernetsko varnost v EU in tako omrežja in informacijske sisteme, telekomunikacijska omrežja ter digitalne izdelke, storitve in

[28] UL C , , str. .
[29] UL C , , str. .

naprave, ki jih uporabljajo posamezniki, vlade in podjetja (od malih in srednjih podjetij do upravljavcev kritičnih infrastruktur), bolje zaščitili pred kibernetskimi grožnjami.

(4) Kibernetski napadi so vse pogostejši ter povezana gospodarstvo in družba, ki sta bolj ranljiva za kibernetske grožnje in napade, potrebujeta boljšo obrambo. Čeprav so kibernetski napadi pogosto čezmejni, so odzivi politike organov za kibernetsko varnost in pristojnosti za kazenski pregon večinoma nacionalni. Veliki kibernetski incidenti lahko povzročijo motnje pri zagotavljanju bistvenih storitev po vsej EU. Zato sta potrebna učinkovit odziv in krizno upravljanje na ravni EU, in sicer na podlagi namenskih politik in širših instrumentov za evropsko solidarnost in medsebojno pomoč. Poleg tega je za oblikovalce politike, podjetja in uporabnike zato pomembno, da se na podlagi zanesljivih podatkov Unije redno ocenjuje stanje kibernetske varnosti in odpornosti v Uniji ter sistematično napovedujejo prihodnji razvoj, izzivi in grožnje, tako na ravni Unije kot na svetovni ravni.

(5) Glede na večje izzive na področju kibernetske varnosti, s katerimi se spopada Unija, je potreben celovit sklop ukrepov, ki bi temeljili na prejšnjih ukrepih Unije in spodbujali cilje, ki se vzajemno krepijo. Ti vključujejo potrebo po nadaljnji krepitvi zmogljivosti in pripravljenosti držav članic in podjetij ter po boljšem sodelovanju in usklajevanju med državami članicami ter institucijami, agencijami in organi EU. Poleg tega je treba glede na to, da kibernetske grožnje ne poznajo meja, povečati zmogljivosti na ravni Unije, ki bi lahko dopolnjevale ukrepe držav članic, zlasti v primeru velikih čezmejnih kibernetskih incidentov in kriz. Potrebna so dodatna prizadevanja za večjo ozaveščenost državljanov in podjetij o vprašanjih kibernetske varnosti. Poleg tega bi bilo treba zaupanje v enotni digitalni trg dodatno okrepiti z zagotavljanjem preglednih informacij o ravni varnosti izdelkov in storitev IKT. To je mogoče lažje doseči s certificiranjem na ravni EU, ki bi zagotavljalo skupne zahteve in merila za ocenjevanje glede kibernetske varnosti za vse nacionalne trge in sektorje.

(6) Leta 2004 sta Evropski parlament in Svet sprejela Uredbo (ES) št. 460/2004[30] o ustanovitvi agencije ENISA, ki naj 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[31], s katero sta mandat Agencije podaljšala do marca 2012. Z Uredbo (ES) št. 580/2011[32] se je mandat Agencije podaljšal do 13. septembra 2013. Leta 2013 sta Evropski parlament in Svet sprejela Uredbo (EU) št. 526/2013[33] o agenciji ENISA in razveljavitvi Uredbe (ES) št. 460/2004, s katero je bil mandat Agencije podaljšan do junija 2020.

---

30 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).

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

32 Uredba (EU) št. 580/2011 Evropskega parlamenta in Sveta z dne 8. junija 2011 o spremembi Uredbe (ES) št. 460/2004 o ustanovitvi Evropske agencije za varnost omrežij in informacij glede njenega trajanja (UL L 165, 24.6.2011, str. 3).

33 Uredba (EU) št. 526/2013 Evropskega parlamenta in Sveta z dne 21. maja 2013 o agenciji Evropske unije za varnost omrežij in informacij (ENISA) in razveljavitvi Uredbe (ES) št. 460/2004 (UL L 165, 18.6.2013, str. 41).

(7) Unija je že sprejela pomembne ukrepe za zagotovitev kibernetske varnosti in okrepitev zaupanja v digitalne tehnologije. Leta 2013 je bila sprejeta strategija Evropske unije za kibernetsko varnost, ki naj bi Uniji zagotavljala smernice pri oblikovanju politike glede odziva na kibernetske grožnje in tveganja. V prizadevanjih za boljšo zaščito evropskih državljanov na spletu je Unija leta 2016 sprejela prvi zakonodajni akt na področju kibernetske varnosti, in sicer Direktivo (EU) 2016/1148 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (v nadaljnjem besedilu: direktiva o varnost omrežij in informacij). Direktiva o varnosti omrežij in informacij določa zahteve glede nacionalnih zmogljivosti na področju kibernetske varnosti, vzpostavlja prve mehanizme za okrepitev strateškega in operativnega sodelovanja med državami članicami ter uvaja obveznosti glede varnostnih ukrepov in priglasitev incidentov v vseh sektorjih, ki so ključni za gospodarstvo in družbo, npr. v energetiki, prometu, vodnem sektorju, bančništvu, infrastrukturah finančnih trgov, zdravstvu, digitalni infrastrukturi, in pri ponudnikih ključnih digitalnih storitev (iskalniki, storitve računalništva v oblaku in spletne tržnice). Pri podpori izvajanju navedene direktive je bila ključna vloga dodeljena agenciji ENISA. Poleg tega je učinkovit boj proti kibernetski kriminaliteti pomembna prednostna naloga v evropski agendi za varnost, saj prispeva k skupnemu cilju doseganja visoke ravni kibernetske varnosti.

(8) Znano je, da se je po sprejetju strategije EU za kibernetsko varnost leta 2013 in po zadnji reviziji mandata Agencije splošni okvir politike znatno spremenil, tudi v zvezi z bolj negotovimi in manj varnimi svetovnimi razmerami. V tem oziru in v okviru nove politike Unije za kibernetsko varnost je treba pregledati mandat agencije ENISA, da bi opredelili njeno vlogo v spremenjenem ekosistemu kibernetske varnosti in zagotovili, da učinkovito prispeva k odzivanju Unije na izzive na področju kibernetske varnosti, ki izhajajo iz teh korenito spremenjenih groženj in za katere, kot je ugotovljeno v oceni Agencije, sedanji mandat ne zadostuje.

(9) Agencija, ustanovljena s to uredbo, bi morala nadomestiti agencijo ENISA, ki je bila ustanovljena z Uredbo (EU) št. 526/2013. Agencija bi morala opravljati naloge, ki so ji podeljene s to uredbo in pravnimi akti Unije na področju kibernetske varnosti, med drugim zagotavljati strokovno znanje in svetovanje ter delovati kot središče informacij in znanja v Uniji. Spodbujati bi morala izmenjavo najboljših praks med državami članicami in zasebnimi zainteresiranimi stranmi, zagotavljati predloge politik Evropski komisiji in državam članicam, delovati kot referenčna točka za sektorske pobude politik Unije v zvezi s kibernetsko varnostjo ter spodbujati operativno sodelovanje med državami članicami ter med državami članicami in institucijami, agencijami in organi EU.

(10) V okviru Sklepa 2004/97/ES, Euratom, ki je bil sprejet na seji Evropskega sveta 13. decembra 2003, so se predstavniki držav članic odločili, da bo sedež agencije ENISA v grškem mestu, ki ga določi grška vlada. Država članica, ki je gostiteljica Agencije, bi morala zagotoviti najboljše možne pogoje za nemoteno in učinkovito delovanje Agencije. Za pravilno in učinkovito izvajanje njenih nalog, zaposlovanje in ohranitev osebja ter večjo učinkovitost dejavnosti mreženja je nujno, da je sedež Agencije na ustrezni lokaciji, kjer so denimo na voljo ustrezne prometne povezave in infrastruktura za zakonce in otroke, ki spremljajo člane osebja Agencije. Potrebne podrobnosti bi morale biti določene v sporazumu med Agencijo in državo članico gostiteljico, sklenjenem po odobritvi upravnega odbora Agencije.

(11) Glede na vse večje izzive na področju kibernetske varnosti, s katerimi se spopada Unija, bi bilo treba finančne in človeške vire, dodeljene Agenciji, povečati, da bi

ustrezali njeni okrepljeni vlogi in nalogam kot tudi kritičnemu položaju v sistemu organizacij, ki varujejo evropski digitalni ekosistem.

(12) Agencija bi morala razviti in ohranjati visoko raven strokovnega znanja ter delovati kot referenčna točka, ki vzbuja zaupanje v enotni trg zaradi svoje neodvisnosti, kakovosti svetovanja, ki ga zagotavlja, in informacij, ki jih razširja, preglednosti svojih postopkov in načina delovanja ter skrbnosti pri izvajanju svojih nalog. Agencija bi morala proaktivno prispevati k prizadevanjem držav članic in Unije ter obenem opravljati svoje naloge ob popolnem sodelovanju z institucijami, organi, uradi in agencijami držav članic. Poleg tega bi moralo delo Agencije temeljiti na prispevkih in sodelovanju zasebnega sektorja ter drugih zadevnih zainteresiranih strani. Sklop nalog bi moral določati, kako naj Agencija doseže svoje cilje, ter hkrati dopuščati prožnost pri njenem delovanju.

(13) Agencija bi morala Komisiji pomagati z nasveti, mnenji in analizami v zvezi z vsemi vprašanji Unije, povezanimi z oblikovanjem, posodabljanjem in pregledovanjem politik in prava na področju kibernetske varnosti, vključno z zaščito kritične infrastrukture in kibernetsko odpornostjo. Agencija bi morala delovati kot referenčna točka za svetovanje in strokovno znanje za sektorsko politiko in zakonodajne pobude Unije pri zadevah v zvezi s kibernetsko varnostjo.

(14) Temeljna naloga Agencije je, da spodbuja dosledno izvajanje zadevnega pravnega okvira, zlasti učinkovito izvajanje direktive o varnosti omrežij in informacij, kar je ključno za povečanje kibernetske odpornosti. Glede na hitro razvijajoče se kibernetske grožnje je jasno, da je treba države članice podpirati s celovitejšim medsektorskim pristopom h krepitvi kibernetske odpornosti.

(15) Agencija bi morala državam članicam ter institucijam, organom, uradom in agencijam Unije pomagati pri njihovih prizadevanjih za vzpostavljanje in krepitev zmogljivosti in pripravljenosti za preprečevanje, odkrivanje in odzivanje na težave in incidente na področju kibernetske varnosti kot tudi pri zadevah v zvezi z varnostjo omrežij in informacijskih sistemov. Agencija bi morala zlasti podpirati razvoj in krepitev nacionalnih skupin CSIRT, da bi te dosegle visoko skupno raven zrelosti v Uniji. Agencija bi morala nuditi pomoč tudi pri oblikovanju in posodabljanju strategij Unije in držav članic za varnost omrežij in informacijskih sistemov, zlasti na področju kibernetske varnosti, ter spodbujati razširjanje teh strategij in spremljati napredek pri njihovem izvajanju. Poleg tega bi morala Agencija javnim organom zagotavljati usposabljanje in gradivo za usposabljanje ter po potrebi „usposabljati izvajalce usposabljanj“, da bi državam članicam pomagala pri razvoju lastnih zmogljivosti za usposabljanje.

(16) Agencija bi morala skupini za sodelovanje, ustanovljeni z direktivo o varnosti omrežij in informacij, pomagati pri izvajanju njenih nalog, predvsem z zagotavljanjem strokovnega znanja in svetovanja ter omogočanjem lažje izmenjave najboljših praks, zlasti glede določitve izvajalcev bistvenih storitev s strani držav članic, tudi glede čezmejnih odvisnosti v zvezi s tveganji in incidenti.

(17) Da bi Agencija spodbujala sodelovanje med javnim in zasebnim sektorjem ter znotraj zasebnega sektorja, zlasti da bi podpirala zaščito kritičnih infrastruktur, bi morala olajševati vzpostavitev sektorskih centrov za izmenjavo in analizo informacij (ISAC) z zagotavljanjem najboljših praks in smernic o razpoložljivih orodjih, postopkov ter smernic o tem, kako obravnavati regulativna vprašanja, povezana z izmenjavo informacij.

(18) Agencija bi morala zbrati in analizirati nacionalna poročila skupin CSIRT in skupine CERT-EU ter določiti skupna pravila, jezik in terminologijo za izmenjavo informacij. Agencija bi morala v okviru direktive o varnosti omrežij in informacij, ki je določila temelje za prostovoljno izmenjavo tehničnih informacij na operativni ravni z ustanovitvijo mreže skupin CSIRT, vključiti tudi zasebni sektor.

(19) Agencija bi morala prispevati k odzivu na ravni EU v primeru velikih čezmejnih kibernetskih incidentov in kriz. Ta naloga bi morala vključevati zbiranje ustreznih informacij ter posredovanje med mrežo skupin CSIRT, tehnično skupnostjo in nosilci odločitev, pristojnimi za krizno upravljanje. Poleg tega bi Agencija lahko nudila podporo pri obravnavi incidentov s tehničnega vidika, tako da bi olajšala ustrezno tehnično izmenjavo rešitev med državami članicami in zagotavljala informacije za komuniciranje z javnostjo. Agencija bi morala ta proces podpirati s preskušanjem načinov takšnega sodelovanja v okviru vsakoletnih vaj na področju kibernetske varnosti.

(20) Agencija bi morala pri izvajanju operativnih nalog uporabljati razpoložljivo strokovno znanje skupine CERT-EU prek strukturiranega sodelovanja v neposredni fizični bližini. Strukturirano sodelovanje bo olajšalo potrebne sinergije in okrepilo strokovno znanje agencije ENISA. Po potrebi bi bilo treba določiti posebno ureditev med tema dvema organizacijama, s katero bi določili praktično izvajanje tega sodelovanja.

(21) Agencija bi morala v skladu s svojimi operativnimi nalogami imeti možnost, da zagotavlja podporo državam članicam, na primer s svetovanjem ali nudenjem tehnične pomoči ali opravljanjem analiz groženj in incidentov. Priporočilo Komisije o usklajenem odzivu na velike kibernetske incidente in krize državam članicam priporoča, naj sodelujejo v dobri veri ter si med seboj in z agencijo ENISA izmenjujejo informacije o velikih kibernetskih incidentih in krizah brez nepotrebnega odlašanja. Take informacije bi morale nadalje pomagati agenciji ENISA pri izvajanju njenih operativnih nalog.

(22) Kot del rednega sodelovanja na tehnični ravni za podporo situacijskemu zavedanju v Uniji bi morala Agencija redno pripravljati tehnično poročilo o stanju na področju kibernetske varnosti v EU glede incidentov in groženj, ki bi temeljilo na javno dostopnih informacijah, lastni analizi ter poročilih, ki ji jih pošljejo skupine CSIRT držav članic (prostovoljno) ali enotne kontaktne točke iz direktive o varnosti omrežij in informacij, Evropski center za boj proti kibernetski kriminaliteti (EC3) pri Europolu, skupina CERT-EU ter po potrebi Obveščevalni in situacijski center Evropske unije (INTCEN) pri Evropski službi za zunanje delovanje (ESZD). Poročilo bi moralo biti na voljo ustreznim telesom Sveta, Komisiji, visokemu predstavniku Unije za zunanje zadeve in varnostno politiko ter mreži skupin CSIRT.

(23) Naknadne tehnične preiskave incidentov z znatnimi posledicami v več kot eni državi članici, ki jih podpira ali opravlja Agencija na zahtevo ali s soglasjem zadevnih držav članic, bi morale biti usmerjene na preprečevanje prihodnjih incidentov in se izvajati brez poseganja v sodne ali upravne postopke za pripisovanje krivde ali odgovornosti.

(24) Zadevne države članice bi morale za namene preiskave ali iz drugih razlogov javne politike zagotoviti potrebne informacije in pomoč Agenciji brez poseganja v člen 346 Pogodbe o delovanju Evropske unije.

(25) Države članice lahko podjetja, ki jih je incident prizadel, povabijo, naj sodelujejo z zagotavljanjem potrebnih informacij in pomoči Agenciji, brez poseganja v njihovo pravico do varovanja poslovno občutljivih informacij.

(26) Agencija mora za boljše razumevanje izzivov na področju kibernetske varnosti in z namenom zagotavljanja dolgoročnega strateškega svetovanja državam članicam in institucijam Unije analizirati sedanja in nastajajoča tveganja. V ta namen bi morala Agencija v sodelovanju z državami članicami ter po potrebi statističnimi uradi in drugimi organi zbirati ustrezne informacije ter opravljati analize nastajajočih tehnologij in tematske ocene o pričakovanih družbenih, pravnih, gospodarskih in regulativnih vplivih tehnoloških inovacij na varnost omrežij in informacij, zlasti na kibernetsko varnost. Agencija bi morala poleg tega države članice ter institucije, agencije in organe Unije podpirati pri prepoznavanju novih trendov in preprečevanju težav v zvezi s kibernetsko varnostjo z opravljanjem analiz groženj in incidentov.

(27) Da bi povečali odpornost Unije, bi morala Agencija razvijati odličnost na področju varnosti internetne infrastrukture in kritičnih infrastruktur z zagotavljanjem svetovanja, smernic in najboljših praks. Agencija bi morala z namenom zagotavljanja lažjega dostopa do bolje strukturiranih informacij o kibernetskih tveganjih in možnih rešitvah razvijati in vzdrževati „informacijsko vozlišče“ Unije – portal „vse na enem mestu“, ki bi javnosti nudil informacije o kibernetski varnosti, ki izhajajo iz institucij, agencij in organov EU in držav članic.

(28) Agencija bi morala prispevati k ozaveščanju javnosti o tveganjih glede kibernetske varnosti in zagotavljati smernice o dobrih praksah za posamezne uporabnike, ki so namenjene državljanom in organizacijam. Agencija bi morala prispevati tudi k spodbujanju najboljših praks in rešitev na ravni posameznikov in organizacij z zbiranjem in analiziranjem javno dostopnih informacij o pomembnih incidentih ter pripravljanjem poročil, da bi zagotovila smernice za podjetja in državljane ter izboljšala splošno raven pripravljenosti in odpornosti. Agencija bi morala poleg tega v sodelovanju z državami članicami ter institucijami, organi, uradi in agencijami Unije organizirati redne kampanje ozaveščanja in redne javne izobraževalne kampanje za končne uporabnike, katerih namen je spodbujati varnejše ravnanje posameznikov na spletu in povečati ozaveščenost o potencialnih grožnjah v kibernetskem prostoru, vključno s kibernetsko kriminaliteto, kot so napadi z zvabljanjem, botneti, finančne in bančne goljufije, pa tudi spodbujati osnovno svetovanje o avtentikaciji in varstvu podatkov. Agencija bi morala imeti osrednjo vlogo pri pospeševanju ozaveščenosti končnih uporabnikov glede varnosti naprav.

(29) Agencija bi morala v podporo podjetjem, ki poslujejo v sektorju kibernetske varnosti, in uporabnikom rešitev kibernetske varnosti vzpostaviti in vzdrževati „tržni observatorij“ z izvajanjem rednih analiz in razširjanjem glavnih trendov na trgu kibernetske varnosti, tako na strani povpraševanja kot na strani ponudbe.

(30) Da bi zagotovili, da lahko Agencija v celoti izpolni svoje cilje, bi morala sodelovati z ustreznimi institucijami, agencijami in organi, vključno s skupino CERT-EU, Evropskim centrom za boj proti kibernetski kriminaliteti (EC3) pri Europolu, Evropsko obrambno agencijo (EDA), Evropsko agencijo za operativno upravljanje obsežnih informacijskih sistemov (eu-LISA), Evropsko agencijo za varnost v letalstvu (EASA) in vsemi drugimi agencijami EU, ki se ukvarjajo s kibernetsko varnostjo. Prav tako bi morala sodelovati z organi, ki se ukvarjajo z varstvom podatkov, da bi izmenjevala tehnično znanje in izkušnje ter najboljše prakse kot tudi nudila svetovanje glede vidikov kibernetske varnosti, ki bi lahko vplivali na njihovo delo. Predstavniki organov odkrivanja in pregona ter organov za varstvo podatkov na ravni držav članic in na ravni Unije bi morali imeti možnost, da so zastopani v stalni skupini zainteresiranih strani Agencije. Agencija bi morala pri sodelovanju z organi odkrivanja

in pregona v zvezi z vidiki varnosti omrežij in informacij, ki bi lahko vplivali na njihovo delo, upoštevati obstoječe informacijske poti in vzpostavljena omrežja.

(31) Agencija bi morala kot članica, ki poleg tega zagotavlja sekretariat za mrežo skupin CSIRT, podpirati skupine CSIRT držav članic in skupino CERT-EU pri operativnem sodelovanju pri vseh zadevnih nalogah mreže skupin CSIRT, kot so opredeljene v direktivi o varnosti omrežij in informacij. Nadalje bi morala Agencija spodbujati in podpirati sodelovanje med ustreznimi skupinami CSIRT v primeru incidentov, napadov ali motenj omrežij ali infrastrukture, ki jo upravljajo ali varujejo skupine CSIRT, in ki vključujejo ali bi lahko vključevali najmanj dve skupini CERT, ob upoštevanju standardnih operativnih postopkov mreže skupin CSIRT.

(32) Da bi Agencija povečala pripravljenost Unije pri odzivanju na kibernetske incidente, bi morala organizirati letne vaje na področju kibernetske varnosti na ravni Unije in, na njihovo zahtevo, podpirati države članice ter institucije, agencije in organe EU pri organiziranju vaj.

(33) Agencija bi morala še naprej razvijati in ohranjati svoje strokovno znanje na področju certificiranja kibernetske varnosti, da bi lahko podpirala politike Unije na tem področju. Agencija bi morala spodbujati uporabo certificiranja kibernetske varnosti v Uniji, vključno s prispevanjem k vzpostavitvi in ohranjanju certifikacijskega okvira za kibernetsko varnost na ravni Unije, da bi tako okrepila preglednost zagotovil izdelkov in storitev IKT glede kibernetske varnosti kot tudi zaupanje na digitalnem notranjem trgu.

(34) Učinkovite politike kibernetske varnosti bi morale v javnem in zasebnem sektorju temeljiti na dobro razvitih metodah za ocenjevanje tveganj. Metode za ocenjevanje tveganj se uporabljajo na različnih ravneh, skupne prakse o tem, kako jih učinkovito izvajati, pa ni. Spodbujanje in razvoj najboljših praks za ocenjevanje tveganj in interoperabilne rešitve za obvladovanje tveganj v javnih in zasebnih organizacijah bosta povečala raven kibernetske varnosti v Uniji. V ta namen bi morala Agencija spodbujati sodelovanje med zainteresiranimi stranmi na ravni Unije ter jih podpirati v prizadevanjih, da vzpostavijo in uvedejo evropske in mednarodne standarde za obvladovanje tveganj in merljivo varnost elektronskih izdelkov, sistemov, omrežij in storitev, ki skupaj s programsko opremo zajemajo omrežja in informacijske sisteme.

(35) Agencija bi morala države članice in ponudnike storitev spodbujati k zvišanju njihovih splošnih varnostnih standardov, da bi vsi uporabniki interneta lahko ustrezno poskrbeli za svojo osebno kibernetsko varnost. Natančneje, ponudniki storitev in proizvajalci izdelkov bi morali umakniti s trga ali reciklirati izdelke in storitve, ki ne izpolnjujejo standardov kibernetske varnosti. Agencija ENISA lahko v sodelovanju s pristojnimi organi razširja informacije o ravni kibernetske varnosti izdelkov in storitev na notranjem trgu ter izdaja opozorila, namenjena ponudnikom storitev in proizvajalcem, s katerimi od njih zahteva, da izboljšajo varnost, tudi kibernetsko, svojih izdelkov in storitev.

(36) Agencija bi morala v celoti upoštevati tekoče dejavnosti na področju raziskav, razvoja in tehnološkega ocenjevanja, zlasti tiste, ki potekajo v okviru raznih raziskovalnih pobud Unije, da bi lahko svetovala institucijam, organom, uradom in agencijam Unije ter, po potrebi in na njihovo zahtevo, državam članicam glede potreb pri raziskavah na področju varnosti omrežij in informacij, zlasti kibernetske varnosti.

(37) Težave, povezane s kibernetsko varnostjo, imajo svetovno razsežnost. Da bi se izboljšali varnostni standardi, je potrebno tesnejše mednarodno sodelovanje, vključno

z opredelitvijo skupnih pravil ravnanja, izmenjavo informacij in spodbujanjem hitrejšega mednarodnega sodelovanja pri odzivanju na zadeve, ki se nanašajo na varnost omrežij in informacij, pa tudi skupnega globalnega pristopa do teh vprašanj. V ta namen bi morala Agencija podpirati nadaljnjo udeležbo in sodelovanje Unije s tretjimi državami in mednarodnimi organizacijami, tako da bi po potrebi ustreznim institucijam, organom, uradom in agencijam Unije zagotavljala potrebno strokovno znanje in analize.

(38) Agencija bi morala imeti možnost, da se odzove na *ad hoc* zahteve po svetovanju in pomoči s strani držav članic ter institucij, agencij in organov EU, ki jih zadevajo cilji Agencije.

(39) Da bi se upoštevala skupna izjava in skupni pristop, o katerih se je julija 2012 dogovorila medinstitucionalna delovna skupina za decentralizirane agencije EU in ki sta namenjena racionalizaciji dejavnosti agencij ter izboljšanju njihovega delovanja, je treba izvajati nekatera načela v zvezi z upravljanjem Agencije. Skupna izjava in skupni pristop bi se morala po potrebi upoštevati tudi pri delovnih programih, ocenah, poročanju in upravnih praksah Agencije.

(40) Upravni odbor, ki ga sestavljajo predstavniki držav članic in Komisije, bi moral določati splošno usmeritev dejavnosti Agencije in zagotavljati, da ta naloge opravlja v skladu s to uredbo. Na upravni odbor bi bilo treba prenesti pooblastila, potrebna za pripravo proračuna, preverjanje njegovega izvrševanja, sprejetje ustreznih finančnih pravil, uvedbo preglednih delovnih postopkov za sprejemanje odločitev Agencije, sprejetje enotnega programskega dokumenta Agencije in lastnega poslovnika, imenovanje izvršnega direktorja ter odločitev o podaljšanju in koncu mandata izvršnega direktorja.

(41) Da bi Agencija pravilno in učinkovito delovala, bi morale Komisija in države članice zagotoviti, da imajo osebe, ki so imenovane v upravni odbor, ustrezno strokovno znanje in izkušnje na funkcijskih področjih. Komisija in države članice bi si morale prizadevati tudi za omejitev menjav svojih predstavnikov v upravnem odboru, da bi zagotovile njegovo neprekinjeno delovanje.

(42) Da bi Agencija delovala nemoteno, je treba njenega izvršnega direktorja imenovati na podlagi zaslug ter dokazanih upravnih in vodstvenih sposobnosti ter ustrezne usposobljenosti in izkušenj s področja kibernetske varnosti, izvršni direktor pa mora svoje naloge opravljati popolnoma neodvisno. V ta namen bi moral izvršni direktor po predhodnem posvetovanju s Komisijo pripraviti predlog delovnega programa Agencije ter sprejeti vse potrebne ukrepe, da bi zagotovil nemoteno izvajanje delovnega programa Agencije. Izvršni direktor bi moral pripraviti letno poročilo, ki se predloži upravnemu odboru, ter osnutek poročila o načrtu prihodkov in odhodkov za Agencijo ter izvrševati proračun. Nadalje bi moral izvršni direktor imeti možnost, da ustanovi *ad hoc* delovne skupine, da preučijo posamezna vprašanja, zlasti znanstvene, tehnološke, pravne ali družbeno-gospodarske narave. Izvršni direktor bi moral zagotoviti, da so člani *ad hoc* delovnih skupin izbrani v skladu z najvišjimi strokovnimi standardi, pri čemer bi moral glede na posamezno vprašanje ustrezno upoštevati ravnovesje med predstavniki javnih uprav držav članic, institucij Unije in zasebnega sektorja, vključno s podjetji, uporabniki in znanstveniki s področja varnosti omrežij in informacij.

(43) Izvršni odbor bi moral prispevati k učinkovitemu delovanju upravnega odbora. V okviru pripravljalnega dela v zvezi z odločitvami upravnega odbora bi bilo treba

podrobno preučiti ustrezne informacije, raziskati razpoložljive možnosti ter ponuditi nasvete in rešitve za pripravo ustreznih odločitev upravnega odbora.

(44) Agencija bi morala imeti stalno skupino zainteresiranih strani, ki bi delovala kot svetovalni organ, da bi zagotovila reden dialog z zasebnim sektorjem, združenji potrošnikov in drugimi ustreznimi zainteresiranimi stranmi. Stalna skupina zainteresiranih strani, ki jo na predlog izvršnega direktorja ustanovi upravni odbor, bi morala obravnavati zadeve, ki so pomembne za zainteresirane strani, in o njih obvestiti Agencijo. Sestava stalne skupine zainteresiranih strani, ki naj bi podala svoj prispevek predvsem glede osnutka delovnega programa, in naloge, dodeljene tej skupini, bi morale zagotoviti zadostno zastopanost zainteresiranih strani pri delu Agencije.

(45) Agencija bi morala sprejeti pravila za preprečevanje in obvladovanje nasprotij interesov. Agencija bi morala poleg tega uporabljati ustrezne predpise Unije o dostopu javnosti do dokumentov iz Uredbe Evropskega parlamenta in Sveta (ES) št. 1049/2001[34]. Agencija bi morala osebne podatke obdelovati v skladu z Uredbo (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[35]. Agencija bi morala spoštovati določbe, ki veljajo za institucije Unije, in nacionalno zakonodajo o ravnanju s podatki, zlasti občutljivimi netajnimi podatki in tajnimi podatki EU.

(46) Da se Agenciji zagotovita popolna samostojnost in neodvisnost ter se ji omogoči, da lahko opravlja dodatne in nove naloge, tudi nepredvidene nujne naloge, bi ji bilo treba dodeliti zadostna lastna proračunska sredstva, ki se večinoma zagotovijo s prispevkom Unije in prispevki tretjih držav, ki sodelujejo pri delu Agencije. Večina osebja Agencije bi morala neposredno sodelovati pri operativnem izvajanju njenega mandata. Državi članici gostiteljici ali vsaki drugi državi članici bi moralo biti dovoljeno, da lahko prostovoljno prispeva k prihodkom Agencije. Za subvencije v breme splošnega proračuna Unije bi se moral še vedno uporabljati postopek za sprejemanje proračuna Unije. Revizijo zaključnih računov Agencije bi moralo opraviti Računsko sodišče, da bi bili zagotovljeni preglednost in odgovornost.

(47) Ugotavljanje skladnosti pomeni proces ugotavljanja, ali so posebne zahteve glede izdelka, postopka, storitve, sistema, osebe ali organa izpolnjene. Za namene te uredbe bi bilo treba certificiranje šteti za vrsto ugotavljanja skladnosti glede lastnosti izdelka, postopka, storitve, sistema ali kombinacije teh elementov (v nadaljnjem besedilu: izdelki in storitve IKT), povezane s kibernetsko varnostjo, ki ga izvede neodvisna tretja stran, ki ni proizvajalec izdelka ali ponudnik storitev. Certificiranje samo po sebi ne more jamčiti, da so certificirani izdelki in storitve IKT kibernetsko varni. Gre bolj za postopek in tehnično metodologijo za potrditev, da so bili izdelki in storitve IKT preskušeni ter da izpolnjujejo nekatere zahteve glede kibernetske varnosti, določene drugje, na primer v tehničnih standardih.

(48) Certificiranje kibernetske varnosti ima pomembno vlogo pri krepitvi zaupanja in varnosti izdelkov in storitev IKT. Enotni digitalni trg, zlasti podatkovno gospodarstvo in internet stvari, lahko uspevajo le, če obstaja splošno zaupanje javnosti, da ti izdelki in storitve nudijo določeno stopnjo zagotovila kibernetske varnosti. Povezani in avtomatizirani avtomobili, elektronski medicinski pripomočki, nadzorni sistemi

---

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

[35] UL L 8, 12.1.2001, str. 1.

industrijske avtomatizacije ter pametna omrežja so le nekateri primeri sektorjev, v katerih je certificiranje že razširjeno ali se bo verjetno uporabljalo v bližnji prihodnosti. Sektorji, ki jih ureja direktiva o varnosti omrežij in informacij, so poleg tega sektorji, v katerih je certificiranje kibernetske varnosti ključnega pomena.

(49) V sporočilu „Krepitev odpornosti evropskega sistema kibernetske varnosti ter spodbujanje konkurenčne in inovativne industrije kibernetske varnosti“ iz leta 2016 je Komisija opredelila potrebo po visokokakovostnih, cenovno dostopnih in interoperabilnih izdelkih in rešitvah na področju kibernetske varnosti. Dobava izdelkov IKT in opravljanje storitev IKT na enotnem trgu sta geografsko še vedno zelo razdrobljena. Razlog za to je, da se je industrija kibernetske varnosti v Evropi razvila predvsem zaradi povpraševanja nacionalnih vlad. Poleg tega so med drugimi vrzelmi, ki vplivajo na enotni trg kibernetske varnosti, pomanjkanje interoperabilnih rešitev (tehničnih standardov), praks in vseevropskih mehanizmov certificiranja. Po eni strani evropska podjetja zato težko konkurirajo na nacionalni, evropski in svetovni ravni. Po drugi strani pa se s tem zmanjšuje izbira učinkovitih in uporabnih tehnologij kibernetske varnosti, do katerih imajo dostop državljani in podjetja. Podobno je Komisija v vmesnem pregledu izvajanja strategije za enotni digitalni trg poudarila potrebo po varnih povezanih izdelkih in sistemih ter navedla, da bi z ustanovitvijo evropskega okvira za varnost IKT s pravili za organizacijo varnostnega certificiranja IKT v Uniji lahko ohranili zaupanje v internet in odpravili sedanjo razdrobljenost trga kibernetske varnosti.

(50) Zdaj se certificiranje izdelkov in storitev IKT glede kibernetske varnosti uporablja le v omejenem obsegu. Če obstaja, večinoma poteka na ravni držav članic ali v okviru shem, ki jih usmerja industrija. Tako certifikat, ki ga izda organ za kibernetsko varnost ene države članice, praviloma ni priznan v drugih državah članicah. Tako je možno, da morajo podjetja svoje izdelke in storitve certificirati v več državah članicah, v katerih poslujejo, da bi na primer lahko sodelovala v nacionalnih postopkih javnega naročanja. Poleg tega se zdi, da ni usklajenega in celovitega pristopa k horizontalnim vidikom kibernetske varnosti (npr. na področju interneta stvari), čeprav se pojavljajo nove sheme. Pri obstoječih shemah se pojavljajo znatne pomanjkljivosti in razlike v smislu pokritosti izdelkov, stopenj zagotovila, vsebinskih meril in dejanske uporabe.

(51) V preteklosti so že potekala prizadevanja za medsebojno priznavanje certifikatov v Evropi. Vendar pa so bila le delno uspešna. Najpomembnejši primer zato je sporazum o vzajemnem priznavanju (MRA) skupine visokih uradnikov za varnost informacijskih sistemov (SOG-IS). Čeprav SOG-IS MRA pomeni najpomembnejši model za sodelovanje in vzajemno priznavanje na področju varnostnega certificiranja, vsebuje nekaj večjih pomanjkljivosti, povezanih z njegovimi visokimi stroški in omejenim področjem uporabe. Do zdaj je bilo razvitih le nekaj profilov zaščite digitalnih izdelkov, kot so digitalni podpis, digitalni tahograf in pametne kartice. Najpomembneje pa je, da SOG-IS zajema le del držav članic Unije. To omejuje učinkovitost SOG-IS MRA z vidika notranjega trga.

(52) Glede na navedeno je treba vzpostaviti evropski certifikacijski okvir za kibernetsko varnost, ki bi določal glavne horizontalne zahteve za evropske certifikacijske sheme za kibernetsko varnost, ki bi jih bilo treba oblikovati, in omogočal, da bi se certifikati za izdelke in storitve IKT priznavali in uporabljali v vseh državah članicah. Evropski okvir bi moral imeti dvojni cilj: po eni strani naj bi pripomogel k povečanju zaupanja v izdelke in storitve IKT, ki so bili certificirani v skladu s takimi shemami; po drugi strani pa naj bi preprečeval kopičenje nasprotujočih si ali prekrivajočih se nacionalnih certifikacijskih shem za kibernetsko varnost in tako zmanjšal stroške za podjetja, ki

poslujejo na enotnem digitalnem trgu. Programi bi morali biti nediskriminatorni in temeljiti na mednarodnih standardih in/ali standardih Unije, razen če so ti standardi neučinkoviti ali neprimerni za dosego legitimnih ciljev EU v tem oziru.

(53) Komisija bi morala biti pooblaščena za sprejemanje evropskih certifikacijskih shem za kibernetsko varnost za določene skupine izdelkov in storitev IKT. Te sheme bi morali izvajati in nadzorovati nacionalni organi za nadzor nad certificiranjem in certifikati, izdani v okviru teh shem, bi morali biti veljavni in priznani po vsej Uniji. Certifikacijske sheme, ki jih izvaja industrija ali druge zasebne organizacije, ne bi smele spadati na področje uporabe te uredbe. Vendar pa lahko organi, ki izvajajo takšne sheme, predlagajo Komisiji, naj preuči možnost, da bi te sheme odobrila kot evropsko shemo.

(54) Določbe te uredbe ne bi smele posegati v zakonodajo Unije, ki vsebuje posebne predpise o certificiranju izdelkov in storitev IKT. Zlasti Splošna uredba o varstvu podatkov vsebuje določbe za uvedbo certifikacijskih mehanizmov ter pečatov in označb za varstvo podatkov, katerih namen je dokazovanje, da so postopki obdelave, ki jih uporabljajo upravljavci in obdelovalci, skladni z navedeno uredbo. Taki certifikacijski mehanizmi ter pečati in označbe za varstvo podatkov bi morali posameznikom, na katere se podatki nanašajo, omogočati, da hitro ocenijo raven varstva podatkov zadevnih izdelkov in storitev. Ta uredba ne posega v certificiranje postopkov obdelave podatkov na podlagi Splošne uredbe o varstvu podatkov, tudi kadar so taki postopki vgrajeni v izdelke in storitve.

(55) Evropske certifikacijske sheme za kibernetsko varnost bi morale zagotoviti, da izdelki in storitve IKT, certificirani v taki shemi, izpolnjujejo navedene zahteve. Takšne zahteve se nanašajo na zmožnost za odpornost, na določeni stopnji zagotovila, na dejanja, katerih namen je ogrožanje razpoložljivosti, avtentičnosti, celovitosti in zaupnosti shranjenih, prenesenih ali obdelanih podatkov ali z njimi povezanih funkcij ali storitev, ki jih ponujajo ali so dostopni prek navedenih izdelkov, postopkov, storitev in sistemov v smislu te uredbe. V tej uredbi ni mogoče podrobno določiti zahtev glede kibernetske varnosti, ki se nanašajo na vse izdelke in storitve IKT. Izdelki in storitve IKT ter s tem povezane potrebe po kibernetski varnosti so tako raznoliki, da je zelo težko oblikovati splošne zahteve glede kibernetske varnosti, ki bi veljale na vseh področjih. Zato je treba sprejeti širok in splošen pojem kibernetske varnosti za namene certificiranja, ki ga dopolnjuje sklop posebnih ciljev za kibernetsko varnost, ki jih je treba upoštevati pri oblikovanju evropskih certifikacijskih shem za kibernetsko varnost. Kako bodo takšni cilji doseženi pri posameznih izdelkih in storitvah IKT, bi bilo treba nadalje podrobno opredeliti na ravni posamezne certifikacijske sheme, ki jo sprejme Komisija, npr. s sklicem na standarde ali tehnične specifikacije.

(56) Komisijo bi morali pooblastiti, da od agencije ENISA zahteva, naj pripravi predloge za sheme za posamezne izdelke ali storitve IKT. Nadalje bi morali Komisijo pooblastiti, da na podlagi predloge za shemo, ki jo predlaga agencija ENISA, sprejme evropsko certifikacijsko shemo za kibernetsko varnost z izvedbenimi akti. Ob upoštevanju splošnega namena in varnostnih ciljev, opredeljenih v tej uredbi, bi moral biti v evropskih certifikacijskih shemah za kibernetsko varnost, ki jih sprejme Komisija, opredeljen minimalni sklop elementov v zvezi z vsebino, področjem uporabe in delovanjem posamezne sheme. Sklop bi moral med drugim vključevati področje uporabe in predmet certificiranja kibernetske varnosti, vključno z zajetimi kategorijami izdelkov in storitev IKT, podrobno specifikacijo zahtev glede kibernetske varnosti, npr. s sklicem na standarde ali tehnične specifikacije, posebnimi merili in

metodami za ocenjevanje ter predvideno stopnjo zagotovila – osnovno, znatno in/ali visoko.

(57) Uporaba evropskega certificiranja kibernetske varnosti bi morala ostati prostovoljna, razen če je v zakonodaji Unije ali nacionalni zakonodaji določeno drugače. Da pa bi dosegli cilje te uredbe in preprečili razdrobljenost notranjega trga, bi nacionalne certifikacijske sheme ali postopki za kibernetsko varnost za izdelke in storitve IKT, ki jih zajema evropska certifikacijska shema za kibernetsko varnost, morali prenehati učinkovati od datuma, ki ga določi Komisija z izvedbenim aktom. Poleg tega države članice ne bi smele uvajati novih nacionalnih certifikacijskih shem, ki bi določale certifikacijske sheme za kibernetsko varnost za izdelke in storitve IKT, ki jih že zajema obstoječa evropska certifikacijska shema za kibernetsko varnost.

(58) Ko bo sprejeta evropska certifikacijska shema za kibernetsko varnost, bi morali proizvajalci izdelkov IKT ali ponudniki storitev IKT imeti možnost, da vložijo vlogo za certificiranje svojih izdelkov ali storitev pri organu za ugotavljanje skladnosti po lastni izbiri. Organe za ugotavljanje skladnosti bi moral akreditirati akreditacijski organ, če izpolnjujejo nekatere posebne zahteve, določene v tej uredbi. Akreditacija bi morala biti izdana za obdobje največ petih let in bi se lahko pod enakimi pogoji podaljšala, če bi organ za ugotavljanje skladnosti izpolnjeval določene zahteve. Akreditacijski organi bi morali preklicati akreditacijo organa za ugotavljanje skladnosti, če pogoji za akreditacijo niso ali niso več izpolnjeni ali če ukrepi, ki jih sprejme organ za ugotavljanje skladnosti, kršijo to uredbo.

(59) Od vseh držav članic je treba zahtevati, naj določijo en organ za nadzor nad certificiranjem kibernetske varnosti, ki bi nadzoroval skladnost organov za ugotavljanje skladnosti in certifikatov, ki jih izdajo organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, z zahtevami iz te uredbe in ustreznih certifikacijskih shem za kibernetsko varnost. Nacionalni organi za nadzor nad certificiranjem bi morali obravnavati pritožbe, ki jih vložijo fizične ali pravne osebe glede certifikatov, ki jih izdajo organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, v ustreznem obsegu preučiti vsebino pritožbe ter pritožnika v razumnem roku obvestiti o napredku in izidih preiskave. Poleg tega bi morali sodelovati z ostalimi nacionalnimi organi za nadzor nad certificiranjem ali drugimi javnimi organi, med drugim tudi z izmenjavo informacij o morebitni neskladnosti izdelkov in storitev IKT z zahtevami iz te uredbe ali posebnih shem za kibernetsko varnost.

(60) Da bi zagotovili dosledno uporabo evropskega certifikacijskega okvira za kibernetsko varnost, bi bilo treba ustanoviti Evropsko certifikacijsko skupino za kibernetsko varnost (v nadaljnjem besedilu: skupina), ki bi jo sestavljali nacionalni organi za nadzor nad certificiranjem. Glavne naloge skupine bi morale biti svetovati in pomagati Komisiji pri njenih prizadevanjih za zagotovitev doslednega izvajanja in uporabe evropskega certifikacijskega okvira za kibernetsko varnost; pomagati in tesno sodelovati z Agencijo pri pripravi predlog za certifikacijske sheme za kibernetsko varnost; predlagati, da Komisija od Agencije zahteva, naj pripravi predlogo za evropsko certifikacijsko shemo za kibernetsko varnost; in sprejeti mnenja, naslovljena na Komisijo, glede ohranjanja in pregledovanja obstoječih evropskih certifikacijskih shem za kibernetsko varnost.

(61) Da bi Evropska komisija okrepila ozaveščenost in olajšala sprejemljivost prihodnjih shem EU za kibernetsko varnost, lahko izda splošne ali sektorske smernice za kibernetsko varnost, npr. o dobrih praksah ali odgovornem ravnanju na področju

kibernetske varnosti, pri čemer poudari pozitivni učinek uporabe certificiranih izdelkov in storitev IKT.

(62) Podpora Agencije certificiranju kibernetske varnosti bi morala vključevati tudi sodelovanje z Varnostnim odborom Sveta in ustreznim nacionalnim organom glede kriptografske odobritve izdelkov, ki se uporabljajo v tajnih omrežjih.

(63) Da bi lahko podrobneje opredelili merila za akreditacijo organov za ugotavljanje skladnosti, bi bilo treba Komisijo pooblastiti za sprejetje aktov v skladu s členom 290 Pogodbe o delovanju Evropske unije. Komisija bi morala med pripravami izvesti ustrezna posvetovanja, vključno s posvetovanji na strokovni ravni. Ta posvetovanja bi morala potekati v skladu z načeli, določenimi v Medinstitucionalnem sporazumu o boljši pripravi zakonodaje z dne 13. aprila 2016. Da bi zagotovila enakopravno sodelovanje pri pripravi delegiranih aktov, bi Evropski parlament in Svet morala prejeti vse dokumente istočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa bi morali imeti možnost, da se sistematično udeležujejo sej strokovnih skupin Komisije, ki se ukvarjajo s pripravo delegiranih aktov.

(64) Da bi zagotovili enotne pogoje izvajanja te uredbe, bi bilo treba na Komisijo prenesti izvedbena pooblastila, kadar je tako določeno v tej uredbi. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011.

(65) Postopek pregleda bi bilo treba uporabiti za sprejetje izvedbenih aktov o evropskih certifikacijskih shemah za kibernetsko varnost za izdelke in storitve IKT, o načinih izvajanja preiskav s strani Agencije ter o okoliščinah, oblikah in postopkih priglasitve akreditiranih organov za ugotavljanje skladnosti Komisiji s strani nacionalnih organov za nadzor nad certificiranjem.

(66) Dejavnosti Agencije bi bilo treba oceniti neodvisno. Pri oceni bi bilo treba upoštevati doseganje ciljev s strani Agencije, njeno delovno prakso in relevantnost njenih nalog. Oceniti pa bi bilo treba tudi učinek, uspešnost in učinkovitost evropskega certifikacijskega okvira za kibernetsko varnost.

(67) Uredbo (EU) št. 526/2013 bi bilo treba razveljaviti.

(68) Ker države članice ciljev te uredbe ne morejo zadovoljivo doseči in ker se ti cilji zato lažje dosežejo na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. Po načelu sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja –

SPREJELA NASLEDNJO UREDBO:

NASLOV I
SPLOŠNE DOLOČBE

Člen 1
Predmet urejanja in področje uporabe

Da bi zagotovili pravilno delovanje notranjega trga in obenem dosegli visoko raven kibernetske varnosti, kibernetske odpornosti in zaupanja v Uniji, ta uredba:

(a) določa cilje, naloge in organizacijske vidike Agencije EU za kibernetsko varnost ENISA (v nadaljnjem besedilu: Agencija) ter

(b) določa okvir za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost za zagotavljanje ustrezne ravni kibernetske varnosti izdelkov in storitev IKT v Uniji. Ta okvir se uporablja brez poseganja v posebne določbe glede prostovoljnega ali obveznega certificiranja v drugih aktih Unije.

Člen 2***Opredelitev pojmov***

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „kibernetska varnost“ zajema vse dejavnosti, ki so potrebne za zaščito omrežij in informacijskih sistemov, njihovih uporabnikov in prizadetih oseb pred kibernetskimi grožnjami;

(2) „omrežje in informacijski sistem“ pomeni sistem, kot je opredeljen v točki (1) člena 4 Direktive (EU) 2016/1148;

(3) „nacionalna strategija za varnost omrežij in informacijskih sistemov“ pomeni okvir, kot je opredeljen v točki (3) člena 4 Direktive (EU) 2016/1148;

(4) „izvajalec bistvenih storitev“ pomeni javni ali zasebni subjekt, kot je opredeljen v točki (4) člena 4 Direktive (EU) 2016/1148;

(5) „ponudnik digitalnih storitev“ pomeni vsako pravno osebo, ki zagotavlja digitalno storitev, kot je opredeljena v točki (6) člena 4 Direktive (EU) 2016/1148;

(6) „incident“ pomeni vsak dogodek, kot je opredeljen v točki (7) člena 4 Direktive (EU) 2016/1148;

(7) „obvladovanje incidentov“ pomeni vsak postopek, kot je opredeljen v točki (8) člena 4 Direktive (EU) 2016/1148;

(8) „kibernetska grožnja“ pomeni vsako potencialno okoliščino ali dogodek, ki bi lahko škodljivo vplival na omrežja in informacijske sisteme, njihove uporabnike in prizadete osebe;

(9) „evropska certifikacijska shema za kibernetsko varnost“ pomeni celovit sklop pravil, tehničnih zahtev, standardov in postopkov, ki so opredeljeni na ravni Unije in se uporabljajo za certificiranje izdelkov in storitev informacijske in komunikacijske tehnologije (IKT), ki spadajo na področje uporabe določene sheme;

(10) „evropski certifikat kibernetske varnosti“ pomeni dokument, ki ga izda organ za ugotavljanje skladnosti in potrjuje, da zadevni izdelek ali storitev IKT izpolnjuje posebne zahteve, določene v evropski certifikacijski shemi za kibernetsko varnost;

(11) „izdelek in storitev IKT“ pomeni vsak element ali skupino elementov omrežij in informacijskih sistemov;

(12) „akreditacija“ pomeni akreditacijo, kot je opredeljena v točki (10) člena 2 Uredbe (ES) št. 765/2008;

(13) „nacionalni akreditacijski organ“ pomeni nacionalni akreditacijski organ, kot je opredeljen v točki (11) člena 2 Uredbe (ES) št. 765/2008;

(14) „ugotavljanje skladnosti“ pomeni ugotavljanje skladnosti, kot je opredeljeno v točki (12) člena 2 Uredbe (ES) št. 765/2008;

(15) „organ za ugotavljanje skladnosti“ pomeni organ za ugotavljanje skladnosti, kot je opredeljen v točki (13) odstavka 2 Uredbe (ES) št. 765/2008;

(16) „standard“ pomeni standard, kot je opredeljen v točki (1) člena 2 Uredbe (EU) št. 1025/2012.

NASLOV II
Agencija EU za kibernetsko varnost ENISA

POGLAVJE I
MANDAT, CILJI IN NALOGE

Člen 3
Mandat

1. Agencija opravlja naloge, ki so ji dodeljene s to uredbo, in tako prispeva k visoki ravni kibernetske varnosti v Uniji.

2. Agencija opravlja naloge, ki so ji dodeljene z akti Unije, ki določajo ukrepe za približevanje zakonov in drugih predpisov držav članic, ki se nanašajo na kibernetsko varnost.

3. Cilji in naloge Agencije ne posegajo v pristojnosti držav članic na področju kibernetske varnosti in nikakor ne v dejavnosti, ki se nanašajo na javno varnost, obrambo in nacionalno varnost, kot tudi ne v dejavnosti države na področju kazenskega prava.

Člen 4
Cilji

1. Agencija je središče strokovnega znanja na področju kibernetske varnosti zaradi svoje neodvisnosti, znanstvene in tehnične kakovosti svetovanja, pomoči in informacij, ki jih zagotavlja, preglednosti svojih postopkov in načina delovanja ter skrbnosti pri izvajanju svojih nalog.

2. Agencija institucijam, agencijam in organom Unije ter državam članicam pomaga pri oblikovanju in izvajanju politik, ki se nanašajo na kibernetsko varnost.

3. Agencija podpira krepitev zmogljivosti in pripravljenost v celotni Uniji tako, da Uniji, državam članicam ter javnim in zasebnim zainteresiranim stranem pomaga krepiti zaščito njihovih omrežij in informacijskih sistemov, razvijati veščine, znanja in spretnosti na področju kibernetske varnosti ter doseči kibernetsko odpornost.

4. Agencija pri zadevah, ki se nanašajo na kibernetsko varnost, spodbuja sodelovanje in usklajevanje na ravni Unije med državami članicami, institucijami, agencijami in organi Unije ter zadevnimi zainteresiranimi stranmi, vključno z zasebnim sektorjem.

5. Agencija krepi zmogljivosti na področju kibernetske varnosti na ravni Unije, da bi dopolnila ukrepe držav članic pri preprečevanju kibernetskih groženj in odzivanju nanje, zlasti v primeru čezmejnih incidentov.

6. Agencija spodbuja uporabo certificiranja, vključno s prispevanjem k vzpostavitvi in ohranjanju certifikacijskega okvira za kibernetsko varnost na ravni Unije v skladu z naslovom III te uredbe, in tako krepi preglednost zagotovil izdelkov in storitev IKT glede kibernetske varnosti kot tudi zaupanje v digitalni notranji trg.

7. Agencija spodbuja visoko raven ozaveščenosti državljanov in podjetij pri vprašanjih v zvezi s kibernetsko varnostjo.

Člen 5

Naloge v zvezi z oblikovanjem in izvajanjem politike in prava Unije

Agencija prispeva k oblikovanju in izvajanju politike in prava Unije s:

1. pomočjo in svetovanjem, zlasti z zagotavljanjem neodvisnega mnenja in pripravljalnega dela za razvoj in pregled politike in prava Unije na področju kibernetske varnosti ter panožne politike in pravnih pobud, kadar gre za zadeve, povezane s kibernetsko varnostjo;
2. pomočjo državam članicam pri doslednem izvajanju politike in prava Unije na področju kibernetske varnosti, zlasti v zvezi z Direktivo (EU) 2016/1148, vključno z mnenji, smernicami, svetovanjem in najboljšimi praksami na področjih, kot so obvladovanje tveganj, poročanje o incidentih in izmenjava informacij, ter lažjo izmenjavo najboljših praks med pristojnimi organi v tem oziru;
3. prispevanjem k delu skupine za sodelovanje v skladu s členom 11 Direktive (EU) 2016/1148, in sicer z zagotavljanjem strokovnega znanja in pomoči;
4. podporo:
    (1) oblikovanju in izvajanju politike Unije na področju elektronske identifikacije in storitev zaupanja, zlasti z zagotavljanjem svetovanja in tehničnih smernic, ter lažji izmenjavi najboljših praks med pristojnimi organi;
    (2) spodbujanju višje ravni varnosti elektronskih komunikacij, med drugim z zagotavljanjem strokovnega znanja in svetovanja, ter lažji izmenjavi najboljših praks med pristojnimi organi;
5. podpiranjem rednega pregleda dejavnosti politike Unije z zagotavljanjem letnega poročila o stanju izvajanja zadevnega pravnega okvira glede:
    (a) priglasitev incidentov s strani držav članic, ki jih skupini za sodelovanje zagotovi enotna kontaktna točka v skladu s členom 10(3) Direktive (EU) 2016/1148;
    (b) uradnih obvestil o kršitvi varnosti in izgubi celovitosti s strani ponudnikov storitev zaupanja, ki jih Agenciji zagotovijo nadzorni organi v skladu s členom 19(3) Uredbe (EU) št. 910/2014;
    (c) uradnih obvestil o kršitvi varnosti, ki jih pošljejo podjetja, ki zagotavljajo javna komunikacijska omrežja ali javno dostopne elektronske komunikacijske storitve, Agenciji pa jih predložijo pristojni organi v skladu s členom 40 [Direktive o Evropskem zakoniku o elektronskih komunikacijah].

Člen 6

Naloge v zvezi s krepitvijo zmogljivosti

1. Agencija pomaga:

(a) državam članicam pri njihovih prizadevanjih za izboljšanje preprečevanja, odkrivanja in analiziranja težav in incidentov na področju kibernetske varnosti ter zmogljivosti odzivanja nanje tako, da jim zagotavlja potrebno strokovno znanje;

(b) institucijam, organom, uradom in agencijam Unije pri njihovih prizadevanjih za izboljšanje preprečevanja, odkrivanja in analiziranja težav in incidentov na področju kibernetske varnosti ter zmogljivosti odzivanja nanje tako, da skupini za odzivanje na računalniške grožnje za evropske institucije, organe in agencije (CERT-EU) zagotavlja ustrezno podporo;

(c) državam članicam, na njihovo zahtevo, pri oblikovanju nacionalnih skupin za odzivanje na incidente na področju računalniške varnosti (CSIRT) v skladu s členom 9(5) Direktive (EU) 2016/1148;

(d) državam članicam, na njihovo zahtevo, pri oblikovanju nacionalnih strategij za varnost omrežij in informacijskih sistemov v skladu s členom 7(2) Direktive (EU) 2016/1148; Agencija prav tako spodbuja razširjanje strategij po vsej Uniji in spremlja napredek pri njihovem izvajanju, da bi spodbujala najboljše prakse;

(e) institucijam Unije pri oblikovanju in pregledovanju strategij Unije na področju kibernetske varnosti s spodbujanjem razširjanja strategij in spremljanjem napredka pri njihovem izvajanju;

(f) skupinam CSIRT na nacionalni ravni in ravni Unije pri povečevanju ravni njihovih zmogljivosti, med drugim s podpiranjem dialoga in izmenjave informacij, z namenom zagotavljanja, da vsaka skupina CSIRT v skladu s tehničnim razvojem izpolnjuje skupni sklop minimalnih zmogljivosti in deluje skladno z najboljšimi praksami;

(g) državam članicam z organiziranjem letnih obsežnih vaj na področju kibernetske varnosti na ravni Unije iz člena 7(6) in z oblikovanjem političnih priporočil, ki temeljijo na postopku ocenjevanja vaj in izkušnjah, pridobljenih z njimi;

(h) ustreznim javnim organom z zagotavljanjem usposabljanja na področju kibernetske varnosti, po potrebi v sodelovanju z zainteresiranimi stranmi;

(i) skupini za sodelovanje z izmenjavo najboljših praks, zlasti glede določitve izvajalcev bistvenih storitev s strani držav članic, tudi glede čezmejnih odvisnosti v zvezi s tveganji in incidenti v skladu s členom 11(3)(l) Direktive (EU) 2016/1148.

2. Agencija olajšuje vzpostavitev sektorskih centrov za izmenjavo in analizo informacij (ISAC) in jih stalno podpira, zlasti v sektorjih, ki so navedeni v Prilogi II k Direktivi (EU) 2016/1148, in sicer z zagotavljanjem najboljših praks in smernic o razpoložljivih orodjih in postopkih ter o tem, kako obravnavati regulativna vprašanja, povezana z izmenjavo informacij.

Člen 7

Naloge v zvezi z operativnim sodelovanjem na ravni Unije

1. Agencija podpira operativno sodelovanje med pristojnimi javnimi organi in med zainteresiranimi stranmi.

2. Agencija na operativni ravni sodeluje in vzpostavi sinergije z institucijami, organi, uradi in agencijami Unije, tudi s skupino CERT-EU, službami, ki se ukvarjajo s kibernetsko kriminaliteto, in nadzornimi organi, ki se ukvarjajo z varstvom zasebnosti in osebnih podatkov, da bi obravnavala zadeve skupnega interesa, med drugim:

   (a) izmenjavo tehničnega znanja in izkušenj ter najboljših praks;

   (b) zagotavljanje svetovanja in smernic o pomembnih vprašanjih glede kibernetske varnosti;

   (c) oblikovanje, po posvetovanju s Komisijo, praktičnih ureditev za izvajanje posebnih nalog.

3. Agencija zagotovi sekretariat mreže skupin CSIRT v skladu s členom 12(2) Direktive (EU) 2016/1148 ter dejavno olajšuje izmenjavo informacij in sodelovanje med njenimi člani.

4. Agencija prispeva k operativnemu sodelovanju v mreži skupin CSIRT in zagotavlja podporo državam članicam s:

   (a) svetovanjem o načinih za izboljšanje njihovih zmogljivosti za preprečevanje in odkrivanje incidentov ter odzivanje nanje;

   (b) zagotavljanjem, na njihovo zahtevo, tehnične pomoči ob incidentih, ki imajo pomembne ali znatne posledice;

   (c) analiziranjem šibkih točk, artefaktov in incidentov.

Agencija in skupina CERT-EU pri opravljanju teh nalog strukturirano sodelujeta, da bi izkoristili sinergije, zlasti glede operativnih vidikov.

5. Agencija na zahtevo dveh ali več zadevnih držav članic in z izključnim namenom zagotavljanja svetovanja za preprečevanje prihodnjih incidentov zagotovi podporo za naknadno tehnično preiskavo ali jo izvede, potem ko prizadeta podjetja priglasijo incidente, ki imajo pomembne ali znatne posledice v skladu z Direktivo (EU) 2016/1148. Agencija takšno preiskavo izvede tudi na ustrezno utemeljeno zahtevo Komisije in v soglasju z zadevnimi državami članicami v primeru incidentov, ki prizadenejo več kot dve državi članici.

   Zadevne države članice in Agencija se dogovorijo o obsegu preiskave in postopku, ki ga je treba upoštevati pri njeni izvedbi, pri čemer ne posegajo v kazensko preiskavo istega incidenta, ki še poteka. Preiskava se zaključi s končnim tehničnim poročilom, ki ga pripravi Agencija zlasti na podlagi informacij in pripomb, ki so jih predložile zadevne države članice in podjetja, ter je dogovorjeno z zadevnimi državami članicami. Povzetek poročila s poudarkom na priporočilih za preprečevanje prihodnjih incidentov se sporoči mreži skupin CSIRT.

6. Agencija organizira letne vaje na področju kibernetske varnosti na ravni Unije ter države članice in institucije, agencije in organe Unije podpira pri organiziranju vaj na podlagi njihovih zahtev. Letne vaje na ravni Unije vključujejo tehnične, operativne in strateške elemente ter pripomorejo k pripravi sodelovalnega odziva na ravni Unije na velike čezmejne kibernetske incidente. Poleg tega Agencija prispeva k sektorskim vajam na področju kibernetske varnosti in jih po potrebi pomaga organizirati skupaj z ustreznimi centri za izmenjavo in analizo informacij (ISAC) ter tem centrom omogoča, da sodelujejo pri vajah na področju kibernetske varnosti tudi na ravni Unije.

7. Agencija pripravi redno tehnično poročilo o incidentih in grožnjah na področju kibernetske varnosti v EU, in sicer na podlagi prosto dostopnih virov, lastne analize in poročil, ki jih predložijo med drugim: skupine CSIRT držav članic (na prostovoljni osnovi) ali enotne kontaktne točke v skladu z direktivo o varnosti omrežij in informacij (členom 14(5) direktive o varnosti omrežij in informacij); Evropski center za boj proti kibernetski kriminaliteti (EC3) pri Europolu, CERT-EU.

8. Agencija prispeva k razvoju sodelovalnega odziva na ravni Unije in ravni držav članic na velike čezmejne incidente ali krize, povezane s kibernetsko varnostjo, in sicer predvsem z:

   (a) združevanjem poročil iz nacionalnih virov, da bi prispevala k skupnemu situacijskemu zavedanju;

   (b) zagotavljanjem učinkovitega pretoka informacij in stopnjevalnih mehanizmov med mrežo skupin CSIRT ter tehničnimi in političnimi nosilci odločanja na ravni Unije;

   (c) podpiranjem tehničnega obravnavanja incidenta ali krize, vključno z olajševanjem izmenjave tehničnih rešitev med državami članicami;

   (d) podpiranjem komuniciranja z javnostjo glede incidenta ali krize;

   (e) preskušanjem načrtov za sodelovanje pri odzivanju na take incidente ali krize.

Člen 8

Naloge v zvezi s trgom, certificiranjem kibernetske varnosti in standardizacijo

Agencija:

(a) podpira in spodbuja oblikovanje in izvajanje politike Unije o certificiranju izdelkov in storitev IKT glede kibernetske varnosti, kot je določeno v naslovu III te uredbe, in sicer s:

   (1) pripravo predlog za evropske certifikacijske sheme za kibernetsko varnost za izdelke in storitve IKT v skladu s členom 44 te uredbe;

   (2) podporo Komisiji pri zagotavljanju sekretariata Evropski certifikacijski skupini za kibernetsko varnost v skladu s členom 53 te uredbe;

   (3) pripravo in objavo smernic ter razvojem dobrih praks glede zahtev na področju kibernetske varnosti za izdelke in storitve IKT v sodelovanju z nacionalnimi organi za nadzor nad certificiranjem in predstavniki industrije;

(b) olajšuje vzpostavitev in uvedbo evropskih in mednarodnih standardov za obvladovanje tveganj in varnost izdelkov in storitev IKT ter v sodelovanju z državami članicami pripravi nasvete in smernice za tehnična področja, povezana z varnostnimi zahtevami za izvajalce bistvenih storitev in ponudnike digitalnih storitev, ter za že obstoječe standarde, vključno z nacionalnimi standardi držav članic, v skladu s členom 19(2) Direktive (EU) 2016/1148;

(c) izvaja in razširja redne analize glavnih trendov na trgu kibernetske varnosti tako na strani povpraševanja kot tudi ponudbe, da bi spodbujala trg kibernetske varnosti v Uniji.

Člen 9

Naloge v zvezi s povečevanjem znanja in informacij ter ozaveščanjem

Agencija:

(a) izvaja analize tehnologij v vzponu in zagotavlja tematske ocene o pričakovanih družbenih, pravnih, ekonomskih in regulativnih učinkih tehnoloških inovacij na kibernetsko varnost;

(b) izvaja dolgoročne strateške analize kibernetskih groženj in incidentov, da bi opredelila nastajajoče trende in pripomogla k preprečevanju težav, povezanih s kibernetsko varnostjo;

(c) v sodelovanju s strokovnjaki iz organov držav članic zagotavlja nasvete, smernice in najboljše prakse za varnost omrežij in informacijskih sistemov, zlasti za varnost internetne infrastrukture in infrastruktur, ki podpirajo sektorje iz Priloge II k Direktivi (EU) 2016/1148;

(d) združuje, organizira in prek namenskega portala da javnosti na voljo informacije o kibernetski varnosti, ki jih predložijo institucije, agencije in organi Unije;

(e) javnost ozavešča o tveganjih glede kibernetske varnosti in zagotavlja smernice o dobrih praksah za posamezne uporabnike, ki so namenjene državljanom in organizacijam;

(f) zbira in analizira javno dostopne informacije o pomembnih incidentih ter pripravlja poročila, da bi zagotovila smernice za podjetja in državljane po vsej Uniji;

(g) v sodelovanju z državami članicami ter institucijami, organi, uradi in agencijami Unije organizira redne kampanje ozaveščanja za izboljšanje kibernetske varnosti in njene prepoznavnosti v Uniji.

Člen 10

Naloge v zvezi z raziskavami in inovacijami

Agencija v zvezi z raziskavami in inovacijami:

(a) svetuje Uniji in državam članicam o potrebah po raziskavah in prednostnih nalogah na področju kibernetske varnosti, da bi omogočila učinkovito odzivanje na aktualna in nastajajoča tveganja in grožnje, vključno z upoštevanjem novih in nastajajočih informacijskih in komunikacijskih tehnologij, ter učinkovito uporabo tehnologij za preprečevanje tveganj;

(b) sodeluje, če jo je Komisija za to pooblastila, v fazi izvajanja programov za financiranje raziskav in inovacij ali kot upravičenec.

Člen 11

Naloge v zvezi z mednarodnim sodelovanjem

Agencija prispeva k prizadevanjem Unije za sodelovanje s tretjimi državami in mednarodnimi organizacijami ter tako spodbuja mednarodno sodelovanje o zadevah, ki se nanašajo na kibernetsko varnost, in sicer s:

(a) sodelovanjem, kadar je to primerno, v vlogi opazovalke pri organizaciji mednarodnih vaj ter analiziranjem in poročanjem o rezultatih teh vaj upravnemu odboru;

(b) olajševanjem, na zahtevo Komisije, izmenjave najboljših praks med ustreznimi mednarodnimi organizacijami;

(c) zagotavljanjem, na zahtevo Komisije, strokovnega znanja.

POGLAVJE II
ORGANIZACIJA AGENCIJE

Člen 12
Sestava

Upravno in vodstveno sestavo Agencije sestavljajo:

(a) upravni odbor, ki izvaja naloge iz člena 14;

(b) izvršni odbor, ki izvaja naloge iz člena 18;

(c) izvršni direktor, ki izvaja dolžnosti iz člena 19, in

(d) stalna skupina zainteresiranih strani, ki izvaja naloge iz člena 20.

ODDELEK 1
UPRAVNI ODBOR

Člen 13
Sestava upravnega odbora

1. Upravni odbor sestavljajo po en predstavnik vsake države članice in dva predstavnika, ki ju imenuje Komisija. Vsi predstavniki imajo glasovalno pravico.

2. Vsak član upravnega odbora ima namestnika, ki ga zastopa med njegovo odsotnostjo.

3. Člani upravnega odbora in njihovi namestniki so imenovani zaradi svojega znanja na področju kibernetske varnosti ob upoštevanju ustreznih vodstvenih, upravnih in proračunskih spretnosti in znanj. Komisija in države članice si prizadevajo za omejitev menjav svojih predstavnikov v upravnem odboru, da bi zagotovile neprekinjeno delovanje tega odbora. Komisija in države članice si prizadevajo za uravnoteženo zastopanost moških in žensk v upravnem odboru.

4. Mandat članov upravnega odbora in njihovih namestnikov traja štiri leta. Ta mandat se lahko podaljša.

Člen 14
Naloge upravnega odbora

1. Upravni odbor:

(a) določi splošno usmeritev delovanja Agencije in zagotavlja, 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 dejavnostmi na ravni Unije;

(b) sprejme osnutek enotnega programskega dokumenta iz člena 21, preden ga predloži Komisiji, ki o njem poda mnenje;

(c) z dvotretjinsko večino glasov članov in v skladu s členom 17 sprejme enotni programski dokument Agencije, pri čemer upošteva mnenje Komisije;

(d) z dvotretjinsko večino glasov članov sprejme letni proračun Agencije in izvaja druge naloge, povezane s proračunom Agencije, v skladu s poglavjem III;

(e) oceni in sprejme konsolidirano letno poročilo o dejavnostih Agencije ter poročilo in njegovo oceno do 1. julija naslednjega leta pošlje Evropskemu parlamentu, Svetu, Komisiji in Računskemu sodišču. Letno poročilo vključuje zaključni račun in opisuje, kako je Agencija izpolnila svoje kazalnike uspešnosti. Letno poročilo se objavi;

(f) sprejme finančna pravila, ki se uporabljajo za Agencijo v skladu s členom 29;

(g) sprejme strategijo za boj proti goljufijam, ki je sorazmerna s tveganji goljufije, in sicer ob upoštevanju analize stroškov in koristi ukrepov, ki jih je treba izvesti;

(h) sprejme pravila za preprečevanje in upravljanje nasprotij interesov med svojimi člani;

(i) zagotovi, da se sprejmejo ustrezni nadaljnji ukrepi v zvezi z ugotovitvami in priporočili na podlagi preiskav Evropskega urada za boj proti goljufijam (OLAF) ter različnih notranjih ali zunanjih revizijskih poročil in ocen;

(j) sprejme svoj poslovnik;

(k) v skladu z odstavkom 2 v zvezi z osebjem Agencije izvaja pooblastila, ki jih Kadrovski predpisi za uradnike Evropske unije podeljujejo organu za imenovanja in ki jih Pogoji za zaposlitev drugih uslužbencev Evropske unije podeljujejo organu, pooblaščenemu za sklenitev pogodbe o zaposlitvi (v nadaljnjem besedilu: pooblastila organa za imenovanja);

(l) sprejme izvedbena pravila za kadrovske predpise in pogoje za zaposlitev drugih uslužbencev v skladu s postopkom iz člena 110 kadrovskih predpisov;

(m) imenuje izvršnega direktorja in po potrebi podaljša njegov mandat ali ga razreši s položaja v skladu s členom 33 te uredbe;

(n) imenuje računovodjo, ki je lahko računovodja Komisije in je pri opravljanju svojih dolžnosti popolnoma neodvisen;

(o) sprejme vse odločitve glede vzpostavitve notranjih struktur Agencije in po potrebi njihovih sprememb, pri čemer upošteva potrebe pri dejavnostih Agencije in dobro proračunsko upravljanje;

(p) odobri sklenitev delovnih dogovorov v skladu s členoma 7 in 39.

2. Upravni odbor v skladu s členom 110 kadrovskih predpisov ter na podlagi člena 2(1) kadrovskih predpisov in člena 6 pogojev za zaposlitev drugih uslužbencev sprejme odločitev o prenosu ustreznih pooblastil organa za imenovanja na izvršnega direktorja in opredelitvi pogojev, v skladu s katerimi se lahko ta prenos pooblastil začasno prekliče. Izvršni direktor je pooblaščen za nadaljnji prenos teh pooblastil.

3. Zaradi izjemnih okoliščin lahko upravni odbor z odločitvijo začasno prekliče prenos pooblastil organa za imenovanja na izvršnega direktorja in njegov nadaljnji prenos pooblastil ter jih izvaja sam ali jih prenese na enega od svojih članov ali uslužbenca, ki ni izvršni direktor.

Člen 15

Predsednik upravnega odbora

Upravni odbor z dvotretjinsko večino glasov članov izmed članov izvoli predsednika in njegovega namestnika za štiri leta z možnostjo enkratnega podaljšanja. Če njuno članstvo v upravnem odboru preneha med njunim mandatom, na isti datum samodejno preneha tudi njun mandat. Namestnik predsednika po uradni dolžnosti nadomešča predsednika, kadar slednji ne more opravljati svojih dolžnosti.

Člen 16

Seje upravnega odbora

1. Seje upravnega odbora sklicuje predsednik.

2. Upravni odbor ima vsaj dve redni seji na leto. Na zahtevo predsednika, Komisije ali najmanj tretjine članov se sestane tudi na izrednih sejah.

3. Izvršni direktor se udeležuje sej upravnega odbora, vendar nima glasovalne pravice.

4. Člani stalne skupine zainteresiranih strani lahko na povabilo predsednika sodelujejo na sejah upravnega odbora, vendar nimajo glasovalne pravice.

5. Članom upravnega odbora in njihovim namestnikom lahko na sejah pomagajo svetovalci ali strokovnjaki, če to omogoča poslovnik.

6. Agencija upravnemu odboru zagotovi sekretariat.

Člen 17

Pravila glasovanja v upravnem odboru

1. Upravni odbor sprejema odločitve z večino članov.

2. Dvotretjinska večina vseh članov upravnega odbora je potrebna za sprejetje enotnega programskega dokumenta in letnega proračuna ter imenovanje, podaljšanje mandata ali odstavitev izvršnega direktorja.

3. Vsak član ima en glas. V odsotnosti člana ima glasovalno pravico njegov namestnik.

4. Predsednik se udeleži glasovanja.

5. Izvršni direktor se glasovanja ne udeleži.

6. V poslovniku upravnega odbora so natančneje določena pravila glasovanja, zlasti pogoji, pod katerimi lahko član deluje v imenu drugega člana.

ODDELEK 2
IZVRŠNI ODBOR

Člen 18
Izvršni odbor

1. Upravnemu odboru pomaga izvršni odbor.

2. Izvršni odbor:

   (a) pripravlja odločitve, ki jih sprejme upravni odbor;

   (b) skupaj z upravnim odborom zagotovi, da se sprejmejo ustrezni nadaljnji ukrepi v zvezi z ugotovitvami in priporočili na podlagi preiskav OLAF ter različnih notranjih ali zunanjih revizijskih poročil in ocen;

   (c) brez poseganja v odgovornosti izvršnega direktorja iz člena 19 pomaga in svetuje izvršnemu direktorju pri izvajanju odločitev upravnega odbora o upravnih in proračunskih zadevah v skladu s členom 19.

3. Izvršni odbor sestavlja pet članov, imenovanih izmed članov upravnega odbora, vključno s predsednikom upravnega odbora, ki lahko predseduje tudi izvršnemu odboru, eden od članov pa je predstavnik Komisije. Izvršni direktor se udeležuje sej izvršnega odbora, vendar nima glasovalne pravice.

4. Mandat članov izvršnega odbora traja štiri leta. Ta mandat se lahko podaljša.

5. Izvršni odbor se sestane vsaj enkrat na tri mesece. Predsednik izvršnega odbora na zahtevo njegovih članov skliče dodatne seje.

6. Upravni odbor določi poslovnik izvršnega odbora.

7. Izvršni odbor lahko po potrebi in zaradi nujnosti sprejme določene začasne odločitve v imenu upravnega odbora, zlasti o zadevah v zvezi z upravnim poslovodenjem, vključno z začasnim preklicem prenosa pooblastil organa za imenovanja in proračunskimi zadevami.

ODDELEK 3
IZVRŠNI DIREKTOR

Člen 19
Odgovornosti izvršnega direktorja

1. Agencijo vodi izvršni direktor, ki svoje dolžnosti opravlja neodvisno. Za svoje ravnanje je odgovoren upravnemu odboru.

2. Izvršni direktor na zahtevo poroča Evropskemu parlamentu o opravljanju svojih dolžnosti. Svet lahko izvršnega direktorja pozove, naj poroča o opravljanju svojih dolžnosti.

3. Izvršni direktor je odgovoren za:

   (a) vsakodnevno upravljanje Agencije;

   (b) izvajanje odločitev, ki jih sprejme upravni odbor;

(c) pripravo osnutka enotnega programskega dokumenta in njegovo predložitev v odobritev upravnemu odboru, preden se predloži Komisiji;

(d) izvajanje enotnega programskega dokumenta in poročanje upravnemu odboru o njem;

(e) pripravo konsolidiranega letnega poročila o dejavnostih Agencije ter njegovo predložitev v oceno in sprejetje upravnemu odboru;

(f) pripravo akcijskega načrta ob upoštevanju zaključkov naknadnih ocen in poročanje Komisiji o napredku vsaki dve leti;

(g) pripravo akcijskega načrta ob upoštevanju zaključkov notranjih ali zunanjih revizijskih poročil in preiskav Evropskega urada za boj proti goljufijam (OLAF) ter poročanje Komisiji o napredku dvakrat letno, upravnemu odboru pa redno;

(h) pripravo osnutka finančnih pravil, ki veljajo za Agencijo;

(i) pripravo osnutka poročila o oceni prihodkov in odhodkov Agencije ter izvrševanje njenega proračuna;

(j) zaščito finančnih interesov Unije z uporabo preventivnih ukrepov proti goljufiji, korupciji in drugim nezakonitim dejavnostim, z učinkovitimi pregledi ter, v primeru ugotovitve nepravilnosti, z izterjavo neupravičeno plačanih zneskov ter po potrebi z učinkovitimi, sorazmernimi in odvračalnimi upravnimi in denarnimi kaznimi;

(k) pripravo strategije Agencije za boj proti goljufijam in njeno predložitev upravnemu odboru v odobritev;

(l) vzpostavljanje in ohranjanje stika s poslovno skupnostjo in potrošniškimi organizacijami, pri čemer zagotavlja reden dialog z ustreznimi zainteresiranimi stranmi;

(m) druge naloge, ki so izvršnemu direktorju dodeljene s to uredbo.

4. Izvršni direktor lahko po potrebi ter v skladu z mandatom, cilji in nalogami Agencije ustanovi ad hoc delovne skupine, ki jih sestavljajo strokovnjaki, tudi iz pristojnih organov držav članic. O tem vnaprej obvesti upravni odbor. Postopki, ki se nanašajo predvsem na sestavo delovnih skupin, imenovanje strokovnjakov delovnih skupin s strani izvršnega direktorja in delovanje delovnih skupin, se določijo v statutu Agencije.

5. Izvršni direktor odloči, ali je treba namestiti člane osebja v eni ali več državah članicah za učinkovito in uspešno opravljanje nalog Agencije. Izvršni direktor pred odločitvijo o ustanovitvi lokalnega urada pridobi predhodno soglasje Komisije, upravnega odbora in zadevnih držav članic. Z navedeno odločitvijo se opredeli obseg dejavnosti, ki naj bi se izvajale v navedenem lokalnem uradu, in sicer tako, da se preprečijo nepotrebni stroški in podvajanje upravnih nalog Agencije. Kadar je to primerno ali potrebno, se doseže sporazum z zadevnimi državami članicami.

ODDELEK 4
STALNA SKUPINA ZAINTERESIRANIH STRANI

Člen 20
Stalna skupina zainteresiranih strani

1. Na predlog izvršnega direktorja upravni odbor ustanovi stalno skupino zainteresiranih strani, ki jo sestavljajo priznani strokovnjaki, ki zastopajo ustrezne zainteresirane strani, kot so podjetja iz sektorja IKT, ponudniki elektronskih komunikacijskih omrežij ali storitev, dostopnih javnosti, skupine potrošnikov, znanstveniki s področja kibernetske varnosti in predstavniki pristojnih organov, ki so uradno obveščeni v skladu z [direktivo o evropskem zakoniku o elektronskih komunikacijah], ter organi pregona in nadzorni organi za varstvo podatkov.
2. Postopki stalne skupine zainteresiranih strani, ki se nanašajo predvsem na število, sestavo, imenovanje članov s strani upravnega odbora, predlog s strani izvršnega direktorja in delovanje skupine, se določijo v statutu Agencije in objavijo.
3. Stalni skupini zainteresiranih strani predseduje izvršni direktor ali katera koli oseba, ki jo izvršni direktor imenuje za vsak primer posebej.
4. Mandat članov stalne skupine zainteresiranih strani traja dve leti in pol. Člani upravnega odbora ne smejo biti člani stalne skupine zainteresiranih strani. Strokovnjaki iz Komisije in držav članic imajo pravico biti prisotni na sejah stalne skupine zainteresiranih strani in sodelovati pri njenem delu. Na seje in k sodelovanju pri delu skupine so lahko povabljeni predstavniki drugih organov, ki niso člani stalne skupine zainteresiranih strani, za katere izvršni direktor meni, da so relevantni.
5. Stalna skupina zainteresiranih strani Agenciji svetuje glede opravljanja dejavnosti. Zlasti svetuje izvršnemu direktorju pri pripravi predloga delovnega programa Agencije in komuniciranju z ustreznimi zainteresiranimi stranmi o zadevah, ki se nanašajo na delovni program.

ODDELEK 5
DELOVANJE

Člen 21
Enotni programski dokument

1. Agencija deluje v skladu z enotnim programskim dokumentom, ki zajema večletni in letni program dejavnosti ter vsebuje vse načrtovane dejavnosti.
2. Izvršni direktor vsako leto pripravi osnutek enotnega programskega dokumenta, ki zajema večletni in letni program dejavnosti ter ustrezno načrtovanje človeških in finančnih virov v skladu s členom 32 Delegirane uredbe Komisije (EU) št. 1271/2013[36], pri čemer upošteva smernice Komisije.

---

[36] Delegirana uredba Komisije (EU) št. 1271/2013 z dne 30. septembra 2013 o okvirni finančni uredbi za organe iz člena 208 Uredbe (EU, Euratom) št. 966/2012 Evropskega parlamenta in Sveta (UL L 328, 7.12.2013, str. 42).

3. Upravni odbor do 30. novembra vsako leto sprejme enotni programski dokument iz odstavka 1 in ga predloži Evropskemu parlamentu, Svetu in Komisiji najpozneje 31. januarja naslednje leto, predloži pa tudi morebitne pozneje posodobljene različice navedenega dokumenta.

4. Enotni programski dokument postane dokončen po dokončnem sprejetju splošnega proračuna Unije in se po potrebi ustrezno prilagodi.

5. Letni delovni program vsebuje podrobne cilje in pričakovane rezultate, vključno s kazalniki uspešnosti. Vsebuje tudi opis ukrepov, ki se bodo financirali, ter navedbo finančnih in človeških virov, dodeljenih vsakemu ukrepu, v skladu z načeli oblikovanja in upravljanja proračuna po dejavnostih. Letni delovni program je skladen z večletnim delovnim programom iz odstavka 7. V njem so jasno navedene naloge, ki so bile v primerjavi s predhodnim proračunskim letom dodane, spremenjene ali črtane.

6. Upravni odbor spremeni sprejeti letni delovni program, kadar se Agenciji dodeli nova naloga. Vsaka bistvena sprememba letnega delovnega programa se sprejme po enakem postopku kot prvotni letni delovni program. Upravni odbor lahko na izvršnega direktorja prenese pooblastilo, da v letni delovni program vnese nebistvene spremembe.

7. Večletni delovni program določa splošno strateško načrtovanje dejavnosti, vključno s cilji, pričakovanimi rezultati in kazalniki uspešnosti. Določa tudi načrtovanje virov, vključno z večletnim proračunom in osebjem.

8. Načrtovanje virov se letno posodablja. Strateško načrtovanje dejavnosti se posodablja po potrebi, zlasti zaradi upoštevanja rezultatov ocene iz člena 56.

Člen 22
Izjava o interesih

1. Člani upravnega odbora, izvršni direktor in iz držav članic začasno napoteni uradniki podajo izjavo o zavezah in izjavo o interesih, v kateri navedejo, ali imajo ali nimajo neposrednih ali posrednih interesov, ki bi lahko ogrozili njihovo neodvisnost. Izjavi sta natančni in izčrpni ter se pisno podata vsako leto, posodobita pa se vsakič, ko je to potrebno.

2. Člani upravnega odbora, izvršni direktor in zunanji strokovnjaki, ki sodelujejo v ad hoc delovnih skupinah, najpozneje na začetku vsake seje podajo natančno in izčrpno izjavo o kakršnih koli interesih, ki bi lahko ogrozili njihovo neodvisnost pri obravnavi točk dnevnega reda, ter se vzdržijo sodelovanja pri razpravah in glasovanja o takih točkah.

3. Agencija v statutu določi praktično ureditev za pravila o izjavah o interesih iz odstavkov 1 in 2.

Člen 23
Preglednost

1. Agencija svoje dejavnosti opravlja z visoko stopnjo preglednosti in v skladu s členom 25.

2. Agencija zagotovi, da javnost in vse zainteresirane strani dobijo ustrezne, objektivne, zanesljive in lahko dostopne informacije, zlasti glede rezultatov njenega dela. Objavi tudi izjave o interesih, ki so bile podane v skladu s členom 22.

3. Upravni odbor lahko na predlog izvršnega direktorja dovoli, da zainteresirane strani pri nekaterih dejavnostih Agencije sodelujejo kot opazovalci.

4. Agencija v statutu določi praktično ureditev za izvajanje pravil o preglednosti iz odstavkov 1 in 2.

Člen 24
Zaupnost

1. Agencija brez poseganja v člen 25 tretjim stranem ne razkrije informacij, ki jih obdeluje ali prejme in v zvezi s katerimi je bilo utemeljeno zahtevano, da se z njimi v celoti ali deloma 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, tudi iz držav članic začasno napoteni uradniki, upoštevajo zahteve glede zaupnosti v skladu s členom 339 Pogodbe o delovanju Evropske unije (PDEU) tudi po prenehanju svojih dolžnosti.

3. Agencija v statutu določi praktično ureditev za izvajanje pravil o zaupnosti iz odstavkov 1 in 2.

4. Upravni odbor Agenciji dovoli, da ravna z zaupnimi informacijami, če je to potrebno za izvajanje nalog Agencije. Pri tem upravni odbor v soglasju s službami Komisije sprejme statut, pri čemer uporabi varnostna načela iz sklepov Komisije (EU, Euratom) 2015/443[37] in 2015/444[38]. Navedena pravila vključujejo določbe o izmenjavi, obdelavi in hrambi tajnih podatkov.

Člen 25
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 PDEU možna pritožba pri varuhu človekovih pravic ali tožba pred Sodiščem Evropske unije v skladu s členom 263 PDEU.

[37] Sklep Komisije (EU, Euratom) 2015/443 z dne 13. marca 2015 o varnosti v Komisiji (UL L 72, 17.3.2015, str. 41).

[38] Sklep Komisije (EU, Euratom) 2015/444 z dne 13. marca 2015 o varnostnih predpisih za varovanje tajnih podatkov EU (UL L 72, 17.3.2015, str. 53).

POGLAVJE III
DOLOČITEV IN SESTAVA PRORAČUNA

Člen 26
Določitev proračuna

1. Izvršni direktor vsako leto pripravi osnutek poročila o oceni prihodkov in odhodkov Agencije za naslednje proračunsko leto in ga skupaj z osnutkom kadrovskega načrta predloži upravnemu odboru. Prihodki in odhodki so uravnoteženi.

2. Upravni odbor na podlagi osnutka poročila o oceni prihodkov in odhodkov iz odstavka 1 vsako leto pripravi poročilo o oceni prihodkov in odhodkov Agencije za naslednje proračunsko leto.

3. Upravni odbor vsako leto do 31. januarja pošlje poročilo o oceni iz odstavka 2, ki je del osnutka enotnega programskega dokumenta, Komisiji in tretjim državam, s katerimi je Unija sklenila sporazume v skladu s členom 39.

4. Komisija na podlagi poročila o oceni v osnutek proračuna Unije, ki ga predloži Evropskemu parlamentu in Svetu v skladu s členoma 313 in 314 PDEU, vnese ocene, ki so po njenem mnenju potrebne v skladu s kadrovskim načrtom, in znesek prispevka v breme splošnega proračuna.

5. Evropski parlament in Svet odobrita proračunska sredstva za prispevek, namenjen Agenciji.

6. Evropski parlament in Svet sprejmeta kadrovski načrt Agencije.

7. Upravni odbor sprejme proračun Agencije skupaj z enotnim programskim dokumentom. Proračun je dokončen, ko je dokončno sprejet splošni proračun Unije. Upravni odbor po potrebi prilagodi proračun in enotni programski dokument Agencije v skladu s splošnim proračunom Unije.

Člen 27
Sestava proračuna

1. Prihodki Agencije brez poseganja v druge vire zajemajo:

   (a) prispevek iz proračuna Unije;

   (b) prihodke, dodeljene za posebne odhodkovne postavke v skladu z njenimi finančnimi pravili iz člena 29;

   (c) sredstva Unije v obliki sporazumov o prenosu pooblastil ali *ad hoc* nepovratnih sredstev v skladu z njenimi finančnimi pravili iz člena 29 in določbami zadevnih instrumentov, ki podpirajo politike Unije;

   (d) prispevke iz tretjih držav, ki sodelujejo pri delu Agencije, kot je določeno v členu 39;

   (e) vse prostovoljne prispevke držav članic v denarju ali v naravi. Države članice, ki zagotovijo prostovoljne prispevke, v zameno za to ne smejo zahtevati nobenih posebnih pravic ali storitev.

2. Odhodke Agencije sestavljajo odhodki za osebje, upravno in tehnično podporo, infrastrukturo, poslovanje ter odhodki, ki izhajajo iz pogodb, sklenjenih s tretjimi stranmi.

Člen 28

Izvrševanje proračuna

1. Za izvrševanje proračuna Agencije je odgovoren izvršni direktor.
2. Notranji revizor Komisije ima za Agencijo enaka pooblastila kot za oddelke Komisije.
3. Računovodja Agencije do 1. marca po vsakem proračunskem letu (1. marca leta N + 1) računovodji Komisije in Računskemu sodišču predloži začasni zaključni račun.
4. Računovodja Agencije po prejemu pripomb Računskega sodišča k začasnemu zaključnemu računu Agencije pripravi končni zaključni račun Agencije na lastno odgovornost.
5. Izvršni direktor predloži končni zaključni račun upravnemu odboru v mnenje.
6. Izvršni direktor do 31. marca leta N + 1 Evropskemu parlamentu, Svetu, Komisiji in Računskemu sodišču pošlje poročilo o upravljanju proračuna in finančnem poslovodenju.
7. Računovodja do 1. julija leta N + 1 Evropskemu parlamentu, Svetu, računovodji Komisiji in Računskemu sodišču pošlje končni zaključni račun skupaj z mnenjem upravnega odbora.
8. Računovodja na isti dan, ko pošlje svoj končni zaključni račun, Računskemu sodišču pošlje tudi pisno razlago končnega zaključnega računa, izvod razlage pa računovodji Komisije.
9. Izvršni direktor objavi končni zaključni račun do 15. novembra naslednjega leta.
10. Izvršni direktor Računskemu sodišču do 30. septembra leta N + 1 pošlje odgovor na njegove pripombe, upravnemu odboru in Komisiji pa pošlje izvod tega odgovora.
11. Izvršni direktor Evropskemu parlamentu na njegovo zahtevo v skladu s členom 165(3) finančne uredbe predloži vse informacije, ki jih ta potrebuje za nemoten potek postopka razrešnice za zadevno proračunsko leto.
12. Evropski parlament izvršnemu direktorju na priporočilo Sveta pred 15. majem leta N + 2 poda razrešnico za izvrševanje proračuna za leto N.

Člen 29

Finančna pravila

Finančna pravila, ki se uporabljajo za Agencijo, sprejme upravni odbor po posvetovanju s Komisijo. Pravila ne odstopajo od Uredbe (EU) št. 1271/2013, razen če je tako odstopanje posebej potrebno za delovanje Agencije in je Komisija dala predhodno soglasje.

Člen 30***Boj proti goljufijam***

1. Za pospešitev boja proti goljufijam, korupciji in drugim nezakonitim dejanjem v skladu z Uredbo (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta[39]

[39] Uredba (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta z dne 11. septembra 2013 o preiskavah, ki jih izvaja Evropski urad za boj proti goljufijam (OLAF), ter razveljavitvi Uredbe (ES)

Agencija v šestih mesecih od začetka svojega delovanja pristopi k Medinstitucionalnemu sporazumu z dne 25. maja 1999 o notranjih preiskavah Evropskega urada za boj proti goljufijam (OLAF) in sprejme ustrezne predpise, ki se uporabljajo za vse zaposlene Agencije, pri čemer uporabi obrazec iz Priloge k navedenemu sporazumu.

2. Računsko sodišče lahko opravi revizije na podlagi dokumentacije in na kraju samem pri vseh upravičencih do nepovratnih sredstev, izvajalcih in podizvajalcih, ki so prejeli sredstva Unije od Agencije.

3. OLAF lahko izvaja preiskave, vključno s pregledi in inšpekcijami na kraju samem, v skladu z določbami in postopki iz Uredbe (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta ter Uredbe Sveta (Euratom, ES) št. 2185/96[40] z dne 11. novembra 1996 o pregledih in inšpekcijah na kraju samem, ki jih opravlja Komisija za zaščito finančnih interesov Evropskih skupnosti pred goljufijami in drugimi nepravilnostmi, da bi ugotovil, ali je prišlo do goljufije, korupcije ali katere koli nezakonite dejavnosti, ki vpliva na finančne interese Unije v povezavi z nepovratnimi sredstvi ali pogodbo, ki jo je financirala Agencija.

4. Brez poseganja v odstavke 1, 2 in 3 sporazumi o sodelovanju s tretjimi državami in mednarodnimi organizacijami, pogodbe, sporazumi o dodelitvi nepovratnih sredstev in sklepi Agencije o dodelitvi nepovratnih sredstev vsebujejo določbe, ki Računsko sodišče in OLAF izrecno pooblaščajo za izvajanje takšnih revizij in preiskav v skladu z njunimi pristojnostmi.

POGLAVJE IV
OSEBJE AGENCIJE

Člen 31
Splošne določbe

Za osebje Agencije veljajo kadrovski predpisi in pogoji za zaposlitev drugih uslužbencev ter pravila za izvajanje teh predpisov, sprejeta z dogovorom med institucijami Unije.

Člen 32
Privilegiji in imunitete

Za Agencijo in njeno osebje se uporablja Protokol št. 7 o privilegijih in imunitetah Evropske unije, ki je priložen Pogodbi o Evropski uniji in Pogodbi o delovanju Evropske unije.

Člen 33
Izvršni direktor

1. Izvršni direktor je zaposlen kot začasni uslužbenec Agencije v skladu s členom 2(a) pogojev za zaposlitev drugih uslužbencev.

št. 1073/1999 Evropskega parlamenta in Sveta in Uredbe Sveta (Euratom) št. 1074/1999 (UL L 248, 18.9.2013, str. 1).

[40] Uredba Sveta (Euratom, ES) št. 2185/96 z dne 11. novembra 1996 o pregledih in inšpekcijah na kraju samem, ki jih opravlja Komisija za zaščito finančnih interesov Evropskih skupnosti pred goljufijami in drugimi nepravilnostmi (UL L 292, 15.11.1996, str. 2).

2. Izvršnega direktorja po odprtem in preglednem izbirnem postopku imenuje upravni odbor s seznama kandidatov, ki ga predlaga Komisija.

3. Agencijo pri sklenitvi pogodbe z izvršnim direktorjem zastopa predsednik upravnega odbora.

4. Kandidat, ki ga izbere upravni odbor, je pred imenovanjem pozvan, da pred zadevnim odborom Evropskega parlamenta poda izjavo in odgovarja na vprašanja članov.

5. Mandat izvršnega direktorja traja pet let. Komisija do konca tega obdobja pripravi oceno, pri kateri upošteva oceno uspešnosti dela izvršnega direktorja ter prihodnjih nalog in izzivov Agencije.

6. Upravni odbor odločitve o imenovanju, podaljšanju mandata ali odstavitvi izvršnega direktorja sprejme na podlagi dvotretjinske večine glasov članov z glasovalno pravico.

7. Upravni odbor lahko na predlog Komisije, ki upošteva oceno iz odstavka 5, enkrat podaljša mandat izvršnega direktorja za največ pet let.

8. Upravni odbor obvesti Evropski parlament, da namerava podaljšati mandat izvršnega direktorja. Izvršni direktor v treh mesecih pred vsakim podaljšanjem mandata na povabilo poda izjavo pred zadevnim odborom Evropskega parlamenta in odgovarja na vprašanja članov.

9. Izvršni direktor, katerega mandat je bil podaljšan, ne sme sodelovati pri drugem izbirnem postopku za isto delovno mesto.

10. Izvršni direktor se lahko odstavi samo z odločitvijo upravnega odbora, sprejeto na predlog Komisije.

Člen 34
Napoteni nacionalni strokovnjaki in drugo osebje

1. Agencija lahko uporabi napotene nacionalne strokovnjake ali drugo osebje, ki ni zaposleno v Agenciji. Za to osebje ne veljajo pogoji za zaposlitev drugih uslužbencev.

2. Upravni odbor sprejme sklep, v katerem določi pravila za napotitev nacionalnih strokovnjakov na Agencijo.

POGLAVJE V
SPLOŠNE DOLOČBE

Člen 35
Pravni status Agencije

1. Agencija je organ Unije in ima pravno osebnost.

2. Agencija ima v vseh državah članicah kar najširšo pravno in poslovno sposobnost, ki jo pravnim osebam priznava nacionalno pravo. Zlasti lahko pridobiva premičnine in nepremičnine ali z njimi razpolaga ter je lahko stranka v sodnem postopku ali oboje.

3. Agencijo zastopa izvršni direktor.

Člen 36

Odgovornost Agencije

1. Pogodbeno odgovornost Agencije ureja pravo, ki se uporablja za zadevno pogodbo.
2. Za odločanje na podlagi katere koli arbitražne klavzule iz pogodb, ki jih sklene Agencija, je pristojno Sodišče Evropske unije.
3. 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.
4. Sodišče Evropske unije je pristojno za odločanje v vseh sporih o odškodninah.
5. Osebno odgovornost uslužbencev do Agencije urejajo ustrezni pogoji, ki veljajo za osebje Agencije.

Člen 37

Jezikovna ureditev

1. Za Agencijo velja Uredba Sveta št. 1[41].Države članice in drugi organi, ki jih te imenujejo, lahko pišejo Agenciji in prejmejo odgovor v uradnem jeziku institucij Unije, ki ga izberejo.
2. Prevajalske storitve, potrebne za delovanje Agencije, zagotavlja Prevajalski center za organe Evropske unije.

Člen 38

Varstvo osebnih podatkov

1. Agencija obdeluje osebne podatke v skladu z Uredbo (ES) št. 45/2001 Evropskega parlamenta in Sveta[42].
2. Upravni odbor sprejme izvedbene ukrepe iz člena 24(8) Uredbe (ES) št. 45/2001. Upravni odbor lahko sprejme dodatne ukrepe, ki so potrebni, da Agencija uporablja Uredbo (ES) št. 45/2001.

Člen 39

Sodelovanje s tretjimi državami in mednarodnimi organizacijami

1. Agencija lahko sodeluje s pristojnimi organi tretjih držav ali mednarodnimi organizacijami ali obojimi, kolikor je to potrebno za dosego ciljev iz te uredbe. V ta namen lahko Agencija na podlagi predhodne odobritve Komisije vzpostavi delovne dogovore z organi tretjih držav in mednarodnimi organizacijami. Ti dogovori ne ustvarjajo novih pravnih obveznosti za Unijo in njene države članice.
2. Agencija je odprta za udeležbo tretjih držav, ki so v ta namen z Unijo sklenile sporazume. Na podlagi ustreznih določb teh sporazumov se dosežejo dogovori, v

---

41 Uredba št. 1 o določitvi jezikov, ki se uporabljajo v Evropski skupnosti za atomsko energijo (UL 17, 6.10.1958, str. 401).

42 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).

katerih so navedeni zlasti značaj, obseg in način udeležbe vsake posamezne države pri delu Agencije, vključno z določbami glede udeležbe pri pobudah Agencije, finančnih prispevkov in osebja. Glede kadrovskih zadev so ti dogovori v vseh pogledih skladni s kadrovskimi predpisi.

3. Upravni odbor sprejme strategijo o odnosih s tretjimi državami ali mednarodnimi organizacijami glede vprašanj, ki so v pristojnosti Agencije. Komisija zagotovi, da Agencija deluje v skladu s svojim mandatom in veljavnim institucionalnim okvirom s sklenitvijo ustreznega delovnega dogovora z izvršnim direktorjem Agencije.

Člen 40

Varnostni predpisi za varovanje tajnih podatkov in občutljivih netajnih podatkov

Agencija ob posvetovanju s Komisijo sprejme varnostne predpise, ki upoštevajo varnostna načela, opredeljena v varnostnih predpisih Komisije za varstvo tajnih podatkov Evropske unije in občutljivih netajnih podatkov iz sklepov Komisije (EU, Euratom) 2015/443 in 2015/444. To med drugim zajema določbe o izmenjavi, obdelavi in hrambi takih podatkov.

Člen 41

Sporazum o sedežu in pogoji delovanja

1. Potrebni dogovori glede namestitve, ki jo je treba Agenciji zagotoviti v državi članici gostiteljici, in infrastrukture, ki ji jo navedena država članica da na voljo, ter posebni predpisi, ki v državi članici gostiteljici veljajo za izvršnega direktorja, člane upravnega odbora, osebje Agencije in njihove družinske člane, so določeni v sporazumu o sedežu, ki ga Agencija in država članica, v kateri se sedež nahaja, skleneta po pridobitvi odobritve upravnega odbora in najpozneje [2 leti po začetku veljavnosti te uredbe].

2. Država članica, ki je gostiteljica Agencije, zagotovi optimalne pogoje za uspešno delovanje Agencije, vključno z dostopnostjo lokacije, ustreznimi šolami za otroke uslužbencev ter ustreznim dostopom do trga dela, socialne varnosti in zdravstvenega varstva za otroke in zakonce.

Člen 42

Upravni nadzor

Delovanje Agencije nadzoruje varuh človekovih pravic v skladu s členom 228 PDEU.

NASLOV III
CERTIFIKACIJSKI OKVIR ZA KIBERNETSKO VARNOST

Člen 43

Evropske certifikacijske sheme za kibernetsko varnost

Evropska certifikacijska shema za kibernetsko varnost dokazuje, da izdelki in storitve IKT, ki so bili certificirani v skladu s tako shemo, izpolnjujejo določene zahteve glede njihove zmožnosti za odpornost, na določeni stopnji zagotovila, na ukrepe, katerih namen je ogrožanje razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti shranjenih, prenesenih ali obdelanih podatkov ali funkcij ali storitev, ki jih ponujajo ali so dostopni prek teh izdelkov, postopkov, storitev in sistemov.

Člen 44

Priprava in sprejetje evropske certifikacijske sheme za kibernetsko varnost

1. Agencija ENISA na zahtevo Komisije pripravi predlogo za evropsko certifikacijsko shemo za kibernetsko varnost, ki izpolnjuje zahteve iz členov 45, 46 in 47 te uredbe. Države članice ali Evropska skupina za kibernetsko varnost (v nadaljnjem besedilu: skupina), ustanovljena v skladu s členom 53, lahko Komisiji predlaga pripravo predloge za evropsko certifikacijsko shemo za kibernetsko varnost.
2. Pri pripravi predlog za sheme iz odstavka 1 tega člena se agencija ENISA posvetuje z vsemi ustreznimi zainteresiranimi stranmi in tesno sodeluje s skupino. Skupina agenciji ENISA zagotavlja pomoč in strokovno svetovanje, ki ju agencija ENISA potrebuje pri pripravi predloge za shemo, vključno s pripravo mnenj, kadar je to potrebno.
3. Agencija ENISA predlogo za evropsko certifikacijsko shemo za kibernetsko varnost, pripravljeno v skladu z odstavkom 2 tega člena, pošlje Komisiji.
4. Komisija lahko na podlagi predloge za shemo, ki jo predlaga agencija ENISA, sprejme izvedbene akte v skladu s členom 55(2), ki določajo evropske certifikacijske sheme za kibernetsko varnost za izdelke in storitve IKT, ki izpolnjujejo zahteve iz členov 45, 46 in 47 te uredbe.
5. Agencija ENISA vzdržuje posebno spletišče, namenjeno obveščanju javnosti o evropskih certifikacijskih shemah za kibernetsko varnost.

Člen 45

Varnostni cilji evropskih certifikacijskih shem za kibernetsko varnost

Evropska certifikacijska shema za kibernetsko varnost je oblikovana tako, da ustrezno upošteva naslednje varnostne cilje:

(a) zaščititi shranjene, prenesene ali kako drugače obdelane podatke pred naključno ali nepooblaščeno hrambo, obdelavo, dostopom ali razkritjem;

(b) zaščititi shranjene, prenesene ali kako drugače obdelane podatke pred naključnim ali nepooblaščenim uničenjem, naključno izgubo ali spremembo;

(c) zagotoviti, da imajo pooblaščene osebe, programi ali stroji dostop izključno do podatkov, storitev ali funkcij, na katere se nanašajo njihove pravice do dostopa;

(d) beležiti, kateri podatki, funkcije ali storitve so bili sporočeni, kdaj in kdo jih je sporočil;

(e) zagotoviti, da je mogoče preveriti, do katerih podatkov, storitev ali funkcij se je dostopalo ali kateri podatki, storitve ali funkcije so se uporabljali ter kdaj in kdo je do njih dostopal oz. jih je uporabljal;

(f) v primeru fizičnega ali tehničnega incidenta pravočasno povrniti razpoložljivost in dostop do podatkov, storitev in funkcij;

(g) zagotoviti, da so izdelki in storitve IKT opremljeni s posodobljeno programsko opremo, ki ne vsebuje znanih šibkih točk, in da so na voljo mehanizmi, ki zagotavljajo varno posodabljanje programske opreme.

Člen 46

Stopnje zagotovila evropskih certifikacijskih shem za kibernetsko varnost

1. Evropska certifikacijska shema za kibernetsko varnost lahko določa eno ali več naslednjih stopenj zagotovila: osnovno, znatno in/ali visoko stopnjo zagotovila za izdelke in storitve IKT v shemi.

2. Osnovna, znatna in visoka stopnja zagotovila izpolnjujejo naslednja merila:

(a) osnovna stopnja zagotovila se nanaša na certifikat, izdan v evropski certifikacijski shemi za kibernetsko varnost, ki zagotavlja omejeno stopnjo zaupanja v navedene ali zagotavljane lastnosti izdelka ali storitve IKT v zvezi s kibernetsko varnostjo, in je opredeljena s sklici na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je zmanjšati tveganje kibernetskih incidentov;

(b) znatna stopnja zagotovila se nanaša na certifikat, izdan v evropski certifikacijski shemi za kibernetsko varnost, ki zagotavlja znatno stopnjo zaupanja v navedene ali zagotavljane lastnosti izdelka ali storitve IKT v zvezi s kibernetsko varnostjo, in je opredeljena s sklici na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je bistveno zmanjšati tveganje kibernetskih incidentov;

(c) visoka stopnja zagotovila se nanaša na certifikat, izdan v evropski certifikacijski shemi za kibernetsko varnost, ki zagotavlja višjo stopnjo zaupanja v navedene ali zagotavljane lastnosti izdelka ali storitve IKT v zvezi s kibernetsko varnostjo, kot jo imajo certifikati z znatno stopnjo zagotovila, in je opredeljena s sklici na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je preprečiti kibernetske incidente.

Člen 47

Elementi evropskih certifikacijskih shem za kibernetsko varnost

1. Evropska certifikacijska shema za kibernetsko varnost vključuje naslednje elemente:

(a) predmet urejanja in področje uporabe certificiranja, vključno z vrsto ali kategorijami zajetih izdelkov in storitev IKT;

(b) podrobno specifikacijo zahtev glede kibernetske varnosti, glede na katere se ocenijo posamezni izdelki in storitve IKT, na primer s sklicem na standarde Unije ali mednarodne standarde ali tehnične specifikacije;

(c) eno ali več stopenj zagotovil, kadar je to ustrezno;

(d) posebna merila in metode za ocenjevanje, vključno z vrstami ocene, ki se uporabljajo za dokazovanje, da so posebni cilji iz člena 45 doseženi;

(e) informacije, ki jih vložnik predloži organom za ugotavljanje skladnosti in so potrebne za certificiranje;

(f) če shema zajema oznake ali znake, pogoje, pod katerimi se te oznake ali znaki lahko uporabijo;

(g) če shema zajema nadzor, pravila za spremljanje skladnosti z zahtevami certifikatov, vključno z mehanizmi za dokazovanje stalnega izpolnjevanja določenih zahtev glede kibernetske varnosti;

(h) pogoje za izdajo, ohranitev, nadaljevanje, razširitev in zmanjšanje področja uporabe certificiranja;

(i) pravila glede posledic neskladnosti certificiranih izdelkov in storitev IKT s certifikacijskimi zahtevami;

(j) pravila glede tega, kako je treba predhodno neodkrite šibke točke izdelkov in storitev IKT na področju kibernetske varnosti prijaviti in obravnavati;

(k) pravila glede hrambe evidenc s strani organov za ugotavljanje skladnosti;

(l) opredelitev nacionalnih certifikacijskih shem za kibernetsko varnost, ki zadeva isto vrsto ali kategorije izdelkov in storitev IKT;

(m) vsebino izdanega certifikata.

2. Navedene zahteve sheme niso v nasprotju z veljavnimi zakonskimi zahtevami, zlasti zahtevami, ki izhajajo iz usklajene zakonodaje Unije.

3. Kadar tako določa posebni akt Unije, se certificiranje na podlagi evropske certifikacijske sheme za kibernetsko varnost lahko uporabi za dokazovanje domneve o skladnosti z zahtevami navedenega akta.

4. Če ni usklajene zakonodaje Unije, lahko pravo držav članic določa tudi, da se evropska certifikacijska shema za kibernetsko varnost lahko uporabi za oblikovanje domneve o skladnosti s pravnimi zahtevami.

Člen 48

Certificiranje kibernetske varnosti

1. Za izdelke in storitve IKT, ki so bili certificirani na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete v skladu s členom 44, se domneva, da so skladni z zahtevami take sheme.

2. Certificiranje je prostovoljno, razen če je v pravu Unije določeno drugače.

3. Evropski certifikat kibernetske varnosti v skladu s tem členom izdajo organi za ugotavljanje skladnosti iz člena 51 na podlagi meril, vključenih v evropsko certifikacijsko shemo za kibernetsko varnost, sprejeto v skladu s členom 44.

4. Z odstopanjem od odstavka 3 in v ustrezno utemeljenih primerih lahko določena evropska shema za kibernetsko varnost določa, da lahko evropski certifikat kibernetske varnosti, ki izhaja iz te sheme, izda le javni organ. Tak javni organ je eden od naslednjih:

   (a) nacionalni organi za nadzor nad certificiranjem iz člena 50(1);

   (b) organ, ki je akreditiran kot organ za ugotavljanje skladnosti v skladu s členom 51(1), ali

   (c) organ, ki je določen v skladu z zakoni, podzakonskimi akti ali drugimi uradnimi upravnimi postopki zadevne države članice in izpolnjuje zahteve za organe, ki potrjujejo izdelke, postopke in storitve na podlagi standarda ISO/IEC 17065:2012.

5. Fizična ali pravna oseba, ki predloži svoje izdelke ali storitve IKT certifikacijskemu mehanizmu, organu za ugotavljanje skladnosti iz člena 51 predloži vse informacije, ki so potrebne za izvedbo certifikacijskega postopka.

6. Certifikat se izda za obdobje največ treh let in se lahko pod enakimi pogoji podaljša, če so zadevne zahteve še vedno izpolnjene.

7. Evropski certifikat kibernetske varnosti, izdan v skladu s tem členom, se prizna v vseh državah članicah.

Člen 49

Nacionalne certifikacijske sheme za kibernetsko varnost in nacionalni certifikati kibernetske varnosti

1. Brez poseganja v odstavek 3 nacionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za izdelke in storitve IKT, ki jih zajema evropska certifikacijska shema za kibernetsko varnost, prenehajo učinkovati z datumom, določenim v izvedbenem aktu, sprejetem v skladu s členom 44(4). Obstoječe nacionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za izdelke in storitve IKT, ki jih evropska certifikacijska shema za kibernetsko varnost ne zajema, še naprej obstajajo.

2. Države članice ne uvedejo novih nacionalnih certifikacijskih shem za kibernetsko varnost za izdelke in storitve IKT, ki jih zajema veljavna evropska certifikacijska shema za kibernetsko varnost.

3. Obstoječi certifikati, izdani na podlagi nacionalnih certifikacijskih shem za kibernetsko varnost, ostanejo veljavni do datuma izteka veljavnosti.

Člen 50

Nacionalni organi za nadzor nad certificiranjem

1. Vsaka država članica imenuje nacionalni organ za nadzor nad certificiranjem.

2. Vsaka država članica obvesti Komisijo o identiteti imenovanega organa.

3. Vsak nacionalni organ za nadzor nad certificiranjem je glede svoje organizacije, odločitev o financiranju, pravne strukture in sprejemanja odločitev neodvisen od subjektov, ki jih nadzoruje.

4. Države članice zagotovijo, da imajo nacionalni organi za nadzor nad certificiranjem ustrezne vire za izvajanje svojih pooblastil ter učinkovito in uspešno opravljanje dodeljenih nalog.

5. Za učinkovito izvajanje te uredbe je primerno, da ti organi sodelujejo v Evropski certifikacijski skupini za kibernetsko varnost, ustanovljeni v skladu s členom 53, na dejaven, učinkovit, uspešen in varen način.

6. Nacionalni organi za nadzor nad certificiranjem:

   (a) spremljajo in izvršujejo uporabo določb iz tega naslova na nacionalni ravni ter nadzorujejo skladnost certifikatov, ki so jih izdali organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, z zahtevami iz tega naslova in ustrezne evropske certifikacijske sheme za kibernetsko varnost;

   (b) spremljajo in nadzorujejo dejavnosti organov za ugotavljanje skladnosti za namene te uredbe, tudi glede priglasitve organov za ugotavljanje skladnosti in s tem povezanih nalog iz člena 52 te uredbe;

   (c) obravnavajo pritožbe, ki jih vložijo fizične ali pravne osebe glede certifikatov, ki jih izdajo organi za ugotavljanje skladnosti s sedežem na njihovem ozemlju, v ustreznem obsegu preučijo vsebino pritožbe ter pritožnika v razumnem roku obvestijo o napredku in izidih preiskave;

   (d) sodelujejo z ostalimi nacionalnimi organi za nadzor nad certificiranjem ali drugimi javnimi organi, med drugim tudi z izmenjavo informacij o morebitni neskladnosti izdelkov in storitev IKT z zahtevami iz te uredbe ali posebnih evropskih certifikacijskih shem za kibernetsko varnost;

   (e) spremljajo razvoj na področju certificiranja kibernetske varnosti.

7. Vsak nacionalni organ za nadzor nad certificiranjem ima vsaj naslednja pooblastila:

   (a) od organov za ugotavljanje skladnosti in imetnikov evropskega certifikata kibernetske varnosti lahko zahteva vse informacije, ki jih potrebuje za opravljanje svojih nalog;

   (b) v obliki revizij izvaja preiskave organov za ugotavljanje skladnosti in imetnikov evropskega certifikata kibernetske varnosti, da preveri skladnost z določbami iz naslova III;

   (c) v skladu z nacionalnim pravom sprejme ustrezne ukrepe, da zagotovi, da organi za ugotavljanje skladnosti ali imetniki certifikata izpolnjujejo zahteve te uredbe ali evropske certifikacijske sheme za kibernetsko varnost;

   (d) pridobi dostop do vseh prostorov organov za ugotavljanje skladnosti in imetnikov evropskega certifikata kibernetske varnosti, da izvede preiskave v skladu s postopkovnim pravom Unije ali države članice;

   (e) v skladu z nacionalnim pravom odvzame certifikate, ki niso skladni s to uredbo ali evropsko certifikacijsko shemo za kibernetsko varnost;

   (f) v skladu z nacionalnim pravom naloži kazni, kot je določeno v členu 54, in zahteva takojšnje prenehanje kršitev obveznosti iz te uredbe.

8. Nacionalni organi za nadzor nad certificiranjem sodelujejo med seboj in s Komisijo ter si zlasti izmenjujejo informacije, izkušnje in dobre prakse glede certificiranja kibernetske varnosti in tehničnih vprašanj, ki zadevajo kibernetsko varnost izdelkov in storitev IKT.

Člen 51

Organi za ugotavljanje skladnosti

1. Organe za ugotavljanje skladnosti akreditira nacionalni akreditacijski organ, imenovan v skladu z Uredbo (ES) št. 765/2008, le, če izpolnjujejo zahteve, določene v Prilogi k tej uredbi.

2. Akreditacija se izda za obdobje največ petih let in se lahko pod enakimi pogoji podaljša, če organ za ugotavljanje skladnosti izpolnjuje zahteve, določene v tem členu. Akreditacijski organi prekličejo akreditacijo organa za ugotavljanje skladnosti v skladu z odstavkom 1 tega člena, če pogoji za akreditacijo niso ali niso več izpolnjeni ali če ukrepi, ki jih sprejme organ za ugotavljanje skladnosti, kršijo to uredbo.

Člen 52

Priglasitev

1. Nacionalni organi za nadzor nad certificiranjem za vsako evropsko certifikacijsko shemo za kibernetsko varnost, sprejeto v skladu s členom 44, Komisiji priglasijo organe za ugotavljanje skladnosti, akreditirane za izdajo certifikatov na določenih stopnjah zagotovil iz člena 46, in nemudoma sporočijo kakršne koli naknadne spremembe glede njih.

2. Komisija eno leto po začetku veljavnosti evropske certifikacijske sheme za kibernetsko varnost seznam priglašenih organov za ugotavljanje skladnosti objavi v *Uradnem listu Evropske unije*.

3. Če Komisija prejme priglasitev po izteku obdobja iz odstavka 2, v *Uradnem listu Evropske unije* objavi spremembe seznama iz odstavka 2 v dveh mesecih po datumu prejema priglasitve.

4. Nacionalni organ za nadzor nad certificiranjem lahko Komisiji predloži zahtevek za črtanje organa za ugotavljanje skladnosti, ki ga je priglasil zadevni nacionalni organ za nadzor nad certificiranjem, s seznama iz odstavka 2 tega člena. Komisija v *Uradnem listu Evropske unije* objavi ustrezne spremembe seznama v enem mesecu po datumu prejema zahtevka nacionalnega organa za nadzor nad certificiranjem.

5. Komisija lahko z izvedbenimi akti opredeli okoliščine, obrazce in postopke priglasitve iz odstavka 1 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 55(2).

Člen 53

Evropska certifikacijska skupina za kibernetsko varnost

1. Ustanovi se Evropska certifikacijska skupina za kibernetsko varnost (v nadaljnjem besedilu: skupina).

2. Skupino sestavljajo nacionalni organi za nadzor nad certificiranjem. Organe zastopajo vodje ali drugi visoki predstavniki nacionalnih organov za nadzor nad certificiranjem.

3. Skupina opravlja naslednje naloge:

(a) svetuje in pomaga Komisiji pri njenem delu, da zagotovi dosledno izvajanje in uporabo tega naslova, zlasti glede vprašanj politike certificiranja kibernetske varnosti, usklajevanja pristopov politike in priprave evropskih certifikacijskih shem za kibernetsko varnost;

(b) podpira, svetuje in sodeluje z agencijo ENISA pri pripravi predloge za shemo v skladu s členom 44 te uredbe;

(c) Komisiji predlaga, da od Agencije zahteva, naj pripravi predlogo za evropsko certifikacijsko shemo za kibernetsko varnost v skladu s členom 44 te uredbe;

(d) sprejme mnenja, naslovljena na Komisijo, glede ohranjanja in pregledovanja obstoječih evropskih certifikacijskih shem za kibernetsko varnost;

(e) prouči zadevni razvoj na področju certificiranja kibernetske varnosti in izmenjuje primere dobrih praks na področju certifikacijskih shem za kibernetsko varnost;

(f) olajšuje sodelovanje med nacionalnimi organi za nadzor nad certificiranjem na podlagi tega naslova prek izmenjave informacij, zlasti z določitvijo metod za učinkovito izmenjavo informacij o vseh vprašanjih v zvezi s certificiranjem kibernetske varnosti.

4. Komisija predseduje skupini in ji zagotovi sekretariat, pri čemer ji v skladu s členom 8(a) pomaga agencija ENISA.

Člen 54
Kazni

Države članice določijo pravila o kaznih, ki se uporabljajo v primeru kršitev določb tega naslova in zahtev evropskih certifikacijskih shem za kibernetsko varnost, ter sprejmejo vse potrebne ukrepe za zagotovitev, da se te kazni izvajajo. Te kazni so učinkovite, sorazmerne in odvračilne. Države članice Komisijo [do …/nemudoma] obvestijo o navedenih pravilih in ukrepih ter o morebitnih poznejših spremembah, ki vplivajo nanje.

NASLOV IV
KONČNE DOLOČBE

Člen 55
Postopek v odboru

1. Komisiji pomaga odbor. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.
2. Pri sklicih na ta odstavek se uporablja člen 5 Uredbe (EU) št. 182/2011.

Člen 56
Ocena in pregled

1. Komisija najpozneje pet let po datumu iz člena 58, nato pa vsakih pet let oceni učinek, uspešnost in učinkovitost Agencije in njenih delovnih praks ter morebitno potrebo po spremembi mandata Agencije kot tudi finančne posledice take spremembe. Pri oceni se upoštevajo vse povratne informacije, ki jih Agencija prejme kot odziv na svoje dejavnosti. Če Komisija meni, da nadaljnji obstoj Agencije glede na zastavljene cilje, mandat in naloge ni več upravičen, lahko predlaga spremembo določb te uredbe, ki se nanašajo na Agencijo.
2. Oceni se tudi vpliv, učinkovitost in uspešnost določb naslova III glede ciljev zagotavljanja ustrezne ravni kibernetske varnosti izdelkov in storitev IKT v Uniji ter izboljšanja delovanja notranjega trga.
3. Komisija poročilo o oceni skupaj s svojimi zaključki predloži Evropskemu parlamentu, Svetu in upravnemu odboru. Ugotovitve iz poročila o oceni se objavijo.

Člen 57
Razveljavitev in nasledstvo

1. Uredba (ES) št. 526/2013 se razveljavi z [….].
2. Sklici na Uredbo (ES) št. 526/2013 oziroma agencijo ENISA se štejejo kot sklici na to uredbo oziroma Agencijo.
3. Agencija je pravna naslednica agencije, ustanovljene z Uredbo (ES) št. 526/2013, kar zadeva lastništvo, dogovore, pravne obveznosti, pogodbe o zaposlitvi, finančne obveznosti in odgovornosti. Vse obstoječe odločitve upravnega in izvršnega odbora ostajajo veljavne, če niso v nasprotju z določbami te uredbe.
4. Agencija se ustanovi za nedoločeno obdobje, ki se začne […].
5. Izvršni direktor, imenovan v skladu s členom 24(4) Uredbe (ES) št. 526/2013, je izvršni direktor Agencije preostanek svojega mandata.
6. Člani in namestniki članov upravnega odbora, imenovani v skladu s členom 6 Uredbe (ES) št. 526/2013, so člani in namestniki članov upravnega odbora Agencije preostali del mandata.

Člen 58

Začetek veljavnosti

1. Ta uredba začne veljati dvajseti dan po objavi v *Uradnem listu Evropske unije*.

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

V Bruslju,

Za Evropski parlament	*Za Svet*
Predsednik	*Predsednik*

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

Predlog uredbe Evropskega parlamenta in Sveta o Agenciji EU za kibernetsko varnost ENISA in razveljavitvi Uredbe (EU) št. 526/2013 ter certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti (uredba o kibernetski varnosti)

1.2. Zadevna področja

Področje: 09 Komunikacijska omrežja, vsebine in tehnologija

Dejavnost: 09 02 Enotni digitalni trg

1.3. Vrsta predloga/pobude

☒ Predlog/pobuda se nanaša na **nov ukrep (naslov III – Certificiranje)**.

☐ Predlog/pobuda se nanaša na **nov ukrep na podlagi pilotnega projekta / pripravljalnega ukrepa**[43].

☒ Predlog/pobuda se nanaša na **podaljšanje obstoječega ukrepa** (**naslov II – Mandat agencije ENISA)**.

☐ Predlog/pobuda se nanaša na **obstoječ ukrep, preusmerjen v nov ukrep**.

1.4. Cilji

1.4.1. Večletni strateški cilji Komisije, ki naj bi bili doseženi s predlogom/pobudo

1. Povečanje odpornosti držav članic, podjetij in EU kot celote

2. Zagotavljanje pravilnega delovanja notranjega trga EU za izdelke in storitve IKT

3. Povečanje globalne konkurenčnosti podjetij EU, ki delujejo na področju IKT

4. Približevanje zakonov in drugih predpisov držav članic, ki določajo kibernetsko varnost

1.4.2. Specifični cilji

Ob upoštevanju splošnih ciljev in širšega konteksta revidirane strategije za kibernetsko varnost naj bi z instrumentom, ki natančno določa obseg in mandat agencije ENISA ter vzpostavlja evropski certifikacijski okvir za izdelke in storitve IKT, dosegli naslednje specifične cilje:

1. povečanje **zmogljivosti in pripravljenosti** držav članic in podjetij;
2. boljše **sodelovanje in usklajevanje** med državami članicami ter institucijami, agencijami in organi EU;
3. povečanje **zmogljivosti na ravni EU, da se dopolni ukrepanje držav članic**, zlasti v primeru čezmejnih kibernetskih kriz;
4. povečanje **ozaveščenosti** državljanov in podjetij o vprašanjih kibernetske varnosti;
5. krepitev zaupanja v enotni digitalni trg in digitalne inovacije s povečanjem splošne **preglednosti zagotovil**[44] izdelkov in storitev IKT glede kibernetske varnosti.

[43] Po členu 54(2)(a) oz. (b) finančne uredbe.

Agencija ENISA bo prispevala k doseganju navedenih ciljev z:

okrepljeno podporo oblikovanju politik – zagotavljala bo smernice in svetovanje Komisiji in državam članicam pri posodobitvi in oblikovanju celovitega normativnega okvira na področju kibernetske varnosti kot tudi sektorskih politik in zakonodajnih pobud, ki zadevajo kibernetsko varnost; prispevala bo k delu skupine za sodelovanje (člen 11 Direktive (EU) 2016/1148) z zagotavljanjem strokovnega znanja in pomoči; podpirala bo oblikovanje in izvajanje politike na področju elektronske identifikacije in storitev zaupanja; spodbujala bo izmenjavo najboljših praks med pristojnimi organi;

okrepljeno podporo krepitvi zmogljivosti – zagotavljala bo podporo državam članicam ter institucijam, organom, uradom in agencijam Unije, da bi lahko razvili in izboljšali preprečevanje, odkrivanje in analiziranje težav in incidentov na področju kibernetske varnosti ter zmogljivosti odzivanja nanje; državam članicam bo na njihovo zahtevo pomagala pri oblikovanju nacionalnih skupin CSIRT in nacionalnih strategij za kibernetsko varnost; institucijam Unije bo pomagala pri oblikovanju in reviziji strategij Unije za kibernetsko varnost; zagotavljala bo usposabljanja o kibernetski varnosti; državam članicam bo prek skupine za sodelovanje pomagala pri izmenjavi najboljših praks; omogočala bo lažje ustanavljanje sektorskih centrov za izmenjavo in analizo informacij (ISAC);

podporo operativnemu sodelovanju in kriznemu upravljanju – podpirala bo sodelovanje med pristojnimi javnimi organi ter med zainteresiranimi stranmi z vzpostavitvijo sistematičnega sodelovanja z institucijami, organi, uradi in agencijami Unije, ki delujejo na področju kibernetske varnosti, kibernetske kriminalitete ter varstva zasebnosti in osebnih podatkov; zagotavljala bo sekretariat za mrežo skupin CSIRT (člen 12(2) Direktive (EU) 2016/1148) in prispevala k operativnemu sodelovanju v okviru mreže z zagotavljanjem, v sodelovanju s skupino CERT-EU, podpore državam članicam na njihovo zahtevo; organizirala bo redne vaje na področju kibernetske varnosti; prispevala bo k razvoju sodelovalnega odziva na velike čezmejne kibernetske incidente in krize; v sodelovanju z mrežo skupin CSIRT bo izvajala naknadne tehnične preiskave večjih incidentov in izdajala priporočila za nadaljnje ukrepanje;

s trgom povezanimi nalogami (standardizacija, certificiranje) – opravljala bo številne funkcije, ki predvsem podpirajo delovanje notranjega trga, Agencija bo v vlogi kibernetskega „tržnega observatorija“ analizirala zadevne trende na trgu kibernetske varnosti, da bi lahko bolje uskladila ponudbo in povpraševanje; podpirala in spodbujala bo oblikovanje in izvajanje politike Unije o certificiranju izdelkov in storitev IKT glede kibernetske varnosti s pripravo predlog za evropske certifikacijske sheme za kibernetsko varnost za izdelke in storitve IKT, zagotavljanjem sekretariata za Evropsko certifikacijsko skupino za kibernetsko varnost kot tudi pripravo smernic in dobrih praks glede varnostnih zahtev za izdelke in storitve IKT v sodelovanju z nacionalnimi organi za nadzor nad certificiranjem in industrijo; **okrepljeno podporo znanju, obveščanju in ozaveščanju** – zagotavljala bo pomoč in svetovanje Komisiji in državam članicam, da bi bila po vsej Uniji dosežena visoka raven znanja o vprašanjih, povezanih z direktivo o varnosti omrežij in informacij, in njeni uporabi pri zainteresiranih straneh v industriji; to vključuje tudi zbiranje in urejanje informacij o varnosti omrežij in informacijskih sistemov [ali kibernetski varnosti] ter dajanje teh informacij na voljo javnosti prek namenskega portala; drug pomemben element so dejavnosti in kampanje za ozaveščanje splošne javnosti o tveganjih na področju kibernetske varnosti;

[44] Preglednost zagotovil kibernetske varnosti pomeni, da se uporabnikom zagotovi dovolj informacij o lastnostih kibernetske varnosti, ki jim omogočajo, da objektivno določijo raven varnosti zadevnega izdelka, storitve ali procesa IKT.

okrepljeno podporo raziskavam in inovacijam – zagotavljala bo svetovanje glede potreb po raziskavah in prednostnih nalog na področju kibernetske varnosti;

podporo mednarodnemu sodelovanju – podpirala bo prizadevanja Unije za sodelovanje s tretjimi državami in mednarodnimi organizacijami ter tako spodbujala mednarodno sodelovanje na področju kibernetske varnosti.

CERTIFICIRANJE

Certifikacijski okvir bo prispeval k doseganju ciljev s povečanjem splošne preglednosti zagotovil[45] izdelkov in storitev IKT glede kibernetske varnosti ter posledično krepitvijo zaupanja v enotni digitalni trg in digitalne inovacije. To bo tudi pripomoglo k preprečevanju razdrobljenosti certifikacijskih shem v EU ter povezanih varnostnih zahtev in meril za ocenjevanje v različnih državah članicah in sektorjih.

1.4.3. Pričakovani rezultati in posledice

Navedite, kakšne posledice naj bi imel(-a) predlog/pobuda za upravičence/ciljne skupine.

Okrepljena agencija ENISA (ki bo podpirala zmogljivosti, preprečevanje, sodelovanje in ozaveščanje na ravni EU in bo tako zasnovana za povečanje splošne kibernetske odpornosti EU) ter podpora certifikacijskemu okviru EU za izdelke in storitve IKT naj bi prinesli naslednje učinke (neizčrpen seznam):

Skupni učinek:

– Skupni pozitivni učinek na notranji trg zaradi manjše razdrobljenosti trga in krepitve zaupanja v digitalne tehnologije z boljšim sodelovanjem, bolj harmoniziranimi pristopi k politikam EU o kibernetski varnosti in večjimi zmogljivostmi na ravni EU. To naj bi imelo pozitiven gospodarski učinek, saj bi pripomoglo k znižanju stroškov kibernetske varnosti / incidentov v zvezi s kibernetsko kriminaliteto, katerih gospodarski učinek v Uniji je ocenjen na 0,41 % BDP Evropske unije (tj. približno 55 milijard EUR).

Posebni rezultati:

Boljše zmogljivosti in boljša pripravljenost držav članic in podjetij na področju kibernetske varnosti

– Boljše zmogljivosti in boljša pripravljenost držav članic na področju kibernetske varnosti (zaradi dolgoročne strateške analize kibernetskih groženj in incidentov, smernic in poročil, posredovanja strokovnega znanja in dobrih praks, razpoložljivosti usposabljanja in gradiva za usposabljanje ter okrepljenih vaj Cyber Europe)

– Boljše zmogljivosti zasebnih akterjev zaradi podpore za vzpostavitev centrov za izmenjavo in analizo informacij (ISAC) v različnih sektorjih

– Boljša pripravljenost EU in držav članic na področju kibernetske varnosti zaradi razpoložljivosti dobro utečenih in dogovorjenih načrtov za primer velikega čezmejnega kibernetskega incidenta, preskušenih v vajah Cyber Europe

Boljše sodelovanje in usklajevanje med državami članicami ter institucijami, agencijami in organi EU

[45] Preglednost zagotovil kibernetske varnosti pomeni, da se uporabnikom zagotovi dovolj informacij o lastnostih kibernetske varnosti, ki jim omogočajo, da objektivno določijo raven varnosti zadevnega izdelka, storitve ali procesa IKT.

– Boljše sodelovanje znotraj javnega in zasebnega sektorja in med njima

– Bolj dosleden pristop do izvajanja direktive o varnosti omrežij in informacij v različnih državah članicah in sektorjih

– Boljše sodelovanje na področju certificiranja zaradi institucionalnega okvira, ki omogoča razvoj evropskih certifikacijskih shem za kibernetsko varnost kot tudi oblikovanje skupne politike na tem področju

Večje zmogljivosti na ravni EU, ki dopolnjujejo ukrepe držav članic

– Boljše „operativne zmogljivosti EU“, ki dopolnjujejo ukrepe držav članic in jih podpirajo na njihovo zahtevo ter v zvezi z omejenimi in vnaprej opredeljenimi storitvami; to naj bi pozitivno vplivalo na uspešnost preprečevanja in odkrivanja incidentov ter odzivanja nanje na ravni držav članic in ravni Unije

Večja ozaveščenost državljanov in podjetij o vprašanjih kibernetske varnosti

– Boljša splošna ozaveščenost državljanov in podjetij o vprašanjih kibernetske varnosti

– Boljša zmožnost sprejemati premišljene odločitve v zvezi z nakupom izdelkov in storitev IKT zaradi certificiranja kibernetske varnosti

Okrepljeno zaupanje v enotni digitalni trg in digitalne inovacije zaradi večje preglednosti zagotovil izdelkov in storitev IKT glede kibernetske varnosti

– Večja preglednost zagotovil[46] izdelkov in storitev IKT glede kibernetske varnosti zaradi poenostavitve postopkov za varnostno certificiranje na podlagi vseevropskega okvira

– Boljša stopnja zagotovil varnostnih lastnosti izdelkov in storitev IKT

– Večja uporaba varnostnega certificiranja, ki jo spodbujajo poenostavljeni postopki, nižji stroški in obeti poslovnih priložnosti v vsej EU, ki jih ne ovira razdrobljenost trga

– Boljša konkurenčnost na trgu kibernetske varnosti v EU zaradi nižjih stroškov in manjšega upravnega bremena za mala in srednja podjetja ter odprave morebitnih ovir za vstop na trg, ki jih povzročajo številni nacionalni sistemi certificiranja

Drugo

– Za nobenega od ciljev ni pričakovan znaten okoljski vpliv.

– Glede proračuna EU se lahko pričakujejo koristi zaradi večje učinkovitosti, ki jih bosta prinesla večje sodelovanje in usklajevanje dejavnosti med institucijami, agencijami in organi EU.

1.4.4. Kazalniki rezultatov in posledic

Navedite, s katerimi kazalniki se bo spremljalo izvajanje predloga/pobude.

(a)

Cilj: povečanje zmogljivosti in pripravljenosti držav članic in podjetij:

- Število usposabljanj, ki jih organizira agencija ENISA

[46] Preglednost zagotovil kibernetske varnosti pomeni, da se uporabnikom zagotovi dovolj informacij o lastnostih kibernetske varnosti, ki jim omogočajo, da objektivno določijo raven varnosti zadevnega izdelka, storitve ali procesa IKT.

- Geografska pokritost (število držav in območij), kjer agencija ENISA zagotavlja neposredno pomoč
- Raven pripravljenosti, ki jo dosežejo države članice glede zrelosti skupine CSIRT in nadzora nad regulativnimi ukrepi, povezanimi s kibernetsko varnostjo
- Število dobrih praks za kritične infrastrukture, ki se izvajajo po EU in ki jih predloži agencija ENISA
- Število dobrih praks za mala in srednja podjetja, ki se izvajajo po EU in ki jih predloži agencija ENISA
- Objava letne strateške analize kibernetskih groženj in incidentov, v kateri agencija ENISA opredeli nove trende
- Redni prispevek agencije ENISA k delu delovnih skupin za kibernetsko varnost evropskih organizacij za standardizacijo (ESO)

Cilj: boljše sodelovanje in usklajevanje med državami članicami ter institucijami, agencijami in organi EU

- Število držav članic, ki so priporočila in mnenja agencije ENISA uporabile pri oblikovanju svojih politik
- Število institucij, agencij in organov EU, ki so priporočila in mnenja agencije ENISA uporabili pri oblikovanju svojih politik
- Redno izvajanje delovnega programa mreže skupin CSIRT ter dobro delujoča informacijska infrastruktura in komunikacijski kanali mreže skupin CSIRT
- Število tehničnih poročil, ki se dajo na voljo skupini za sodelovanje in ki jih skupina uporabi
- Dosleden pristop k izvajanju direktive o varnosti omrežij in informacij v različnih državah članicah in sektorjih
- Število ocen regulativne skladnosti, ki jih opravi agencija ENISA
- Število centrov ISAC, ustanovljenih v različnih sektorjih, zlasti za kritične infrastrukture
- Vzpostavitev in redno vzdrževanje informacijske platforme za razširjanje informacij glede kibernetske varnosti, ki izhajajo iz institucij, agencij in organov EU
- Redni prispevek k pripravi delovnih programov EU za raziskave in inovacije
- Dosežen sporazum o sodelovanju med agencijo ENISA, EC3 in skupino CERT-EU
- Število certifikacijskih shem, ki so bile vključene in oblikovane na podlagi okvira

Cilj: povečanje zmogljivosti na ravni EU, ki dopolnjujejo ukrepe držav članic, zlasti v primeru čezmejnih kibernetskih kriz:

- Objava letne strateške analize kibernetskih groženj in incidentov, v kateri agencija ENISA opredeli nove trende
- Objava zbirnih podatkov o incidentu, sporočenem na podlagi direktive o varnosti omrežij in informacij, s strani agencije ENISA
- Število vseevropskih vaj, ki jih usklajuje Agencija, ter število sodelujočih

držav članic in organizacij

- Število prošenj držav članic agenciji ENISA za podporo pri odzivanju v izrednih razmerah in število ugodenih prošenj
- Število analiz šibkih točk, artefaktov in incidentov, ki jih opravi agencija ENISA v sodelovanju s skupino CERT-EU
- Razpoložljivost vseevropskih poročil o stanju na podlagi informacij, ki jih države članice in drugi subjekti dajo na voljo agenciji ENISA v primeru velikega čezmejnega kibernetskega incidenta

Cilj: povečanje ozaveščenosti državljanov in podjetij o vprašanjih kibernetske varnosti:

- Redno izvajanje vseevropskih in nacionalnih kampanj za ozaveščanje in redno posodabljanje tem glede na nove potrebe po učenju
- Povečanje ozaveščenosti državljanov EU o kibernetski varnosti
- Redno izvajanje vprašalnika o ozaveščenosti o kibernetski varnosti in sčasoma povečanje odstotka pravilnih odgovorov
- Redno objavljanje dobrih praks glede kibernetske varnosti in kibernetske higiene za zaposlene in organizacije

Cilj: krepitev zaupanja v enotni digitalni trg in digitalne inovacije s povečanjem splošne preglednosti zagotovil[47] izdelkov in storitev IKT glede kibernetske varnosti:

- Število shem, ki upoštevajo okvir EU
- Nižji stroški za pridobitev varnostnega certifikata za IKT
- Število organov za ugotavljanje skladnosti v državah članicah, ki so specializirani za certificiranje IKT
- Vzpostavitev Evropske certifikacijske skupine za kibernetsko varnost in redno organiziranje sej
- Smernice za certificiranje v skladu z vzpostavljenim okvirom EU
- Redno objavljanje analiz glavnih trendov na trgu kibernetske varnosti v EU
- Število certificiranih izdelkov in storitev IKT v skladu s pravili evropskega okvira za varnostno certificiranje IKT
- Večje število končnih uporabnikov, ki poznajo varnostne lastnosti izdelkov in storitev IKT

(b)

1.4.5. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno

Glede na regulativne zahteve in hiter razvoj kibernetskih groženj je treba revidirati mandat agencije ENISA ter določiti prenovljen sklop nalog in funkcij, da bi Agencija lahko uspešno in učinkovito podpirala prizadevanja držav članic, institucij EU in drugih zainteresiranih strani za zagotovitev varnega kibernetskega prostora v Evropski uniji. Predlagani obseg mandata je natančno določen, pri čemer so okrepljena področja, na katerih se je pokazalo, da ima Agencija jasno dodano vrednost, in dodana so nova

[47] Preglednost zagotovil kibernetske varnosti pomeni, da se uporabnikom zagotovi dovolj informacij o lastnostih kibernetske varnosti, ki jim omogočajo, da objektivno določijo raven varnosti zadevnega izdelka, storitve ali procesa IKT.

področja, na katerih je potrebna podpora glede na nove prednostne naloge politik in instrumente, zlasti direktivo o varnosti omrežij in informacij, revizijo strategije EU za kibernetsko varnost, načrt EU za kibernetsko varnost na področju sodelovanja ob kibernetskih krizah in varnostno certificiranje IKT. Z novim predlaganim mandatom naj bi Agencija dobila močnejšo in osrednejšo vlogo, zlasti tako, da države članice tudi dejavneje podpira pri preprečevanju posameznih groženj (operativna zmogljivost), ter tako, da postane strokovno središče, ki podpira Komisijo in države članice na področju certificiranja kibernetske varnosti.

Predlog obenem vzpostavlja evropski certifikacijski okvir za kibernetsko varnost za izdelke in storitve IKT ter podrobno določa bistvene funkcije in naloge agencije ENISA na področju certificiranja kibernetske varnosti. Okvir določa skupne določbe in postopke, ki omogočajo uvedbo vseevropskih certifikacijskih shem za kibernetsko varnost za posamezne izdelke in storitve IKT ali kibernetska tveganja. Oblikovanje evropskih certifikacijskih shem za kibernetsko varnost v skladu z okvirom bo omogočilo, da bodo certifikati, izdani na podlagi navedenih shem, veljavni in priznani v vseh državah članicah, ter bo obravnavalo zdajšnjo razdrobljenost trga.

1.4.6. Dodana vrednost ukrepanja Unije

Kibernetska varnost je resnično svetovni problem, ki po naravi presega meje in postaja vedno bolj medsektorski zaradi soodvisnosti med omrežji in informacijskimi sistemi. Število, kompleksnost in razsežnost kibernetskih incidentov ter njihov učinek na gospodarstvo in družbo naraščajo in naj bi se še dodatno povečali skupaj s tehnološkim razvojem, na primer širjenjem interneta stvari. To pomeni, da ne moremo pričakovati, da se bo potreba po večjih skupnih prizadevanjih držav članic, institucij EU in zasebnih zainteresiranih strani za reševanje kibernetskih groženj v prihodnosti zmanjšala.

Agencija ENISA si je od svoje ustanovitve leta 2004 prizadevala za spodbujanje sodelovanja med državami članicami in zainteresiranimi stranmi na področju varnosti omrežij in informacij, tudi s podpiranjem sodelovanja med javnim in zasebnim sektorjem. Ta podpora sodelovanju je vključevala tehnično delo za opredelitev kibernetskih groženj v EU, vzpostavitev strokovnih skupin in organizacijo vseevropskih vaj na področju kibernetskih incidentov in kriznega upravljanja za javni in zasebni sektor (zlasti Cyber Europe). Z direktivo o varnosti omrežij in informacij so bile agenciji ENISA dodeljene dodatne naloge, vključno z vlogo sekretariata mreže skupin CSIRT za operativno sodelovanje med državami članicami.

Dodana vrednost ukrepanja na ravni EU, zlasti za okrepitev sodelovanja med državami članicami, pa tudi med skupnostmi na področju varnosti omrežij in informacij, je bila priznana v sklepih Sveta[48] iz leta 2016 in je tudi jasno razvidna iz ocene agencije ENISA iz leta 2017, ki kaže, da je dodana vrednost Agencije predvsem njena zmožnost, da okrepi sodelovanje med temi zainteresiranimi stranmi. Na ravni EU ni nobenega drugega akterja, ki podpira sodelovanje tako različnih zainteresiranih strani na področju varnosti omrežij in informacij.

Dodana vrednost agencije ENISA pri združevanju skupnosti in zainteresiranih strani na področju kibernetske varnosti velja tudi za področje certificiranja. Porast kibernetske kriminalitete in varnostnih groženj je povzročil pojav nacionalnih pobud, ki določajo zahteve glede kibernetske varnosti in certificiranja na visoki ravni za sestavne dele IKT,

[48] Sklepi Sveta o krepitvi odpornosti evropskega sistema kibernetske varnosti ter spodbujanju konkurenčne in inovativne industrije kibernetske varnosti, 15. novembra 2016.

ki se uporabljajo v tradicionalni infrastrukturi. Čeprav so te pobude pomembne, lahko povzročijo razdrobljenost enotnega trga in ovire za interoperabilnost. Možno je, da mora ponudnik IKT opraviti več certifikacijskih postopkov, da lahko prodaja v več državah članicah.Ni verjetno, da bi lahko neuspešnost/neučinkovitost certifikacijskih shem rešili brez ukrepanja na ravni EU. Brez ukrepanja se bo razdrobljenost trga zelo verjetno povečala kratko- do srednjeročno (v naslednjih petih do desetih letih), saj se bodo pojavile nove sheme certificiranja. Pomanjkanje usklajevanja in interoperabilnosti takšnih shem zmanjšuje potencial enotnega digitalnega trga. To dokazuje dodano vrednost vzpostavitve evropskega certifikacijskega okvira za kibernetsko varnost za izdelke in storitve IKT, ki bo določal ustrezne pogoje za učinkovito reševanje težav, povezanih s soobstojem več certifikacijskih postopkov v različnih državah članicah, in zmanjšanje stroškov certificiranja, s čimer bo postalo certificiranje v EU na splošno privlačnejše s trgovskega in konkurenčnega vidika.

1.4.7. Spoznanja iz podobnih izkušenj v preteklosti

V skladu s pravno podlago za agencijo ENISA je Komisija izvedla oceno Agencije, ki je vključevala neodvisno študijo in javno posvetovanje. V oceni je bilo ugotovljeno, da so cilji agencije ENISA še vedno aktualni. Glede na tehnološki razvoj, spreminjajoče se grožnje ter znatno potrebo po večji varnosti omrežij in informacij v EU je potrebno tehnično znanje o razvoju vprašanj glede varnosti omrežij in informacij. V državah članicah je treba vzpostaviti zmogljivosti za razumevanje groženj in odzivanje nanje, zainteresirane strani pa morajo sodelovati na različnih tematskih področjih in medinstitucionalno.

Agencija je uspešno prispevala k večji varnosti omrežij in informacij v Evropi z zagotavljanjem krepitve zmogljivosti v 28 državah članicah ter spodbujanjem sodelovanja med državami članicami in zainteresiranimi stranmi na področju varnosti omrežij in informacij kot tudi zagotavljanjem strokovnega znanja, oblikovanjem skupnosti in podporo politikam.

Agenciji ENISA je uspelo vsaj deloma pustiti pečat na obsežnem področju varnosti omrežij in informacij, vendar ji ni v celoti uspelo razviti močne blagovne znamke ter pridobiti zadostne prepoznavnosti, da bi postala priznana kot glavno središče strokovnega znanja v Evropi. Razlog za to je v širokem mandatu agencije ENISA, ki pa ni imela sorazmerno velikih virov. Poleg tega agencija ENISA ostaja edina agencija EU z mandatom za določen čas, kar omejuje njeno zmožnost razvoja dolgoročne vizije in trajnostne podpore zainteresiranih strani. To je v nasprotju z določbami direktive o varnosti omrežij in informacij, ki agenciji ENISA dodeljujejo naloge brez končnega roka.

Kar zadeva kibernetsko certificiranje izdelkov in storitev IKT, trenutno ni nobenega evropskega okvira. Zaradi porasta kibernetske kriminalitete in varnostnih groženj so se pojavile nacionalne pobude, ki lahko vodijo v razdrobljenost enotnega trga.

1.4.8. Skladnost in možnosti sinergij z drugimi ustreznimi instrumenti

Pobuda v veliki meri upošteva obstoječe politike, zlasti na področju notranjega trga. Zasnovana je v skladu s splošnim pristopom h kibernetski varnosti, ki je bil opredeljen pri reviziji strategije za enotni digitalni trg, s katero naj bi dopolnili obsežen sklop ukrepov, kot so revizija strategije EU za kibernetsko varnost, načrt za sodelovanje ob kibernetskih krizah in pobude za boj proti kibernetski kriminaliteti. Zagotovila bi uskladitev z določbami obstoječe zakonodaje na področju kibernetske varnosti (zlasti direktive o varnosti omrežij in informacij), na katerih bi tudi temeljila, da bi tako še okrepila

kibernetsko odpornost EU z večjimi zmogljivostmi, sodelovanjem, obvladovanjem tveganj in kibernetsko ozaveščenostjo.

Predlagani ukrepi certificiranja bi morali obravnavati tveganje razdrobljenosti, ki ga prinašajo obstoječe in nove nacionalne certifikacijske sheme, in s tem prispevati k razvoju enotnega digitalnega trga. Pobuda tudi podpira in dopolnjuje izvajanje direktive o varnosti omrežij in informacij, tako da podjetjem, za katera velja direktiva, nudi orodje za dokazovanje skladnosti z zahtevami iz direktive o varnosti omrežij in informacij v celotni Uniji.

Predlagani evropski certifikacijski okvir za kibernetsko varnost na področju IKT ne posega v Splošno uredbo o varstvu podatkov[49], zlasti ustrezne določbe o certificiranju[50], kot se uporabljajo za varnost obdelave osebnih podatkov. Nenazadnje bi morale sheme, predlagane v prihodnjem evropskem okviru, čim bolj temeljiti na mednarodnih standardih, da bi tako preprečili nastanek ovir za trgovanje in zagotovili skladnost z mednarodnimi pobudami.

[49] Uredba (EU) 2016/679 z dne 27. aprila 2016 o varstvu posameznikov pri obdelavi osebnih podatkov in o prostem pretoku takih podatkov ter o razveljavitvi Direktive 95/46/ES (Splošna uredba o varstvu podatkov).

[50] Na primer člena 42 (Potrjevanje) in 43 (Organi za potrjevanje) ter členi 57, 58 in 70 glede ustreznih nalog oziroma pooblastil neodvisnih nadzornih organov oziroma nalog Evropskega odbora za varstvo podatkov.

1.5. Trajanje ukrepa in finančnih posledic

☐ **Časovno omejen(-a)** predlog/pobuda:

– ☐ trajanje predloga/pobude od [D. MMMM] LLLL do [D. MMMM] LLLL,

– ☐ finančne posledice med letoma LLLL in LLLL.

☒ **Časovno neomejen(-a)** predlog/pobuda:

– izvajanje z obdobjem uvajanja med letoma 2019 in 2020,

– ki mu sledi izvajanje predloga/pobude v celoti.

1.6. Načrtovani načini upravljanja[51]

☒ **Neposredno upravljanje** – Komisija (naslov III – Certificiranje):

– ☐ prek izvajalskih agencij.

☐ **Deljeno upravljanje** z državami članicami.

☒ **Posredno upravljanje** s poverjanjem nalog izvrševanja proračuna:

☐ mednarodnim organizacijam in njihovim agencijam (navedite),

☐ EIB in Evropskemu investicijskemu skladu,

☒ organom iz členov 208 in 209 (naslov II – Agencija ENISA),

☐ subjektom javnega prava,

☐ subjektom zasebnega prava, ki opravljajo javne storitve, kolikor ti subjekti zagotavljajo ustrezna finančna jamstva,

☐ subjektom zasebnega prava države članice, ki so pooblaščeni za izvajanje javno-zasebnih partnerstev in ki zagotavljajo ustrezna finančna jamstva,

☐ osebam, pooblaščenim za izvajanje določenih ukrepov SZVP v skladu z naslovom V PEU in opredeljenim v zadevnem temeljnem aktu.

Opombe

Uredba zajema: – naslov II predlagane uredbe zajema revizijo mandata Agencije Evropske unije za varnost omrežij in informacij (agencije ENISA), pri čemer Agenciji daje pomembno vlogo pri certificiranju; – naslov III določa okvir za oblikovanje evropskih certifikacijskih shem za kibernetsko varnost za izdelke in storitve IKT, pri katerem ima agencija ENISA pomembno vlogo.

[51] Pojasnila o načinih upravljanja in sklici na finančno uredbo so na voljo na spletišču BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

Navedite pogostost in pogoje.

Spremljanje se bo začelo takoj po sprejetju zakonodajnega akta in bo usmerjeno v njegovo izvajanje. Komisija bo organizirala sestanke z agencijo ENISA, predstavniki držav članic (npr. skupinami strokovnjakov) in zadevnimi zainteresiranimi stranmi, da bi zlasti olajšala izvajanje pravil o certificiranju, npr. ustanovitev odbora.

Prva ocena bi morala biti izvedena pet let po začetku veljavnosti pravnega instrumenta, če je na voljo dovolj podatkov. V pravni instrument je vključena tudi izrecna klavzula o oceni in pregledu [člen XXX], v skladu s katero bo Komisija izvedla neodvisno oceno. Komisija bo nato o oceni poročala Evropskemu parlamentu in Svetu ter ji bo po potrebi priložila predlog za revizijo akta, da se izmerita učinek Uredbe in njena dodana vrednost. Nadaljnje ocene bi morale biti izvedene vsakih pet let. Za ocene se bo uporabljala metodologija Komisije za boljše pravno urejanje. Ocene bodo izvedene s pomočjo usmerjenih strokovnih razprav, študij in širokih posvetovanj z zainteresiranimi stranmi.

Izvršni direktor agencije ENISA bi moral upravnemu odboru vsaki dve leti predložiti naknadno oceno dejavnosti Agencije. Agencija bi morala pripraviti tudi akcijski načrt za nadaljnje ukrepe glede ugotovitev naknadnih ocen in Komisiji vsaki dve leti poročati o napredku. Upravni odbor bi moral biti odgovoren za nadzor nad ustreznimi nadaljnjimi ukrepi na podlagi teh ugotovitev.

Domnevni primeri nepravilnosti v dejavnostih Agencije lahko preiskuje evropski varuh človekovih pravic v skladu z določbami člena 228 Pogodbe.

Viri podatkov za načrtovano spremljanje bi bili večinoma agencija ENISA, Evropska certifikacijska skupina za kibernetsko varnost, skupina za sodelovanje, mreža skupin CSIRT in organi držav članic. Poleg podatkov iz poročil (vključno z letnimi poročili o dejavnostih) agencije ENISA, Evropske certifikacijske skupine za kibernetsko varnost, skupine za sodelovanje in mreže skupin CSIRT bodo po potrebi uporabljena posebna orodja za zbiranje podatkov (npr. raziskave nacionalnih organov, raziskave Eurobarometer ter poročila v okviru kampanje meseca kibernetske varnosti in vseevropskih vaj).

2.2. Upravljavski in kontrolni sistem

2.2.1. Ugotovljena tveganja

Ugotovljena tveganja so omejena: agencija Unije že obstaja in njen mandat bo natančno določen, pri čemer bodo okrepljena področja, na katerih se je pokazalo, da ima Agencija jasno dodano vrednost, in dodana bodo nova področja, na katerih je potrebna podpora glede na nove prednostne naloge politik in instrumente, zlasti direktivo o varnosti omrežij in informacij, revizijo strategije EU za kibernetsko varnost, prihodnji načrt EU za kibernetsko varnost na področju sodelovanja ob kibernetskih krizah in varnostno certificiranje IKT.

Predlog zato podrobno opredeljuje naloge Agencije in prinaša večjo učinkovitost. Večje operativne pristojnosti in naloge ne pomenijo resničnega tveganja, saj bi dopolnjevale ukrepe

držav članic in jih podpirale na njihovo zahtevo ter v zvezi z omejenimi in vnaprej opredeljenimi storitvami.

Poleg tega predlagani model Agencije, skladen s skupnim pristopom, zagotavlja zadosten nadzor za zagotovitev, da agencija ENISA deluje v smeri zastavljenih ciljev. Operativna in finančna tveganja predlaganih sprememb se zdijo omejena.

Obenem je treba zagotoviti ustrezna finančna sredstva, da bi lahko agencija ENISA izpolnila naloge, ki so ji podeljene z novim mandatom, vključno na področju certificiranja.

2.2.2. Načrtovani načini kontrole

Zaključni račun Agencije, za katerega se uporablja postopek razrešnice, se predloži v odobritev Računskemu sodišču, načrtovane pa so tudi revizije.

Tudi varuh človekovih pravic nadzira delovanje Agencije v skladu z določbami člena 228 Pogodbe.

Glej točki 2.1 in 2.2.1.

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

Navedite obstoječe ali načrtovane preprečevalne in zaščitne ukrepe.

Uporabljali bi se preprečevalni in zaščitni ukrepi agencije ENISA, in sicer:

– Plačila zahtevanih storitev ali študij pred izplačilom preveri osebje Agencije, pri čemer upošteva pogodbene obveznosti, gospodarska načela ter dobro finančno prakso in dobro prakso upravljanja. Določbe o preprečevanju goljufij (nadzor, zahteve glede poročanja itn.) se vključijo v vse sporazume in pogodbe, ki jih sklenejo agencija in prejemniki plačil.

– Za boj proti goljufijam, korupciji in drugim nezakonitim dejavnostim se brez omejitev uporabljajo določbe Uredbe (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta z dne 11. septembra 2013 o preiskavah, ki jih izvaja Evropski urad za boj proti goljufijam (OLAF).

– Agencija v šestih mesecih od datuma začetka veljavnosti te uredbe pristopi k Medinstitucionalnemu sporazumu z dne 25. maja 1999 med Evropskim parlamentom, Svetom Evropske unije in Komisijo Evropskih skupnosti o notranjih preiskavah Evropskega urada za boj proti goljufijam (OLAF) in brez odlašanja izda ustrezne predpise, ki veljajo za vse zaposlene v Agenciji.

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

- Obstoječe proračunske vrstice

Po vrstnem redu razdelkov večletnega finančnega okvira in proračunskih vrstic.

Razdelek večletnega finančnega okvira	Proračunska vrstica	Vrsta odhodkov	Prispevek			
		dif./nedif.[52]	držav Efte[53]	držav kandidatk[54]	tretjih držav	po členu 21(2)(b) finančne uredbe
1a Konkurenčnost za rast in zaposlovanje	09 02 03 Agencija ENISA ter varnostno certificiranje informacijske in komunikacijske tehnologije	dif.	DA	NE	NE	NE
5 Odhodki za upravno delovanje]	09 01 01 Odhodki za aktivno zaposlene na področju „komunikacijska omrežja, vsebine in tehnologija“ 09 01 02 Odhodki za aktivno zaposleno zunanje osebje na področju „komunikacijska	nedif.	NE	NE	NE	NE

[52] Dif. = diferencirana sredstva / nedif. = nediferencirana sredstva.

[53] Efta: Evropsko združenje za prosto trgovino.

[54] Države kandidatke in po potrebi potencialne države kandidatke z Zahodnega Balkana.

	omrežja, vsebine in tehnologija“ 09 01 02 11 Ostali odhodki za upravljanje					

3.2. Ocenjene posledice za odhodke

3.2.1. Povzetek ocenjenih posledic za odhodke

v mio. EUR (na tri decimalna mesta natančno)

Razdelek večletnega finančnega okvira	1a	Konkurenčnost za rast in zaposlovanje

Agencija ENISA			**Osnovni scenarij** **2017 (31. 12. 2016)**		**2019** ***(od 1. 7. 2019)***	**2020**	**2021**	**2022**	**SKUPAJ**
Naslov 1: Odhodki za zaposlene *(vključno z odhodki za zaposlovanje, usposabljanje, socialno in zdravstveno infrastrukturo in zunanje storitve)*	obveznosti	(1)	6,387		9,899	12,082	13,349	13,894	**49,224**
	plačila	(2)	6,387		9,899	12,082	13,349	13,894	**49,224**
Naslov 2: Infrastruktura in odhodki iz poslovanja	obveznosti	(1a)	1,770		1,957	2,232	2,461	2,565	**9,215**
	plačila	(2a)	1,770		1,957	2,232	2,461	2,565	**9,215**
Naslov 3: Odhodki iz poslovanja	obveznosti	(3a)	3,086		4,694	6,332	6,438	6,564	**24,028**
	plačila	(3b)	3,086		4,694	6,332	6,438	6,564	**24,028**
Odobritve za agencijo ENISA SKUPAJ	obveznosti	= 1 + 1a + 3a	**11,244**		16,550	20,646	22,248	23,023	**82,467**
	plačila	= 2 + 2a + 3b	**11,244**		**16,550**	**20,646**	**22,248**	**23,023**	**82,467**

Razdelek večletnega finančnega okvira	**5**	„Upravni odhodki“

v mio. EUR (na tri decimalna mesta natančno)

		2019 *(od 1. 7. 2019)*	**2020**	**2021**	**2022**	**SKUPAJ**
GD CNECT						
• Človeški viri		0,216	0,846	0,846	0,846	**2,754**
• Drugi upravni odhodki		0,102	0,235	0,238	0,242	**0,817**
GD CNECT **SKUPAJ**	odobritve	0,318	1,081	1,084	1,088	**3,571**

Stroški zaposlenih so bili izračunani glede na predvideni datum zaposlitve (zaposlovanje je predvideno od 1. 7. 2019).

Predvideni viri po letu 2020 so okvirni in ne posegajo v predloge Komisije za večletni finančni okvir po letu 2020.

Odobritve iz RAZDELKA 5 večletnega finančnega okvira **SKUPAJ**	(obveznosti skupaj = plačila skupaj)	0,318	1,081	1,084	1,088	**3,571**

v mio. EUR (na tri decimalna mesta natančno)

	2019	**2020**	**2021**	**2022**	**SKUPAJ**

Odobritve iz RAZDELKOV od 1 do 5 večletnega finančnega okvira **SKUPAJ**	obveznosti	16,868	21,727	23,332	24,11	**86,038**
	plačila	16,868	21,727	23,332	24,11	**86,038**

3.2.2. Ocenjene posledice za odobritve Agencije

– ☐ Za predlog/pobudo niso potrebne odobritve za poslovanje.

– ☒ Za predlog/pobudo so potrebne odobritve za poslovanje, kot je pojasnjeno v nadaljevanju:

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

Cilji in realizacije[55] ⇩	**2019**	**2020**	**2021**	**2022**	**SKUPAJ**
Povečanje zmogljivosti in pripravljenosti držav članic in podjetij	1,408	1,900	1,931	1,969	7,208
Boljše sodelovanje in usklajevanje med državami članicami ter institucijami, agencijami in organi EU	0,939	1,266	1,288	1,313	4,806
Povečanje zmogljivosti na ravni EU, ki dopolnjujejo ukrepe držav članic, zlasti v primeru čezmejnih kibernetskih kriz	0,704	0,950	0,965	0,985	3,604
Povečanje ozaveščenosti državljanov in podjetij o vprašanjih kibernetske varnosti	0,704	0,950	0,965	0,985	3,604
Krepitev zaupanja v enotni digitalni trg in digitalne inovacije s povečanjem splošne preglednosti zagotovil izdelkov in storitev IKT glede kibernetske varnosti	0,939	1,266	1,288	1,313	4,806
STROŠKI SKUPAJ	4,694	6,332	6,437	6,565	24,028

[55] V preglednici so prikazani le odhodki iz poslovanja iz naslova 3.

3.2.3. Ocenjene posledice za človeške vire Agencije

3.2.3.1. Povzetek

– ☐ Za predlog/pobudo niso potrebne odobritve za upravne zadeve.

– ☒ Za predlog/pobudo so potrebne odobritve za upravne zadeve, kot je pojasnjeno v nadaljevanju:

v mio. EUR (na tri decimalna mesta natančno)

	Tretje/četrto četrtletje leta 2019	**2020**	**2021**	**2022**
Začasni uradniki (razredi AD)	4,242	5,695	6,381	6,709
Začasni uradniki (razredi AST)	1,601	1,998	2,217	2,217
Pogodbeni uslužbenci	2,041	2,041	2,041	2,041
Napoteni nacionalni strokovnjaki	0,306	0,447	0,656	0,796
SKUPAJ	**8,190**	**10,181**	**11,295**	**11,763**

Stroški zaposlenih so bili izračunani glede na predvideni datum zaposlitve (za sedanje zaposlene agencije ENISA je bila polna zaposlitev predvidena s 1. 1. 2019). Za nove zaposlene je bilo predvideno postopno zaposlovanje s 1. 7. 2019, pri čemer bi bila polna zaposlenost dosežena leta 2022. Predvideni viri po letu 2020 so okvirni in ne posegajo v predloge Komisije za večletni finančni okvir po letu 2020.

Ocenjene posledice za zaposlene (dodatni EPDČ) – kadrovski načrt

Funkcijska skupina in razred	2017 **Sedanja agencija ENISA**	Tretje/četrto četrtletje leta 2019	2020	2021	2022
AD16					
AD15	1				
AD14					
AD13					
AD12	3	3			
AD11					
AD10	5				
AD9	10	2			
AD8	15	4	2		1
AD7			3	3	2
AD6			3	3	
AD5					

Skupaj AD	34	9	8	6	3
AST11 AST10 AST9 AST8 AST7 AST6 AST5 AST4 AST3 AST2 AST1	 2 5 5 2	 1 2	 1 1	 1	
Skupaj AST	14	3	2	1	
AST/SC 6 AST/SC 5 AST/SC 4 AST/SC 3 AST/SC 2 AST/SC 1					
Skupaj AST/SC					
VSE SKUPAJ	48	12	10	7	3

Naloge za dodatne zaposlene AD/AST za dosego ciljev instrumenta, kot je opisano v razdelku 1.4.2:

Naloge	AD	AST	NNS	Skupaj
Politika in krepitev zmogljivosti	8	1		9
Operativno sodelovanje	8	1	7	16
Certificiranje (s trgom povezane naloge)	9	3	2	14
Znanje, informacije in ozaveščanje	1	1		2
SKUPAJ	26	6	9	41

Opis nalog:

Naloge	**Dodatni potrebni viri**
Razvoj in izvajanje politike EU ter krepitev zmogljivosti	Naloge bi vključevale pomoč skupini za sodelovanje, podpiranje doslednega izvajanja direktive o varnosti omrežij in informacij, redno poročanje o stanju izvajanja pravnega okvira EU, svetovanje in usklajevanje sektorskih pobud na področju kibernetske varnosti, vključno z energetiko, prometom (npr. letalstvom, cestnim prometom, pomorstvom in povezanimi vozili), zdravstvom, financami, ter zagotavljanje podpore

	za vzpostavitev centrov za izmenjavo in analizo informacij (ISAC) v različnih sektorjih.
Operativno sodelovanje in krizno upravljanje	**Naloge bi vključevale:** Zagotavljanje sekretariata za mrežo skupin CSIRT, med drugim z zagotavljanjem dobro delujoče informacijske infrastrukture in komunikacijskih kanalov mreže skupin CSIRT. Zagotavljanje strukturiranega sodelovanja s skupino CERT-EU, EC3 in drugimi zadevnimi organi EU. Organiziranje **vaj Cyber Europe**[56] – naloge v zvezi z nadgradnjo vaj, tako da bi dogodek, ki poteka enkrat na dve leti, postal vsakoletni dogodek, in zagotavljanjem, da se v okviru vaj incident preuči od začetka do konca. Naloge **tehnične pomoči** bi vključevale strukturirano sodelovanje s skupino CERT-EU, da se zagotovi tehnična pomoč v primeru večjih incidentov in podpora pri analizi incidenta. To bi vključevalo pomoč državam članicam pri reševanju incidentov in analizi šibkih točk, artefaktov in incidentov. Olajšanje sodelovanja med posameznimi državami članicami pri odzivanju v izrednih razmerah z analizo in združevanjem nacionalnih poročil o stanju na podlagi informacij, ki so jih države članice in drugi subjekti dali na razpolago Agenciji. **Načrt za usklajen odziv na velike čezmejne kibernetske incidente** – Agencija bo prispevala k razvoju sodelovalnega odziva na ravni Unije in ravni držav članic pri velikih čezmejnih incidentih ali krizah, povezanih s kibernetsko varnostjo, in sicer s številnimi nalogami, od prispevanja k situacijskemu zavedanju na ravni Unije do preskušanja načrtov za sodelovanje pri incidentih. **Naknadne tehnične preiskave nesreč** – izvajanje naknadnih tehničnih preiskav incidentov ali prispevanje k njim v sodelovanju z mrežo skupin CSIRT z namenom izdaje priporočil in krepitve zmogljivosti v obliki javnih poročil za boljše preprečevanje prihodnjih

[56] Cyber Europe je doslej najobsežnejša in najbolj celovita vaja EU na področju kibernetske varnosti, v kateri sodeluje več kot 700 strokovnjakov iz 28 držav članic. Poteka vsako drugo leto. Ocena agencije ENISA in strategija EU za kibernetsko varnost iz leta 2013 kažeta, da številne zainteresirane strani glede na hiter razvoj kibernetskih groženj zagovarjajo organiziranje vsakoletnega dogodka. Vendar to trenutno ni izvedljivo zaradi omejenih virov Agencije.

	incidentov.
S trgom povezane naloge (standardizacija, certificiranje)	Naloge bi vključevale dejavno podpiranje dela, opravljenega v okviru certifikacijskega okvira, vključno z zagotavljanjem tehničnega strokovnega znanja za pripravo predlog za evropske certifikacijske sheme za kibernetsko varnost. Naloge bodo vključevale tudi podporo za oblikovanje in izvajanje politik Unije na področju standardizacije, certificiranja in tržnega observatorija. Zato bo treba spodbujati uporabo standardov za obvladovanje tveganj pri elektronskih izdelkih, omrežjih in storitvah ter svetovati izvajalcem bistvenih storitev in ponudnikom digitalnih storitev glede zahtev za tehnično varnost. Naloge bodo vključevale tudi pripravo analize glavnih trendov na trgu kibernetske varnosti.
Znanje in informacije, ozaveščanje:	Za zagotavljanje lažjega dostopa do bolje strukturiranih informacij o tveganjih na področju kibernetske varnosti in možnih rešitvah predlog dodeljuje Agenciji nove naloge razvoja in vzdrževanja „informacijskega vozlišča“ Unije. Naloge bi vključevale zbiranje in urejanje informacij o varnosti omrežij in informacijskih sistemov, zlasti o kibernetski varnosti, ki jih predložijo institucije, agencije in organi Unije, ter dajanje teh informacij na voljo javnosti prek namenskega portala. Naloge bi vključevale tudi podporo dejavnostim agencije ENISA na področju ozaveščanja, kar bi Agenciji omogočilo okrepiti prizadevanja.

3.2.3.2. Ocenjene potrebe po človeških virih za matični GD

– ☐ Za predlog/pobudo niso potrebni človeški viri.

– ☒ Za predlog/pobudo so potrebni človeški viri, kot je pojasnjeno v nadaljevanju:

ocena, izražena v celih številkah (ali na največ eno decimalno mesto natančno)

		Dodatni uslužbenci			
	Osnovni scenarij 2017	Tretje/četrto četrtletje 2019	2020	2021	2020
• **Delovna mesta v skladu s kadrovskim načrtom (uradniki in začasni uslužbenci)**					
09 01 01 01 (sedež in predstavništva Komisije)	1	2	3		
• **Zunanji sodelavci (v ekvivalentu polnega delovnega časa: EPDČ)**[57]					
09 01 02 01 (PU, NNS, ZU iz splošnih sredstev)	1	2			
SKUPAJ		**4**	**3**		

Opis nalog:

Uradniki in začasni uslužbenci	Zastopajo Komisijo v upravnem odboru Agencije. Pripravijo mnenje Komisije o enotnem programskem dokumentu agencije ENISA in spremljajo njegovo izvajanje. Nadzorujejo pripravo proračuna Agencije in spremljajo njegovo izvrševanje. Pomagajo Agenciji pri razvoju njenih dejavnosti v skladu s politikami Unije, tudi s sodelovanjem na sestankih delovnih skupin. Nadzirajo izvajanje okvira za evropske certifikacijske sheme za kibernetsko varnost za izdelke in storitve IKT. Vzdržujejo stike z državami članicami in drugimi zadevnimi zainteresiranimi stranmi glede certificiranja. Sodelujejo z agencijo ENISA glede predlog za sheme. Pripravijo predloge za evropske sheme na področju kibernetske varnosti.

[57] PU = pogodbeni uslužbenec; LU = lokalni uslužbenec; NNS = napoteni nacionalni strokovnjak; ZU = začasni uslužbenec; MSD = mladi strokovnjak na delegaciji.

Zunanji sodelavci	Kot zgoraj.

3.2.4. Skladnost z veljavnim večletnim finančnim okvirom

– ☐ Predlog/pobuda je v skladu z veljavnim večletnim finančnim okvirom.

– ☒ Za predlog/pobudo je potrebna sprememba zadevnega razdelka večletnega finančnega okvira.

Za predlog je potrebna sprememba člena 09 02 03 zaradi revizije mandata agencije ENISA, ki Agenciji nalaga nove naloge, med drugim v zvezi z izvajanjem direktive o varnosti omrežij in informacij ter evropskim certifikacijskim okvirom za kibernetsko varnost. Ustrezni zneski:

Leto	Predvideni znesek	Zahtevani znesek
2019	10,739	16,550
2020	10,954	20,646
2021	ni relevantno	22,248*
2022	ni relevantno	23,023*

* To je ocena. Financiranje EU po letu 2020 bo preučeno v razpravi znotraj Komisije o vseh predlogih za obdobje po letu 2020. To pomeni, da bo Komisija po predložitvi predloga za naslednji večletni finančni okvir predložila tudi spremenjeno oceno finančnih posledic zakonodajnega predloga, pri čemer bo upoštevala sklepne ugotovitve ocene učinka[58].

– ☐ Za predlog/pobudo je potrebna uporaba instrumenta prilagodljivosti ali sprememba večletnega finančnega okvira[59].

3.2.5. Udeležba tretjih oseb pri financiranju

– ☐ V predlogu/pobudi ni načrtovano sofinanciranje tretjih oseb.

– ☒ V predlogu/pobudi je načrtovano sofinanciranje, kot je ocenjeno v nadaljevanju:

	Leto **2019**	Leto **2020**	Leto **2021**	Leto **2022**
Efta	p. m[60].	p. m.	p. m.	p. m.

58 Povezava na stran z oceno učinka.

59 Glej člena 11 in 17 Uredbe Sveta (EU, Euratom) št. 1311/2013 o večletnem finančnem okviru za obdobje 2014–2020.

60 Točni znesek za naslednja leta bo znan, ko bo za zadevno leto določen sorazmernostni faktor Efte.

3.3. Ocenjene posledice za prihodke

– ☒ Predlog/pobuda nima finančnih posledic za prihodke.

– ☐ Predlog/pobuda ima finančne posledice, kot je pojasnjeno v nadaljevanju:

  – ☐ za lastna sredstva,

  – ☐ za razne prihodke.