Svet
Evropske unije

Bruselj, 29. maj 2018
(OR. en)

9350/18

Medinstitucionalna zadeva:
2017/0225 (COD)

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

DOPIS

Pošiljatelj:	predsedstvo
Prejemnik:	Svet
Št. predh. dok.:	8834/18
Št. dok. Kom.:	12183/17
Zadeva:	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) – splošni pristop

I. UVOD

1. Komisija je 13. septembra 2017 v okviru strategije za enotni digitalni trg sprejela zadevni predlog[1], katerega pravna podlaga je člen 114 PDEU, ter ga posredovala Svetu in Evropskemu parlamentu. Namen predloga, ki je del t. i. svežnja o kibernetski varnosti, je vzpostaviti visoko raven kibernetske varnosti, kibernetske odpornosti in zaupanja v Uniji, da bi zagotovili pravilno delovanje notranjega trga.

2. Predlagana uredba določa cilje, naloge in organizacijske vidike agencije ENISA – Agencije EU za kibernetsko varnost ter oblikuje okvir za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost za zagotavljanje ustrezne ravni kibernetske varnosti izdelkov in storitev IKT v Uniji. Predlogu Komisije je priložena ocena učinka, v kateri je preučen poseben niz osmih možnosti politike v zvezi s pregledom agencije ENISA in certificiranjem kibernetske varnosti IKT.

3. Predlagana uredba obravnava dve pomembni vprašanji:

   - trajno pooblastilo za Agencijo z natančno določenim obsegom glede na potrebe v okviru novih prednostnih nalog in instrumentov politike ter prenovljenim sklopom nalog in funkcij Agencije, da bi lahko uspešno in učinkovito podpirala prizadevanja držav članic, institucij EU in drugih deležnikov za zagotovitev varnega kibernetskega prostora;

   - evropski certifikacijski okvir za kibernetsko varnost za izdelke in storitve IKT in pravila, ki urejajo evropske certifikacijske sheme za kibernetsko varnost, kar bo omogočilo, da bodo certifikati, izdani na podlagi navedenih shem, veljavni in priznani v vseh državah članicah, ter odpravljena zdajšnja razdrobljenost trga.

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

4. Evropski svet[2] je oktobra 2017 pozval Komisijo, naj bodo njeni predlogi o kibernetski varnosti celostni, pravočasno predloženi in nemudoma preučeni na podlagi akcijskega načrta, ki ga bo oblikoval Svet.

5. Svet za splošne zadeve je 12. decembra 2017 sprejel akcijski načrt[3] za izvajanje sklepov Sveta[4] o Skupnem sporočilu[5] Evropskemu parlamentu in Svetu: „Odpornost, odvračanje in obramba: okrepitev kibernetske varnosti za EU“. V akcijskem načrtu je izražena namera Sveta, da bi se do junija 2018 dogovorili o splošnem pristopu glede predloga.

6. V Evropskem parlamentu je bila za poročevalko imenovana Angelika NIEBLER (ITRE, EPP). Odbor ITRE naj bi o poročilu glasoval 19. junija 2018.

7. Evropski ekonomsko-socialni odbor je mnenje sprejel 14. februarja 2018.

II. DELO V SVETU

8. Komisija je ta predlog in pripadajočo oceno učinka predstavila na seji Horizontalne delovne skupine za kibernetska vprašanja (v nadaljnjem besedilu: delovna skupina) 26. septembra 2017; delovna skupina je oceno učinka nato obravnavala na seji 20. oktobra 2017. Nadaljnje razprave so bile osredotočene na operativno zmogljivost Agencije in obseg sodelovanja s pristojnimi nacionalnimi organi ter na vpliv certifikacijskega okvira na trg in konkurenčnost podjetij. Tako ocena učinka kot predlog sta na splošno naletela na pozitiven odziv delegacij.

---

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

9. Delovna skupina je o samem predlogu začela razpravljati novembra 2017 v okviru estonskega predsedstva, razprave pa so se nadaljevale še v času bolgarskega predsedovanja. Obravnavi tega predloga je bilo namenjenih 12 sej, na podlagi katerih je nastalo osem zaporednih spremenjenih različic predloga, da bi dosegli dogovor o splošnem pristopu na naslednji seji Sveta PTE (telekomunikacije) 8. junija 2018.

10. Izid razprav v delovni skupini, ki so potekale 14 in 15. maja 2018, ter revidirano kompromisno besedilo predsedstva sta v prilogi k temu dopisu. Uvodne izjave so bile prilagojene, da odražajo spremembe v vsebinskih določbah. Spremembe v primerjavi s predlogom Komisije so označene s **krepkim tiskom** ali znakom [...]. Spremembe glede na zadnji dokument delovne skupine 8834/18 so označene s **krepkim podčrtanim tiskom**, črtano besedilo pa je označeno z znakom **[...]**.

III. SKLEPNA UGOTOVITEV

11. Kompromisno besedilo predsedstva iz priloge odraža prizadevanja predsedstva in držav članic, da v besedilu najdejo ustrezno ravnotežje.

12. Odbor stalnih predstavnikov je 25. maja 2018 dosegel dogovor o kompromisnem besedilu predsedstva ob upoštevanju sprememb v členih 19(5) in 48(5), kot je navedeno v prilogi.

13. Svet naj zato na seji 8. junija 2018 sprejme splošni pristop in predsedstvo pooblasti za začetek pogajanj s predstavniki Evropskega parlamenta in Evropske komisije o tej zadevi.

PRILOGA

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o *„Agenciji [...] Evropske unije 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[6],

ob upoštevanju mnenja Odbora regij[7],

v skladu z rednim zakonodajnim postopkom,

[6] UL C,, str. .
[7] UL C,, str. .

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 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[8] 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[9], s katero sta mandat Agencije podaljšala do marca 2012. Z Uredbo (ES) št. 580/2011[10] se je mandat Agencije podaljšal do 13. septembra 2013. Leta 2013 sta Evropski parlament in Svet sprejela Uredbo (EU) št. 526/2013[11] o agenciji ENISA in razveljavitvi Uredbe (ES) št. 460/2004, s katero je bil mandat Agencije podaljšan do junija 2020.

---

8 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).

9 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).

10 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).

11 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 varnosti 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 deležniki, 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 **podpirati [...] nacionalna prizadevanja in proaktivno prispevati** k prizadevanjem Unije ter obenem opravljati svoje naloge ob popolnem sodelovanju z institucijami, [...] agencijami **in organi** držav članic. Poleg tega bi moralo delo Agencije temeljiti na prispevkih in sodelovanju zasebnega sektorja ter drugih zadevnih deležnikov. 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 ter prava na področju kibernetske varnosti **in njenih sektorskih vidikov, da bi politike in pravo EU bolj prilagodili kibernetski razsežnosti in omogočili njihovo usklajeno izvajanje na nacionalni ravni [...]**. 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, [...] agencijam **in organom** Unije pomagati pri njihovih prizadevanjih za vzpostavljanje in krepitev zmogljivosti in pripravljenosti za preprečevanje, odkrivanje in odzivanje na [...] **grožnje** 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. **Dejavnosti, ki jih agencija ENISA izvaja v zvezi z operativnimi zmogljivostmi držav članic, bi morale biti zgolj dopolnitev ukrepov, ki jih države članice sprejmejo zaradi izpolnitve obveznosti v skladu z direktivo o varnosti omrežij in informacij, in jih zato ne bi smele nadomeščati** [...].

(15a) Agencija bi morala pomagati tudi pri oblikovanju in posodabljanju strategij Unije za varnost omrežij in informacijskih sistemov, na zahtevo pa tudi strategij držav članic, zlasti na področju kibernetske varnosti, ter spodbujati razširjanje teh strategij in spremljati njihovo izvajanje. 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) Zaradi [...] spodbujanja sodelovanje med javnim in zasebnim sektorjem ter znotraj zasebnega sektorja **bi morala Agencija podpirati znotrajsektorsko in medsektorsko izmenjavo informacij, zlasti v sektorjih iz Priloge II k Direktivi (EU) 2016/1148, in sicer z zagotavljanjem najboljših praks in smernic o razpoložljivih orodjih, postopkov ter smernic o tem, kako obravnavati regulativna vprašanja, povezana z izmenjavo informacij, na primer z omogočanjem lažjega** [...] ustanavljanja sektorskih centrov za izmenjavo in analizo informacij (ISAC) [...].

(18) Agencija bi morala zbrati in analizirati nacionalna poročila skupin CSIRT in skupine CERT-EU, **ki so bila prostovoljno dana v skupno rabo, da bi tako pomagala državam članicam** določiti skupne [...] **postopke**, 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 [...] **znotraj** 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. To nalogo bi morala **izvajati v skladu s svojim mandatom na podlagi te uredbe in pristopom, o katerem se dogovorijo države članice v okviru priporočila Komisije o usklajenem odzivu na velike kibernetske incidente in krize. To bi lahko vključevalo** zbiranje ustreznih informacij ter posredovanje med mrežo skupin CSIRT, tehnično skupnostjo in nosilci odločitev, pristojnimi za krizno upravljanje. Poleg tega bi Agencija lahko dajala podporo pri obvladovanju 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 [...] **rednih** vaj na področju kibernetske varnosti.

(20) Agencija bi morala [...] **med podpiranjem** operativnega **sodelovanja** uporabljati razpoložljivo **tehnično in operativno** strokovno znanje skupine CERT-EU prek strukturiranega sodelovanja [...]. [...] Po potrebi bi bilo treba sprejeti posebne dogovore med tema dvema organizacijama, s katerimi bi določili praktično izvajanje tega sodelovanja **in se izogibali podvajanju dejavnosti**.

(21) **Zaradi podpore operativnemu sodelovanju v mreži skupin CSIRT** bi morala Agencija v skladu s svojimi [...] nalogami imeti možnost, da države članice **na njihovo zahtevo** podpira, na primer s svetovanjem **o načinih za izboljšanje njihove zmogljivosti za preprečevanje in odkrivanje incidentov ter odzivanje nanje z [...] omogočanjem lažjega** [...] tehničnega **obvladovanja incidentov, ki imajo pomembne ali znatne posledice,** [...] ali **z** opravljanjem analiz groženj in incidentov. **Agencija ENISA bi omogočala lažje tehnično obvladovanje incidentov, ki imajo pomembne ali znatne posledice, zlasti tako, da bi podpirala prostovoljno izmenjavo tehničnih rešitev med državami članicami ali s pripravo kombiniranih tehničnih informacij, na primer o tehničnih rešitvah, ki si jih države članice prostovoljno izmenjujejo.** 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 [...] **podpiranju operativnega sodelovanja**.

(22) Kot del rednega sodelovanja na tehnični ravni za podporo situacijskemu zavedanju v Uniji bi morala Agencija redno **in ob tesnem sodelovanju z državami članicami** 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 [...] ali enotne kontaktne točke iz direktive o varnosti omrežij in informacij **(v obeh primerih na prostovoljni podlagi)**, 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) **Podpora Agencije pri** naknadnih tehničnih preiskavah incidentov z znatnimi posledicami, [...] opravljenih na zahtevo [...] **zadevnih** držav članic, bi morala biti usmerjena na preprečevanje prihodnjih incidentov [...]. **Da bi Agenciji omogočile, da učinkovito podpre tehnične preiskave, bi morale zadevne države članice zagotoviti potrebne informacije.**

(24) [...]

(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, **ki so javno dostopne ali prostovoljno izmenjane,** 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 [...] **kibernetskih incidentov** z opravljanjem analiz groženj in incidentov.

(27) Da bi povečali odpornost Unije, bi morala Agencija razvijati odličnost na področju **kibernetske** varnosti [...] **infrastrukture, ki podpira zlasti sektorje iz Priloge II k Direktivi o varnosti omrežij in informacij, ter infrastrukture, ki jo uporabljajo ponudniki digitalnih storitev iz Priloge III k navedeni direktivi, in sicer** 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, [...] agencijami **in organi** 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 svetovanje o osnovni 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 lahko Agencija v celoti izpolnila 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)**, Agencijo za evropski globalni satelitski navigacijski sistem (Agencijo za evropski GNSS)** [...] 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 deležnikov 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 **v vlogi** [...] sekretariata 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 [...] **redne** 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 vzdrževanju 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 deležniki 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, [...] agencijam **in organom** [...] Unije ter, po potrebi in na njihovo zahtevo, državam članicam glede potreb pri raziskavah na področju [...] kibernetske varnosti. **Zaradi ugotavljanja raziskovalnih potreb in prednostnih nalog bi se morala Agencija posvetovati tudi z ustreznimi skupinami uporabnikov.**

(37) [...] Kibernetske **grožnje** imajo svetovno razsežnost. Da bi se izboljšali standardi **kibernetske** varnostni, 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, [...] agencijam **in organom** 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, **tudi o izvajanju letnega delovnega programa**, 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 deležnikov, ki bi delovala kot svetovalni organ, da bi zagotovila reden dialog z zasebnim sektorjem, združenji potrošnikov in drugimi ustreznimi deležniki. Stalna skupina deležnikov, ki jo na predlog izvršnega direktorja ustanovi upravni odbor, bi morala obravnavati zadeve, ki so pomembne za deležnike, in o njih obvestiti Agencijo. Sestava stalne skupine deležnikov, ki naj bi svetovala zlasti v zvezi z osnutkom delovnega programa, in naloge, dodeljene tej skupini, bi morale zagotoviti zadostno zastopanost deležnikov 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[12]. 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[13]. 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.

---

[12] 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).

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

(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) [...]

(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 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 sektor 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 **postopkov,** 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 je SOG-IS [...] najpomembnejši model za sodelovanje in vzajemno priznavanje na področju varnostnega certificiranja, pa vključuje samo del držav članic EU. 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 **ter izjave EU o skladnosti** 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 **evropskih** standardih [...], 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 **postopkov,** izdelkov in storitev IKT. Te sheme bi morali izvajati in nadzorovati nacionalni organi za [...] **certificiranje kibernetske varnosti,** certifikati, izdani v okviru teh shem, pa 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 bi morale zagotoviti, da **postopki,** izdelki in storitve IKT, ki so bili certificirani v skladu s takimi shemami, izpolnjujejo določene zahteve [...]**, da se zaščitijo** razpoložljivost, avtentičnost, celovitost in zaupnost 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 celotnem življenjskem ciklu** v smislu te uredbe. V tej uredbi ni mogoče podrobno določiti zahtev glede kibernetske varnosti, ki se nanašajo na vse **postopke,** izdelke in storitve IKT. **Postopki,** 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 **postopkih,** 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, **kadar ustrezni standardi niso na voljo**.

(55a) Tehnične specifikacije, ki naj bi bile uporabljene v evropski certifikacijski shemi za kibernetsko varnost, bi bilo treba določiti ob upoštevanju načel, določenih v Prilogi II k Uredbi (EU) št. 1025/2012. Toda v ustrezno utemeljenih primerih bi morda bila potrebna nekatera odstopanja od teh načel, kadar naj bi bile navedene tehnične specifikacije uporabljene v evropski certifikacijski shemi za kibernetsko varnost, ki se nanaša na visoko stopnjo zagotovila. Razlogi za takšna odstopanja morajo biti objavljeni.

(55b) Certifikacijsko ugotavljanje skladnosti je postopek ugotavljanja, ali so posebne zahteve glede postopka, izdelka, ali storitve izpolnjene. Ta postopek izvede neodvisna tretja oseba, ki ni proizvajalec izdelka ali ponudnik storitev. Postopek izdaje certifikata se izpelje po uspešni oceni postopka, izdelka ali storitve IKT. To bi moralo veljati kot potrdilo, da je bila zadevna ocena ustrezno opravljena. Evropska shema za kibernetsko varnost bi glede na stopnjo zagotovila morala določati, ali certifikat izda zasebni ali javni organ. Ugotavljanje skladnosti in 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 testirani ter da izpolnjujejo nekatere zahteve glede kibernetske varnosti, določene drugje, na primer v tehničnih standardih.

(55c) Uporabnik certifikata naj izbere ustrezno raven certifikacije in z njo povezanih varnostnih zahtev na podlagi analize tveganja v zvezi z uporabo postopka, izdelka ali storitve IKT. Stopnja zagotovila bi morala biti sorazmerna s stopnjo tveganja, povezano s predvideno uporabo postopka, izdelka ali storitve IKT.

(55d) Evropska certifikacijska shema za kibernetsko varnost bi lahko omogočala, da se ugotavljanje skladnosti izvede na izključno odgovornost proizvajalca ali ponudnika izdelkov in storitev IKT (samoocenjevanje skladnosti). V takih primerih bi bilo dovolj, da proizvajalec ali ponudnik sam izvede vse preglede, da bi zagotovil skladnost postopkov, izdelkov ali storitev IKT s certifikacijsko shemo. Ta vrsta ugotavljanja skladnosti bi bila primerna za manj kompleksne izdelke in storitve IKT (npr. preprosta zasnova in mehanizem proizvodnje), ki pomenijo nizko tveganje za javni interes. Poleg tega bi se lahko samoocenjevanje skladnosti izvedlo samo pri izdelkih in storitvah IKT, ki ustrezajo osnovni stopnji zagotovila.

(55e) V okviru evropske certifikacijske sheme za kibernetsko varnost bi se lahko dopustilo tako certificiranje kot tudi samoocenjevanje skladnosti izdelkov in storitev IKT. V teh primerih bi morala shema potrošnikom in drugim uporabnikom ponuditi jasne in razumljive načine za razlikovanje med izdelki in storitvami, ki so ocenjeni na odgovornost proizvajalca ali ponudnika, ter izdelki in storitvami, ki jih je certificirala tretja stran.

(55f) Proizvajalec ali ponudnik izdelkov in storitev IKT, ki izvede samoocenjevanje skladnosti, bi moral v okviru postopka ugotavljanja skladnosti oblikovati in podpisati izjavo EU o skladnosti. Izjava EU o skladnosti je dokument, v katerem je navedeno, da nek izdelek ali storitev IKT izpolnjuje zahteve sheme. Proizvajalec ali ponudnik z oblikovanjem in podpisom izjave EU o skladnosti prevzame odgovornost za skladnost izdelka ali storitve IKT s pravimi zahtevami sheme. Kopijo izjave EU o skladnosti bi bilo treba predložiti nacionalnemu organu za certificiranje kibernetske varnosti in agenciji ENISA.

(55g) Proizvajalec ali ponudnik izdelkov in storitev IKT bi moral za obdobje, opredeljeno v določeni evropski certifikacijski shemi za kibernetsko varnost, hraniti izjavo EU o skladnosti in tehnično dokumentacijo z vsemi ustreznimi informacijami, ki se nanašajo na skladnost izdelkov ali storitev IKT s shemo, tako da je na voljo pristojnemu nacionalnemu organu za certificiranje kibernetske varnosti. V tehnični dokumentaciji bi morale biti določene veljavne zahteve, pri čemer v obsegu, ki je pomemben za tako ugotavljanje, zajema zasnovo, proizvodnjo in delovanje izdelka ali storitve IKT. Tehnična dokumentacija bi morala biti pripravljena tako, da bi omogočala ugotavljanje skladnosti izdelkov in storitev IKT z ustreznimi zahtevami.

(55h) Države članice in zainteresirane organizacije deležnikov bi morale imeti možnost, da Evropski certifikacijski skupini za kibernetsko varnost predlagajo pripravo predloge za shemo. Zainteresirane organizacije deležnikov so predstavniki sektorja in potrošniških organizacij, kar vključuje tudi predstavnike organizacij MSP, ki imajo upravičen interes za razvoj posamezne evropske certifikacijske sheme za kibernetsko varnost. Te predloge bi bilo treba preučiti z vidika meril, ki jih oblikuje Evropska certifikacijska skupina za kibernetsko varnost na podlagi smernic, utemeljenih na načelih preglednosti, odprtosti, nepristranskosti, konsenza, uspešnosti, ustreznosti in skladnosti.

(56) Komisijo **in skupino** bi morali pooblastiti, da od agencije ENISA zahtevata, naj **brez nepotrebnega odlašanja** pripravi predloge za sheme za posamezne **postopke,** 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 **postopkov,** izdelkov in storitev IKT, podrobno specifikacijo zahtev glede kibernetske varnosti, na primer s sklicem na standarde ali tehnične specifikacije, posebnimi merili in metodami za ocenjevanje ter predvideno stopnjo zagotovila – osnovno, znatno in/ali visoko – **in po potrebi stopnje ocenjevanja**.

(56a) Zagotovilo evropske certifikacijske sheme za kibernetsko varnost je podlaga za zaupanje, da postopek, izdelek ali storitev IKT izpolnjuje varnostne zahteve določene evropske certifikacijske sheme za kibernetsko varnost; Zaradi skladnosti okvira za certificirane postopke, izdelke in storitve IKT bi lahko evropska certifikacijska shema za kibernetsko varnost opredeljevala stopnje zagotovila za evropske certifikate kibernetske varnosti in izjave EU o skladnosti, izdane v okviru te sheme. Vsak certifikat bi se lahko nanašal na eno od stopenj zagotovil: osnovno, znatno ali visoko, medtem ko bi se lahko izjava EU o skladnosti nanašala samo na osnovno stopnjo zagotovila. Stopnje zagotovila opredeljujejo ustrezno stopnjo prizadevanj za oceno [...] in so opredeljene s sklici na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je ublažiti ali preprečiti kibernetske incidente. Vsaka stopnja zagotovila bi morala biti usklajena s posameznimi sektorskimi področji, v katerih se uporablja certificiranje.

(56b) V evropski certifikacijski shemi za kibernetsko varnost se lahko določi več stopenj ocenjevanja – odvisno od strogosti in obsega uporabljene metodologije za ocenjevanje –, ki bi morale ustrezati eni od stopenj zagotovila in biti povezane z ustrezno kombinacijo elementov, ki sestavljajo zagotovilo. Izdelek ali storitev IKT bi moral za vse stopnje zagotovila vsebovati vrsto varnih funkcij, kot so opredeljene s shemo in ki lahko vključujejo: varne vnaprej določene konfiguracije, podpisane kode, varne posodobitve in ublažitev nevarnosti izkoriščanja ter polna zaščita spomina, organiziranega v skladu/kopici. Te funkcije bi bilo treba razvijati in vzdrževati z uporabo v varnost usmerjenega razvojnega pristopa in pripadajočih orodij, da bi tako zagotovili zanesljivo vključitev učinkovitih mehanizmov (za programsko in strojno opremo). Pri osnovni stopnji zagotovila bi morali vodilo ocenjevanja biti vsaj naslednji elementi zagotovila: organ za ugotavljanje skladnosti bi moral pri ocenjevanju najmanj pregledati tehnično dokumentacijo izdelka ali storitve IKT. Kadar certifikacija vključuje tudi postopke IKT, bi bilo treba tehničnemu pregledu podvreči tudi postopek, uporabljen pri zasnovi, razvoju in vzdrževanju izdelka ali storitve IKT. Če evropska certifikacijska shema za kibernetsko varnost predvideva samoocenjevanje skladnosti, bi moralo zadostovati, da proizvajalec ali ponudnik izvede samooceno skladnosti postopkov, izdelkov ali storitev IKT s certifikacijsko shemo. Pri znatni stopnji zagotovila bi moralo vodilo ocenjevanja poleg elementov iz osnovne stopnje zagotovila biti vsaj še preverjanje skladnosti varnostnih funkcionalnosti izdelka ali storitve IKT s pripadajočo tehnično dokumentacijo. Pri visoki stopnji zagotovila bi moralo vodilo ocenjevanja poleg elementov iz znatne stopnje zagotovila biti vsaj še testiranje učinkovitosti, s katerim se preveri odpornost varnostnih funkcionalnosti izdelka ali storitve IKT proti izvajalcem kompleksnih kibernetskih napadov, ki imajo precejšnje znanje in vire.

(56c) Agencija ENISA bi se morala ob pripravi predloge za shemo posvetovati z vsemi ustreznimi deležniki, npr. z evropskimi organizacijami za standardizacijo, ustreznimi nacionalnimi organi, organizacijami, utemeljenimi na sporazumih o vzajemnem priznavanju, kot je na primer SOG-IS MRA, MSP, potrošniškimi organizacijami, pa tudi deležniki, ki zastopajo okoljske in socialne interese.

(56d) Agencij ENISA bi morala vzdrževati spletišče, namenjeno obveščanju javnosti o evropskih certifikacijskih shemah za kibernetsko varnost, ki bi med drugim moralo vključevati zahteve za pripravo predloge za evropsko certifikacijsko shemo za kibernetsko varnost, pa tudi povratne informacije, prejete med posvetovalnim postopkom, ki ga je v pripravljalni fazi izvedla agencija ENISA. Takšno spletišče bi moralo vsebovati tudi informacije o certifikatih in izjavah EU o skladnosti, izdanih na podlagi te uredbe.

(57) Uporaba evropskega certificiranja kibernetske varnosti **in izjave EU o skladnosti** bi morala ostati prostovoljna, razen če je v zakonodaji Unije ali nacionalni zakonodaji, **sprejeti v skladu s pravom Unije,** določeno drugače. **Kadar zakonodaja ni usklajena, lahko države članice sprejmejo nacionalne tehnične predpise v skladu z Direktivo (EU) 2015/1535 in določijo obvezno certificiranje v okviru evropske certifikacijske sheme za kibernetsko varnost. Države članice lahko evropsko certificiranje na področju kibernetske varnosti uporabijo tudi v okviru javnega naročanja in Direktive 2014/24/EU**.[...]

(57a) Da 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. Vendar državam članicam ne bi smeli preprečiti, da sprejmejo ali ohranjajo nacionalne certifikacijske sheme za namene nacionalne varnosti.

(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 **omejiti, začasno preklicati ali** 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) [...]Države članice [...]**bi morale** imenovati enega **ali več** [...] **organov** za certificiranje kibernetske varnosti, ki bi nadzoroval skladnost **z zahtevami iz te uredbe. Če država članica meni, da je to primerno, se lahko te naloge dodelijo tudi že obstoječim organom. Države članice bi poleg tega morale imeti možnost, da v dogovoru z drugo državo članico imenujejo enega ali več nadzornih organov na ozemlju te druge države članice. Ta organ bi moral zlasti spremljati in izvrševati obveznosti proizvajalcev ali ponudnikov izdelkov in storitev IKT s sedežem na njegovem ozemlju, ki se nanašajo na izjavo EU o skladnosti, nacionalnim akreditacijskim organom pomagati pri spremljanju in nadziranju dejavnosti organov za ugotavljanje skladnosti, tako da jim zagotavlja strokovno znanje in potrebne informacije, pooblastiti organe za ugotavljanje skladnosti za izvajanje svojih nalog, če izpolnjujejo dodatne zahteve iz sheme, in spremljati razvoj na področju certificiranja kibernetske varnosti**[...]. Nacionalni organi za [...] certificiranje **kibernetske varnosti** bi morali obravnavati pritožbe, ki jih vložijo fizične ali pravne osebe glede certifikatov, ki jih izdajo **sami, ali certifikatov, ki jih izdajo organi za ugotavljanje skladnosti in se nanašajo na visoko stopnjo zagotovila** [...], 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 [...] certificiranje **kibernetske varnosti** 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 **predstavniki** nacionalnih organov za [...] certificiranje **kibernetske varnosti ali drugih ustreznih nacionalnih organov**. 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 **Agencijo glede predlog za sheme in na** Komisijo glede ohranjanja in pregledovanja obstoječih evropskih certifikacijskih shem za kibernetsko varnost.

(60a) Skupina bi morala olajšati izmenjavo dobrih praks in strokovnega znanja med nacionalnimi organi za certificiranje kibernetske varnosti, pristojnimi za izdajanje certifikatov in odobritev organov za ugotavljanje skladnosti. Skupina bi morala v okviru priprave predloge za shemo in njenega izvajanja podpirati razvoj mehanizma medsebojnih strokovnih pregledov za organe, ki izdajajo evropske certifikate kibernetske varnosti za visoko stopnjo zagotovila. Pri teh strokovnih pregledih bi bilo zlasti treba oceniti, ali imajo zadevni organi ustrezno strokovno znanje in ali lahko usklajeno opravljajo svoje naloge. Rezultati medsebojnih strokovnih pregledov bi morali biti javno objavljeni. Ti organi lahko sprejmejo ustrezne ukrepe za prilagoditev svojih praks in strokovnega znanja.

(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.

(61a) Glede na globalni značaj dobavnih verig za IKT bi lahko Unija, da bi še bolj olajšala trgovino, v skladu s členom 218 PDEU sklepala sporazume o vzajemnem priznavanju glede certifikatov, izdanih v okviru shem, ki so bile ustanovljene na podlagi evropskega certifikacijskega okvira za kibernetsko varnost. Komisija lahko ob upoštevanju nasveta agencije ENISA in Evropske certifikacijske skupine za kibernetsko varnost priporoči začetek ustreznih pogajanj. Vsaka shema bi morala določati posebne pogoje za vzajemno priznavanje certifikacijskih shem s tretjimi državami.

(62) [...]

(63) [...]

(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 [...] certificiranje **kibernetske varnosti**.

(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

1. 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 [...] **Evropske unije** 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 **postopkov,** izdelkov in storitev IKT v Uniji. Ta okvir se uporablja brez poseganja v posebne določbe glede prostovoljnega ali obveznega certificiranja v drugih aktih Unije.

2. **Ta uredba ne posega 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 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 **poškodoval, prekinil ali drugače** 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 **ali ugotavljanje skladnosti postopkov,** izdelkov in storitev informacijske in komunikacijske tehnologije (IKT), ki spadajo na področje uporabe določene sheme;

(9a) „nacionalna certifikacijska shema za kibernetsko varnost“ pomeni celovit sklop pravil, tehničnih zahtev, standardov in postopkov, ki so jih oblikovali in sprejeli nacionalni javni organi in se uporabljajo za certificiranje ali ugotavljanje skladnosti postopkov, izdelkov in storitev IKT, ki spadajo na področje uporabe določene sheme;

(10) „evropski certifikat kibernetske varnosti“ pomeni dokument, ki [...] potrjuje, da je bil zadevni **postopek,** izdelek ali storitev IKT [...] **ocenjen glede skladnosti s** posebnimi **varnostnimi** zahtevami, določenimi v evropski certifikacijski shemi za kibernetsko varnost;

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

(11a) „storitev IKT“ pomeni vsako storitev, ki v celoti ali pretežno sestoji iz prenosa, shranjevanja, priklica ali obdelave informacij prek omrežij in informacijskih sistemov;

(11b) „postopek IKT“ pomeni vrsto dejavnosti, ki se izvajajo za zasnovo, razvoj, dobavo in vzdrževanje izdelka ali storitve IKT;

(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**;**

(16a) „tehnična specifikacija“ pomeni dokument, ki določa tehnične zahteve, ki jih mora izpolnjevati postopek, izdelek ali storitev IKT;

(16b) „stopnja zagotovila“ pomeni podlago za zaupanje, da postopek, izdelek ali storitev IKT izpolnjuje varnostne zahteve določene evropske certifikacijske sheme za kibernetsko varnost, navaja pa tudi raven, na kateri je bila ta ocenjena; s stopnjo zagotovila se ne meri varnost samega postopka, izdelka ali storitve IKT.

NASLOV II

ENISA – „*[...]Agencija Evropske unije za kibernetsko varnost*“

POGLAVJE I

MANDAT IN CILJI*[...]*

Člen 3

Mandat

1. Agencija opravlja naloge, ki so ji dodeljene s to uredbo, in tako prispeva k visoki ravni kibernetske varnosti v Uniji, **zlasti s podpiranjem prizadevanj držav članic ter institucij, agencij in organov Unije za izboljšanje kibernetske varnosti**. **Agencija deluje kot referenčna točka za svetovanje in strokovno znanje v zvezi s kibernetsko varnostjo za institucije, agencije in organe Unije.**

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.

2a. Agencija pri opravljanju svojih nalog deluje neodvisno in čim bolj upošteva strokovno znanje nacionalnih strokovnjakov iz ustreznih organov držav članic, pri čemer se je treba izogibati podvajanju dejavnosti.

3. [...]

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 **Unije**, ki se nanašajo na kibernetsko varnost**, vključno s sektorskimi politikami na področju kibernetske varnosti**.

3. Agencija podpira krepitev zmogljivosti in pripravljenost v celotni Uniji tako, da **institucijam, agencijam in organom** Unije, **pa tudi** državam članicam ter javnim in zasebnim deležnikom pomaga krepiti zaščito njihovih omrežij in informacijskih sistemov, razvijati **in izboljševati kibernetsko odpornost in odzivne zmogljivosti, ter razvijati** veščine, znanja in spretnosti na področju kibernetske varnosti [...].

4. Agencija pri vprašanjih, ki se nanašajo na kibernetsko varnost, spodbuja sodelovanje in usklajevanje na ravni Unije med državami članicami, institucijami, agencijami in organi Unije ter ustreznimi **javnimi in zasebnimi** deležniki [...].

5. Agencija **prispeva h krepitvi zmogljivosti** [...] na področju kibernetske varnosti na ravni Unije, da bi [...] **pomagala** državam članicam pri preprečevanju kibernetskih groženj in odzivanju nanje, zlasti v primeru čezmejnih incidentov.

6. Agencija spodbuja uporabo certificiranja, **da se prepreči razdrobljenosti certifikacijskih shem v EU. Agencija zlasti prispeva k** [...] vzpostavitvi in vzdrževanju 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.

POGLAVJE IA

NALOGE

Člen 5

*[...]**Oblikovanje in izvajanje 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 [...] varnostnih **incidentih**, 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

*[...]**Krepitev zmogljivosti***

1. Agencija pomaga:

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

(b) institucijam, [...] agencijam **in organom** Unije pri njihovih prizadevanjih za izboljšanje preprečevanja, odkrivanja in analiziranja [...] **groženj** in incidentov na področju kibernetske varnosti ter zmogljivosti odzivanja nanje **zlasti** 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** [...] njihovo izvajanje, 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 **rednih** [...] 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 deležniki;

(i) skupini za sodelovanje **pri** [...] izmenjavi 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 **podpira znotrajsektorsko in medsektorsko izmenjavo informacij** [...], 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

*[...]**Operativno sodelovanje na ravni Unije***

1. Agencija podpira operativno sodelovanje med [...] **državami članicami ter institucijami, agencijami in organi Unije ter** med deležniki.

2. Agencija na operativni ravni sodeluje in vzpostavi sinergije z institucijami, [...] agencijami **in organi** 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 **v tej funkciji** [...] olajšuje izmenjavo informacij in sodelovanje med njenimi člani.

4. Agencija **podpira** [...] operativno sodelovanje v mreži skupin CSIRT in **na njihovo zahtevo** zagotavlja podporo državam članicam s:

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

(b) **omogočanjem lažjega** [...] tehničnega **obvladovanja** incidentov [...], ki imajo pomembne ali znatne posledice**, med drugim zlasti s podpiranjem prostovoljne izmenjave tehničnih rešitev med državami članicami**;

(c) analiziranjem šibkih točk [...] in incidentov**;**

(ca) zagotavljanjem podpore pri naknadnih tehničnih preiskavah incidentov, ki imajo pomembne ali znatne posledice v skladu z Direktivo (EU) 2016/1148.

Agencija in skupina CERT-EU pri opravljanju teh nalog strukturirano sodelujeta, da bi izkoristili sinergije **in se izognili podvajanju dejavnosti** [...].

5. [...]

[...]

6. Agencija organizira **redne** [...]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. **Takšne vaje na ravni Unije lahko vključujejo tehnične, operativne in strateške elemente** [...]. **Enkrat na dve leti se organizira obsežna vaja, ki zajema vse navedene elemente.** Poleg tega Agencija prispeva k sektorskim vajam na področju kibernetske varnosti in jih po potrebi pomaga organizirati skupaj z ustreznimi [...] **organizacijami, ki lahko** sodelujejo pri vajah na področju kibernetske varnosti tudi na ravni Unije.

7. Agencija **ob tesnem sodelovanju z državami članicami** 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 [...] ali enotne kontaktne točke iz direktive o varnosti omrežij **(v obeh primerih na prostovoljni podlagi**[...]); 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, **ki so bila prostovoljno dana v skupno rabo,** 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) [...] **olajševanjem, na zahtevo držav članic,** tehničnega obravnavanja incidenta ali krize, [...] **med drugim zlasti s podpiranjem prostovoljne** izmenjave tehničnih rešitev med državami članicami;

(d) podpiranjem **institucij, agencij in organov EU, na zahtevo pa tudi držav članic,** pri komuniciranju z javnostjo glede incidenta ali krize;

(e) **podpiranjem držav članic na podlagi njihove zahteve pri testiranju** [...] načrtov za sodelovanje pri odzivanju na take incidente ali krize.

Člen 8

*[...]**Trg, certificiranje kibernetske varnosti in standardizacija***

Agencija:

(a) podpira in spodbuja oblikovanje in izvajanje politike Unije o certificiranju **postopkov,** 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 **postopke,** izdelke in storitve IKT v **sodelovanju s sektorjem in 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 [...] certificiranje **kibernetske varnosti** in predstavniki sektorja;

(3a) dajanjem priporočil v skladu s členom 47(1)(b) glede ustreznih tehničnih specifikacij, namenjenih razvoju evropske certifikacijske sheme za kibernetsko varnost, če standardi niso na voljo;

(3b) podpiranjem prizadevanj za zadostni razvoj zmogljivosti v zvezi s postopki ocenjevanja in certificiranja, tako da pripravi in objavi smernice, ter s podpiranjem držav članicam na njihovo zahtevo;

(b) omogoča lažjo vzpostavitev in uvedbo evropskih in mednarodnih standardov za obvladovanje tveganja in za varnost **postopkov,** izdelkov [...] in storitev IKT;

(ba) 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

*[...]**Znanje*** **in** ***informacije***[...]

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 kibernetskih [...] **incidentov**;

(c) v sodelovanju s strokovnjaki iz organov držav članic zagotavlja nasvete, smernice in najboljše prakse za varnost omrežij in informacijskih sistemov, zlasti za varnost [...] infrastruktur, ki podpirajo sektorje iz Priloge II k Direktivi (EU) 2016/1148**, in infrastruktur, ki jih uporabljajo ponudniki digitalnih storitev iz Priloge III k navedeni direktivi**;

(d) združuje, organizira in prek namenskega portala da javnosti na voljo informacije o kibernetski varnosti, ki jih sporočijo institucije, agencije in organi Unije, **ter informacije, ki jih prostovoljno sporočijo države članice ter zasebni in javni deležniki**;

(e) [...]

(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) [...].

Člen 9a

Ozaveščanje in izobraževanje

Agencija:

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

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

(c) državam članicam pomaga pri prizadevanjih za krepitev ozaveščenosti o kibernetski varnosti in spodbujanju izobraževanja o kibernetski varnosti;

(d) podpira tesnejše usklajevanje in izmenjavo najboljših praks med državami članicami na področju izobraževanja in ozaveščanja o kibernetski varnosti, s tem ko omogoča lažje vzpostavljanje in vzdrževanje mreže nacionalnih kontaktnih točk za izobraževanje.

Člen 10

*[...]**Raziskave in inovacije***

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

*[...]**Mednarodno sodelovanje***

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 [...] izmenjave najboljših praks **znotraj ustreznih mednarodnih okvirov sodelovanja**, [...].

(c) zagotavljanjem, na zahtevo Komisije, strokovnega znanja**;**

(ca) v sodelovanju z Evropsko certifikacijsko skupino za kibernetsko varnost, ustanovljeno na podlagi člena 53, svetovanjem in pomočjo Komisiji pri zadevah, povezanih s sporazumi o vzajemnem priznavanju certifikatov kibernetske varnosti s tretjimi državami.

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;[...]

(d) stalna skupina deležnikov, ki izvaja naloge iz člena 20**;**

(da) mreža nacionalnih uradnikov za zvezo, ki izvaja naloge iz člena 20a.

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;

(ca) nadzira izvajanje večletnega in letnega programa dejavnosti iz enotnega programskega dokumenta;

(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 deležnikov 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. [...]

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**, vključno z izvajanjem letnega delovnega programa,** 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 deležniki;

(la) redno izmenjavo z institucijami, agencijami in organi Unije v zvezi z njihovimi dejavnostmi na področju kibernetske varnosti, da se zagotovili skladnost pri razvoju in izvajanju politike EU;

(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 **se za učinkovito in uspešno opravljanje nalog Agencije ter na podlagi ustrezne analize stroškov in koristi po potrebi lahko** odloči, [...] **da se vzpostavi en ali več lokalnih uradov v eni ali več državah članicah**. Izvršni direktor pred odločitvijo o ustanovitvi lokalnega urada **zaprosi za mnenje zadevne države članice, vključno z državo članico, v kateri je sedež agencije, ter** pridobi predhodno soglasje Komisije **in** upravnega odbora[...]. **V primeru nesoglasja v posvetovalnem postopku med izvršnim direktorjem in zadevnimi državami članicami o zadevi razpravlja Svet.** 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.[...] **Število zaposlenih v vseh lokalnih uradih mora biti čim manjše in skupaj ne presega 40 % [...] osebja v državi članici, v kateri je sedež Agencije. Število zaposlenih v posameznem lokalnem uradu ne sme presegati 10 % [...] števila [...] zaposlenih v državi članici, v kateri je sedež Agencije.**

ČLEN 4
STALNA SKUPINA DELEŽNIKOV

Člen 20

Stalna skupina deležnikov

1. Na predlog izvršnega direktorja upravni odbor ustanovi stalno skupino deležnikov, ki jo sestavljajo priznani strokovnjaki, ki zastopajo ustrezne deležnike, kot so podjetja iz sektorja IKT, ponudniki elektronskih komunikacijskih omrežij ali storitev, dostopnih javnosti, **izvajalci bistvenih storitev,** 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 deležnikov, 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 deležnikov predseduje izvršni direktor ali katera koli oseba, ki jo izvršni direktor imenuje za vsak primer posebej.

4. Mandat članov stalne skupine deležnikov traja dve leti in pol. Člani upravnega odbora ne smejo biti člani stalne skupine deležnikov. Strokovnjaki iz Komisije in držav članic imajo pravico biti prisotni na sejah stalne skupine deležnikov in sodelovati pri njenem delu. Na seje in k sodelovanju pri delu skupine so lahko povabljeni predstavniki drugih organov, ki niso člani stalne skupine deležnikov, za katere izvršni direktor meni, da so relevantni.

5. Stalna skupina deležnikov Agenciji svetuje glede opravljanja dejavnosti. Zlasti svetuje izvršnemu direktorju pri pripravi predloga delovnega programa Agencije in komuniciranju z ustreznimi deležniki o zadevah, ki se nanašajo na delovni program.

5a. Stalna skupina deležnikov o svojih dejavnostih redno obvešča upravni odbor.

ODDELEK 4A
MREŽA NACIONALNIH URADNIKOV ZA ZVEZO

Člen 20a

Mreža nacionalnih uradnikov za zvezo

1. Upravni odbor na predlog izvršnega direktorja ustanovi mrežo nacionalnih uradnikov za zvezo, ki jo sestavljajo predstavniki držav članic.

2. Mrežo nacionalnih uradnikov za zvezo sestavljajo predstavniki vseh držav članic. Vsaka država članica imenuje enega predstavnika. Sestanki mreže lahko potekajo v različnih sestavah strokovnjakov.

3. Mreža nacionalnih uradnikov za zvezo predvsem omogoča lažjo izmenjavo informacij med agencijo ENISA in državami članicami. Zlasti podpira agencijo ENISA pri razširjanju njenih dejavnosti, ugotovitev in priporočil po vsej EU ali zadevnim deležnikom.

4. Nacionalni uradniki za zvezo delujejo kot kontaktne točke na nacionalni ravni, da se olajša sodelovanje med agencijo ENISA in nacionalnimi strokovnjaki v okviru izvajanja delovnega programa agencije ENISA.

5. Medtem ko bi morali nacionalni uradniki za zvezo tesno sodelovati s predstavniki svojih držav v upravnem odboru, pa mreža sama ne podvaja dela upravnega odbora ali drugih forumov EU.

6. Funkcije in postopki za mrežo nacionalnih uradnikov za zvezo se določijo v statutu Agencije in objavijo.

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[14], pri čemer upošteva smernice Komisije.

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.

[14] 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).

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 vsi deležniki 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 deležniki 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 deležnikov, 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[15] in 2015/444[16]. Navedena pravila vključujejo določbe o izmenjavi, obdelavi in hrambi tajnih podatkov.

---

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

[16] 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).

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.

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 (ES) št. 883/2013 Evropskega parlamenta in Sveta[17] 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.

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

3. OLAF lahko izvaja preiskave, vključno s pregledi in inšpekcijami na kraju samem, v skladu z določbami in postopki iz Uredbe 883/2013 Evropskega parlamenta in Sveta ter Uredbe Sveta (Euratom, ES) št. 2185/96[18] 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.

[18] 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).

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.

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 **štiri** [...] leta. 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 **štiri** [...] leta.

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 je lahko odstavljen samo z odločitvijo upravnega odbora[...].

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 kadrovski predpisi in 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[...].

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[19]. 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[20].

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.

---

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

[20] 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).

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 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 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 [...]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

Evropski certifikacijski* okvir *za kibernetsko varnost[…]

1. **Za izboljšanje pogojev za delovanje notranjega trga z zvišanjem ravni kibernetske varnosti v Uniji se vzpostavi evropski certifikacijski okvir za kibernetsko varnost. Določa upravljanje, ki omogoča usklajen pristop na ravni EU glede evropskih certifikacijskih shem za kibernetsko varnost, da bi se oblikoval enotni digitalni trg za postopke, izdelke in storitve IKT.**

2. **Evropski certifikacijski okvir za kibernetsko varnost opredeljuje mehanizem za vzpostavitev** [...]evropskih certifikacijskih shem za kibernetsko varnost [...] **in za** potrjevanje, da **postopki,** izdelki in storitve IKT, ki so bili [...]**ocenjeni** v skladu s takimi shemami, izpolnjujejo določene **varnostne** zahteve[...]**, da se zaščitijo** razpoložljivost, avtentičnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali funkcij ali storitev, ki jih ponujajo ali so dostopni prek teh izdelkov, postopkov **in** storitev [...]**v celotnem življenjskem ciklu**.

Člen 44

Priprava in sprejetje evropske certifikacijske sheme za kibernetsko varnost

1. Agencija ENISA na zahtevo Komisije **ali Evropske skupine za kibernetsko varnost (v nadaljnjem besedilu: skupina), ustanovljene v skladu s členom 53,** pripravi predlogo za evropsko certifikacijsko shemo za kibernetsko varnost, ki izpolnjuje zahteve iz členov 45, 46 in 47 te uredbe.[...]

1a. Pripravo predloge za evropsko certifikacijsko shemo za kibernetsko varnost lahko skupini predlagajo države članice ali zainteresirane organizacije deležnikov. Skupina take predloge oceni glede na merila, ki jih opredeli na podlagi smernic v skladu s členom 53(3)(ca), za pripravo predloge za evropsko certifikacijsko shemo za kibernetsko varnost pa lahko zaprosi agencijo ENISA.

2. Pri pripravi predlog za sheme iz odstavka 1 tega člena se agencija ENISA **na podlagi preglednih posvetovalnih postopkov** posvetuje z vsemi ustreznimi deležniki in tesno sodeluje s skupino. Skupina agenciji ENISA zagotavlja pomoč in strokovno svetovanje [...]pri pripravi predloge za shemo **ter o njej sprejme mnenje, preden jo predloži Komisiji**[...]. **Agencija ENISA zagotovi, da so predloge za sheme skladne z veljavnim harmoniziranim standardom, ki se uporablja za akreditacijo organa za ugotavljanje skladnosti.**

3. Agencija ENISA **v največji možni meri upošteva mnenje skupine, preden** predlogo za[...] shemo[...], 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 **postopke,** izdelke in storitve IKT, ki izpolnjujejo zahteve iz členov 45, 46 in 47 te uredbe.

5. [...]

Člen 44a

Vzdrževanje evropske certifikacijske sheme za kibernetsko varnost

1. Agencija vzdržuje posebno spletišče, namenjeno obveščanju javnosti o evropskih certifikacijskih shemah za kibernetsko varnost, certifikatih in izjavah EU o skladnosti, izdanih na podlagi člena 47a.

2. Agencija v tesnem sodelovanju s skupino najmanj vsakih pet let pregleda sprejeto evropsko certifikacijsko shemo za kibernetsko varnost ob upoštevanju povratnih informacij, ki jih prejme od deležnikov. Komisija ali skupina lahko, če menita, da je to potrebno, zaprosita Agencijo, da začne postopek oblikovanja revidirane predloge za shemo v skladu s členom 44(2) in (3).

Člen 45

Varnostni cilji evropskih certifikacijskih shem za kibernetsko varnost

Evropska certifikacijska shema za kibernetsko varnost je oblikovana tako, da **se** ustrezno [...]**dosežejo najmanj** naslednji varnostni cilji:

(a) zaščititi shranjene, prenesene ali kako drugače obdelane podatke pred naključno ali nepooblaščeno hrambo, obdelavo, dostopom ali razkritjem **med celotnim življenjskim ciklom postopka, izdelka ali storitve**;

(b)

zaščititi shranjene, prenesene ali kako drugače obdelane podatke pred naključnim ali nepooblaščenim uničenjem, [...]izgubo ali spremembo **ali slabo razpoložljivostjo med celotnim življenjskim ciklom postopka, izdelka ali storitve**;

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

(d) beležiti, [...]do katerih podatkov, storitev ali funkcij **se je dostopalo ali kateri podatki, storitve ali funkcije so se uporabljali oziroma kako drugače obdelovali ter** kdaj in kdo **je do njih dostopal oz. jih je uporabljal ali obdeloval**;

(e) [...]mogoče je preveriti, do katerih podatkov, storitev ali funkcij se je dostopalo ali kateri podatki, storitve ali funkcije so se uporabljali **oziroma kako drugače obdelovali** ter kdaj in kdo je do njih dostopal oz. jih je uporabljal **ali obdeloval**;

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

(g) [...]**postopki,** izdelki in storitve IKT so opremljeni s posodobljeno programsko **in strojno** opremo, ki ne vsebuje [...]**javno** znanih šibkih točk, in na voljo so mehanizmi, ki zagotavljajo varno posodabljanje[...]**;**

(ga) postopki, izdelki in storitve IKT so razviti, proizvedeni in dobavljeni v skladu z varnostnimi zahtevami iz določene sheme.

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 **postopke,** izdelke in storitve IKT[...]. **Stopnja zagotovila je sorazmerna s stopnjo tveganja, povezano s predvideno uporabo postopka, izdelka ali storitve IKT.**

2. Osnovna, znatna in visoka stopnja zagotovila [...]**se nanaša na certifikat ali izjavo EU o skladnosti, izdano v evropski certifikacijski shemi za kibernetsko varnost, ki za vsako stopnjo zagotovila določa ustrezne varnostne zahteve, vključno z varnostnimi funkcionalnostmi, in ustrezno stopnjo prizadevanj za oceno postopka, izdelka ali storitve IKT. Certifikat ali izjava EU o skladnosti je s sklici na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je zmanjšati tveganje kibernetskih incidentov ali jih preprečiti, opredeljena na naslednji način:**

(a) **evropski certifikat kibernetske varnosti ali izjava EU o skladnosti, ki se nanaša na** osnovno stopnjo zagotovila**, zagotavlja, da postopki, izdelki in storitve IKT izpolnjujejo ustrezne varnostne zahteve, vključno z varnostnimi funkcionalnostmi, in da so bili ocenjeni do stopnje, na kateri so kar najbolj zmanjšana znana osnovna tveganja za kibernetske incidente in kibernetske napade. Ocenjevanje vključuje vsaj pregled tehnične dokumentacije, če to ni mogoče, pa nadomestne dejavnosti z enakovrednim učinkom**[...];

(b) **evropski certifikat kibernetske varnosti, ki se nanaša na** znatno stopnjo zagotovila, zagotavlja**, da postopki, izdelki in storitve IKT izpolnjujejo ustrezne varnostne zahteve, vključno z varnostnimi funkcionalnostmi, in da so bili ocenjeni do stopnje, na kateri so kar najbolj zmanjšana znana kibernetska tveganja ter tveganja kibernetskih incidentov in kibernetskih napadov, ki jih izvajajo akterji z omejenim znanjem in viri. Ocenjevanje vključuje najmanj: preverjanje, da se splošno znane šibke točke ne pojavljajo, in testiranje, da se pri postopkih, izdelkih ali storitvah IKT pravilno uporabljajo potrebne varnostne funkcionalnosti; če to ni mogoče, pa vključuje nadomestne dejavnosti z enakovrednim učinkom**[...]**;**

(c) **evropski certifikat kibernetske varnosti, ki se nanaša na** visoko stopnjo zagotovila [...], zagotavlja**, da postopki, izdelki in storitve IKT izpolnjujejo ustrezne varnostne zahteve, vključno z varnostnimi funkcionalnostmi, in da so bili ocenjeni do stopnje, na kateri je kar najbolj zmanjšano tveganje naprednih kibernetskih napadov, ki jih izvajajo akterji z obsežnim znanjem in viri. Ocenjevanje vključuje najmanj: preverjanje, da se splošno znane šibke točke ne pojavljajo, ter testiranje, da se pri postopkih, izdelkih ali storitvah IKT pravilno uporabljajo potrebne najsodobnejše varnostne funkcionalnosti, in ocenjevanje njihove odpornosti proti izurjenim napadalcem s penetracijskim testiranjem; če to ni mogoče, pa vključuje nadomestne dejavnosti z enakovrednim učinkom**[...].

2a. V evropski certifikacijski shemi za kibernetsko varnost se lahko določi več stopenj ocenjevanja, odvisno od strogosti in obsega metodologije za ocenjevanje. Vsaka od stopenj ocenjevanja ustreza eni od stopenj zagotovila in je opredeljena z ustrezno kombinacijo elementov, ki sestavljajo zagotovilo.

Člen 47

Elementi evropskih certifikacijskih shem za kibernetsko varnost

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

(a) predmet urejanja in področje uporabe certifikacijske **sheme**, vključno z vrsto ali kategorijami zajetih **postopkov,** izdelkov in storitev IKT **ter utemeljitvijo, kako certifikacijska shema izpolnjuje potrebe pričakovanih ciljnih skupin**;

(b) [...]sklic na [...]mednarodne**, evropske ali nacionalne** standarde**, upoštevane pri ocenjevanju. Če standardi niso na voljo, se navede sklic na** [...]tehnične specifikacije**, ki izpolnjujejo zahteve iz Priloge II k Uredbi 1025/2012, ali, če te niso na voljo, sklic na tehnične specifikacije ali druge zahteve glede kibernetske varnosti, opredeljene v shemi**;

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

(ca) kadar je ustrezno, posebne ali dodatne zahteve, ki se uporabljajo za organe za ugotavljanje skladnosti, da se zagotovi njihova tehnična usposobljenost za ocenjevanje zahtev glede kibernetske varnosti;

(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) **kadar je ustrezno,** informacije, ki jih vložnik predloži **ali kako drugače da na voljo** 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) [...]pravila za spremljanje skladnosti z zahtevami certifikatov **ali izjave EU o skladnosti**, vključno z mehanizmi za dokazovanje stalnega izpolnjevanja določenih zahtev glede kibernetske varnosti;

(h) **kadar je ustrezno,** pogoje za izdajo **in obnovitev certifikata ter za** ohranitev, nadaljevanje, razširitev **ali** zmanjšanje področja uporabe certificiranja;

(i) pravila glede posledic neskladnosti certificiranih **ali samoocenjenih** izdelkov in storitev IKT z [...]zahtevami **sheme**;

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

(k) **kadar je ustrezno,** pravila glede hrambe evidenc s strani organov za ugotavljanje skladnosti;

(l) opredelitev nacionalnih **ali mednarodnih** certifikacijskih shem za kibernetsko varnost, ki zadeva isto vrsto ali kategorije **postopkov,** izdelkov in storitev IKT**, varnostnih zahtev ter meril in metod za ocenjevanje**;

(m) vsebino izdanega certifikata **ali izjave EU o skladnosti**;

(ma) obdobje hranjenja izjave EU o skladnosti in tehnične dokumentacije z vsemi ustreznimi informacijami pri proizvajalcu ali ponudniku izdelkov in storitev IKT;

(mb[...]) najdaljši rok veljavnosti certifikata;

(mc[...]) politiko razkritja za podeljene, spremenjene in odvzete certifikate;

(md[...]) pogoje za vzajemno priznavanje certifikacijskih shem s tretjimi državami;

(me[...]) kadar je ustrezno, pravila glede mehanizma medsebojnih strokovnih pregledov za organe, ki izdajajo evropske certifikate kibernetske varnosti, za visoko stopnjo zagotovila v skladu s členom 48(4a).

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 **ali izjava EU o skladnosti** 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 47a

Samoocenjevanje skladnosti

1. V okviru evropske certifikacijske sheme za kibernetsko varnost se lahko dopusti ugotavljanje skladnosti, za katero je v celoti odgovoren proizvajalec ali ponudnik izdelkov in storitev IKT. Tako ugotavljanje skladnosti se uporablja samo za izdelke in storitve IKT z nizkim tveganjem, ki ustreza osnovni stopnji zagotovila.

2. Proizvajalec ali ponudnik izdelkov in storitev IKT lahko izda izjavo EU o skladnosti, v kateri je navedeno, da je dokazano izpolnjevanje zahtev iz sheme. Z izdajo take izjave proizvajalec ali ponudnik izdelkov in storitev IKT prevzame odgovornost za skladnost izdelka ali storitve IKT z zahtevami iz sheme.

3. Proizvajalec ali ponudnik izdelkov in storitev IKT za obdobje, opredeljeno v ustrezni evropski certifikacijski shemi za kibernetsko varnost, hrani izjavo EU o skladnosti in tehnično dokumentacijo z vsemi ustreznimi informacijami, ki se nanašajo na skladnost izdelkov ali storitev IKT s shemo, tako da je na voljo nacionalnemu organu za certificiranje kibernetske varnosti iz člena 50(1). Kopija izjave EU o skladnosti se predloži nacionalnemu organu za nadzor nad certificiranjem kibernetske varnosti in agenciji ENISA.

4. Izdajanje izjav EU o skladnosti je prostovoljno, razen če je v pravu Unije ali držav članic določeno drugače.

5. Izjava EU o skladnosti, izdana na podlagi tega člena, se prizna v vseh državah članicah.

Člen 48

Certificiranje kibernetske varnosti

1. Za **postopke,** 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 **ali držav članic** določeno drugače.

3. Evropski certifikat kibernetske varnosti na podlagi tega člena**, ki se nanaša na osnovno ali znatno stopnjo zagotovila,** 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 **certifikacijska** shema za kibernetsko varnost določa, da lahko evropski certifikat kibernetske varnosti, ki izhaja iz te sheme, izda le javni organ. Tak [...]organ je eden od naslednjih:

(a) nacionalni organ za [...]certificiranje **kibernetske varnosti** iz člena 50(1);

(b) **javni** organ, ki je akreditiran kot organ za ugotavljanje skladnosti v skladu s členom 51(1)[...]

(c) [...].

4a. V primerih, ko se v okviru evropske certifikacijske sheme za kibernetsko varnost na podlagi člena 44 zahteva visoka stopnja zagotovila, lahko certifikat izda samo nacionalni organ za certificiranje kibernetske varnosti iz člena 50(1), pod naslednjimi pogoji pa tudi organ za ugotavljanje skladnosti iz člena 51:

(a) po predhodni odobritvi s strani nacionalnega organa za certificiranje kibernetske varnosti za vsak posamezen certifikat, ki ga izda organ za ugotavljanje skladnosti, ali

(b) po splošnem prenosu te naloge na organ za ugotavljanje skladnosti s strani nacionalnega organa za certificiranje kibernetske varnosti.

5. Fizična ali pravna oseba, ki predloži svoje **postopke,** izdelke ali storitve IKT certifikacijskemu mehanizmu, **da** organu za ugotavljanje skladnosti iz člena 51 **ali nacionalnemu organu za certificiranje kibernetske varnosti iz člena 50**, **<u>če je to organ, ki je izdal certifikat,</u> na voljo** [...]vse informacije, ki so potrebne za izvedbo certifikacijskega postopka.

5a. Imetnik certifikata obvesti organ, ki je izdal certifikat, o vseh pozneje odkritih šibkih točkah ali nepravilnostih v zvezi z varnostjo certificiranih postopkov, izdelkov ali storitev IKT, ki bi lahko vplivale na zahteve, povezane s certifikacijo. Zadevni organ te informacije brez nepotrebnega odlašanja posreduje nacionalnemu organu za certificiranje kibernetske varnosti.

6. Certifikat se izda za [...]**obdobje, opredeljeno v določeni certifikacijski shemi,** in se lahko [...]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 **postopke,** 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). **N**acionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za **postopke,** 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 **postopke,** izdelke in storitve IKT, ki jih zajema veljavna evropska certifikacijska shema za kibernetsko varnost.

3. Obstoječi certifikati, ki so bili izdani na podlagi nacionalnih certifikacijskih shem za kibernetsko varnost **in jih zajema evropska certifikacijska shema za kibernetsko varnost**, ostanejo veljavni do datuma izteka veljavnosti.

Člen 50

***Nacionalni [...]organi za certificiranje* kibernetske varnosti**

1. Vsaka država članica **na svojem ozemlju imenuje enega ali več** nacionalnih[...] organov za certificiranje **kibernetske varnosti ali pa – po medsebojnem dogovoru z drugo državo članico – imenuje enega ali več organov s sedežem v tej drugi državi članici, ki so odgovorni za nadzorne naloge v državi članici, ki organe imenuje.**

2. Vsaka država članica obvesti Komisijo o identiteti **imenovanih [...]organov in o nalogah, ki so mu dodeljene.**

3. Vsak nacionalni [...]organ za certificiranje **kibernetske varnosti** je **brez poseganja v člen 48(4)(a) in člen 48(4a)** glede svoje organizacije, odločitev o financiranju, pravne strukture in sprejemanja odločitev neodvisen od subjektov, ki jih nadzoruje.

3a. Države članice zagotovijo, da se pri dejavnostih nacionalnega organa za certificiranje kibernetske varnosti, ki se nanašajo na izdajanje certifikatov v skladu s členom 48(4)(a) in členom 48(4a), spoštuje stroga delitev vlog in pristojnosti v razmerju do nadzornih dejavnosti ter da se oba sklopa dejavnosti izvajata neodvisno drug od drugega.

4. Države članice zagotovijo, da imajo nacionalni [...]organi za certificiranje **kibernetske varnosti** 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 certificiranje **kibernetske varnosti**:

(a) [...]

(aa) spremljajo in izvršujejo obveznosti proizvajalca ali ponudnika izdelkov in storitev IKT s sedežem na njihovem ozemlju, kot je določeno v členu 47a(2) in (3) in v ustrezni evropski certifikacijski shemi za kibernetsko varnost;

(b) [...]**brez poseganja v člen 51(1b) nacionalnim akreditacijskim organom pomagajo pri spremljanju in nadziranju** dejavnosti organov za ugotavljanje skladnosti za namene te uredbe[...];

(ba) spremljajo in nadzirajo dejavnosti organov iz člena 48(4);

(bb) pooblastijo organe za ugotavljanje skladnosti iz člena 51(1b) ter omejijo, začasno prekličejo ali odvzamejo obstoječo pooblastilo v primerih neizpolnjevanja zahtev iz te uredbe;

(c) obravnavajo pritožbe, ki jih vložijo fizične ali pravne osebe glede certifikatov, ki jih izda [...]**nacionalni organ za certificiranje kibernetske varnosti ali – v skladu s členom 48(4a) – organ za ugotavljanje skladnosti**, v ustreznem obsegu preučijo vsebino pritožbe ter pritožnika v razumnem roku obvestijo o napredku in izidih preiskave;

(d) sodelujejo z ostalimi nacionalnimi [...]organi za certificiranje **kibernetske varnosti** ali drugimi javnimi organi, med drugim tudi z izmenjavo informacij o morebitni neskladnosti **postopkov,** 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 certificiranje **kibernetske varnosti** ima vsaj naslednja pooblastila:

(a) od organov za ugotavljanje skladnosti**,** [...]imetnikov evropskega certifikata kibernetske varnosti **in izdajateljev izjave EU o skladnosti** lahko zahteva vse informacije, ki jih potrebuje za opravljanje svojih nalog;

(b) v obliki revizij izvaja preiskave organov za ugotavljanje skladnosti**,** [...]imetnikov evropskega certifikata kibernetske varnosti **in izdajateljev izjave EU o skladnosti**, da preveri skladnost z določbami iz naslova III;

(c) v skladu z nacionalnim pravom sprejme ustrezne ukrepe, da zagotovi, da organi za ugotavljanje skladnosti, [...]imetniki certifikata **in izdajatelji izjave EU o skladnosti** 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 jih izda nacionalni organ za certificiranje kibernetske varnosti ali – v skladu s členom 48(4a) – organ za ugotavljanje skladnosti in** 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 [...]certificiranje **kibernetske varnosti** 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 **postopkov,** 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.

1a. V primerih, ko evropski certifikat kibernetske varnosti izda nacionalni organ za certificiranje kibernetske varnosti na podlagi člena 48(4)(a) in člena 48(4a), se certifikacijski organ nacionalnega organa za certificiranje kibernetske varnosti akreditira kot organ za ugotavljanje skladnosti na podlagi odstavka 1 tega člena.

1b. Kadar je ustrezno, nacionalni organ za certificiranje kibernetske varnosti za izvajanje svojih nalog pooblasti organe za ugotavljanje skladnosti, če izpolnjujejo posebne ali dodatne zahteve iz evropske certifikacijske sheme na podlagi člena 47(1)(ca).

2. Akreditacija se izda za največ pet let in se lahko pod enakimi pogoji podaljša, če organ za ugotavljanje skladnosti izpolnjuje zahteve, določene v tem členu. Akreditacijski organi **sprejmejo vse ustrezne ukrepe, da v razumnem roku omejijo, začasno prekličejo ali** 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 [...]certificiranje **kibernetske varnosti** za vsako evropsko certifikacijsko shemo za kibernetsko varnost, sprejeto na podlagi člena 44, Komisiji priglasijo organe za ugotavljanje skladnosti, akreditirane **in po potrebi pooblaščene na podlagi člena 51(1b)** 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 [...]certificiranje **kibernetske varnosti** lahko Komisiji predloži zahtevek za črtanje organa za ugotavljanje skladnosti, ki ga je priglasila zadevna država članica, 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 [...]certificiranje **kibernetske varnosti**.

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 predstavniki nacionalnih organov za [...]certificiranje **kibernetske varnosti ali predstavniki drugih ustreznih nacionalnih organov**. [...]**Vsak član skupine lahko zastopa največ eno dodatno državo članico.**

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;

(ba) sprejme mnenje o predlogi za shemo na podlagi člena 44 te uredbe;

(c) [...]od Agencije **zahteva**, naj pripravi predlogo za evropsko certifikacijsko shemo za kibernetsko varnost v skladu s členom 44 te uredbe;

(ca) oblikuje in sprejme smernice o merilih za oceno predlogov za pripravo predloge sheme, ki se predložijo [...]skupini na podlagi člena 44(1a);

(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 [...]certificiranje **kibernetske varnosti** na podlagi tega naslova s **krepitvijo zmogljivosti,** izmenjavo informacij, zlasti z določitvijo metod za učinkovito izmenjavo informacij o vseh vprašanjih v zvezi s certificiranjem kibernetske varnosti**;**

(fa) podpira izvajanje mehanizma medsebojnih strokovnih pregledov v skladu s pravili, določenimi v evropski certifikacijski shemi za kibernetsko varnost na podlagi člena 47(1)(md) te uredbe.

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

Člen 53a

***Pravica do vložitve pritožbe pri nacionalnem organu za [...]certificiranje* kibernetske varnosti**

1. Fizične ali pravne osebe imajo pravico, da vložijo pritožbo pri nacionalnem organu za certificiranje kibernetske varnosti v zvezi s certifikatom, ki ga je izdal ta isti organ ali – v skladu s členom 48(4a) – organi za ugotavljanje skladnosti.

2. Nacionalni organ za certificiranje kibernetske varnosti, pri katerem je vložena pritožba, obvesti pritožnika o stanju zadeve in odločitvi o pritožbi, vključno z možnostjo pravnega sredstva na podlagi člena 53b.

Člen 53b

Pravica do učinkovitega pravnega sredstva

1. Fizične ali pravne osebe imajo pravico do učinkovitega pravnega sredstva zoper pravno zavezujočo odločitev nacionalnega organa za certificiranje kibernetske varnosti v zvezi z njimi.

2. Fizične ali pravne osebe imajo pravico do učinkovitega pravnega sredstva, če nacionalni organ za certificiranje kibernetske varnosti pritožbe ne obravnava.

3. Za postopke zoper nacionalni organ za certificiranje kibernetske varnosti so pristojna sodišča države članice, v kateri ima organ sedež.

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**(4)(b)** 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.

1a. Ta uredba se uporablja od […], razen členov 50, 51, 52, 53a, 53b in 54, ki se uporabljajo od [24 mesecev 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*

PRILOGA

ZAHTEVE, KI JIH MORAJO IZPOLNJEVATI ORGANI ZA UGOTAVLJANJE SKLADNOSTI

Organi za ugotavljanje skladnosti, ki želijo biti akreditirani, izpolnjujejo naslednje zahteve:

1. Organ za ugotavljanje skladnosti se ustanovi v skladu z nacionalnim pravom in je pravna oseba.

2. Organ za ugotavljanje skladnosti je organ tretje strani, neodvisen od organizacije oz. izdelka ali storitve IKT, katerega skladnost ugotavlja.

3. Organ, ki je del poslovnega združenja ali strokovne zveze, ki zastopa podjetja, vključena v zasnovo, proizvodnjo, dobavo oz. opravljanje, sestavljanje, uporabo ali vzdrževanje izdelkov ali storitev IKT, katerih skladnost ugotavlja, se lahko šteje kot organ za ugotavljanje skladnosti, če je zagotovljena njegova neodvisnost in ni nasprotja interesov.

4. Organ za ugotavljanje skladnosti, njegovo najvišje vodstvo in osebje, odgovorno za izvajanje nalog ugotavljanja skladnosti, niso snovalci, proizvajalci, dobavitelji oz. ponudniki, monterji, kupci, lastniki, uporabniki ali vzdrževalci izdelkov ali storitev IKT, katerih skladnost ugotavljajo, niti pooblaščeni zastopniki katere koli od navedenih strani. To ne onemogoča uporabe izdelkov, za katere ugotavlja skladnost in ki so nujni za delovanje organa za ugotavljanje skladnosti, ali uporabe takšnih izdelkov za osebne namene.

5. Organ za ugotavljanje skladnosti, njegovo najvišje vodstvo in osebje, odgovorno za izvajanje nalog ugotavljanja skladnosti, ne sodelujejo neposredno pri snovanju, proizvodnji ali izdelavi, trženju, montaži, uporabi ali vzdrževanju teh izdelkov ali storitev IKT niti ne zastopajo strani, ki sodelujejo pri teh dejavnostih. Ne sodelujejo pri nobenih dejavnostih, ki bi lahko bile v nasprotju z njihovo neodvisno presojo ali integriteto v zvezi z dejavnostmi za ugotavljanje skladnosti, za katere so priglašeni. To velja zlasti za svetovalne storitve.

6. Organi za ugotavljanje skladnosti zagotovijo, da dejavnosti njihovih odvisnih družb ali podizvajalcev ne vplivajo na zaupnost, objektivnost ali nepristranskost njihovih dejavnosti za ugotavljanje skladnosti.

7. Organi za ugotavljanje skladnosti in njihovo osebje izvajajo dejavnosti za ugotavljanje skladnosti z največjo poklicno integriteto in potrebno tehnično usposobljenostjo na določenem področju brez kakršnih koli pritiskov in spodbud, tudi finančnih, ki bi lahko vplivali na njihovo presojo ali rezultate njihovih dejavnosti za ugotavljanje skladnosti, zlasti od oseb ali skupin oseb, za katere so rezultati navedenih dejavnosti pomembni.

8. Organ za ugotavljanje skladnosti je zmožen izvajati vse naloge ugotavljanja skladnosti, ki so mu dodeljene s to uredbo, ne glede na to, ali te naloge izvaja organ za ugotavljanje skladnosti sam ali se izvajajo v njegovem imenu in pod njegovo odgovornostjo.

9. Vedno ter za vsak postopek ugotavljanja skladnosti in vsako vrsto ali kategorijo ali podkategorijo izdelka ali storitve IKT ima organ za ugotavljanje skladnosti na razpolago:

(a) potrebno osebje s tehničnim znanjem ter zadostnimi in ustreznimi izkušnjami za izvajanje nalog ugotavljanja skladnosti;

(b) potrebne opise postopkov, v skladu s katerimi se izvaja ugotavljanje skladnosti, ki zagotavljajo preglednost in zmožnost reprodukcije navedenih postopkov. Izvaja ustrezne politike in postopke, na podlagi katerih se ločijo naloge, ki jih izvaja kot priglašeni organ, in druge dejavnosti;

(c) postopke za izvajanje dejavnosti, pri katerih je ustrezno upoštevana velikost podjetja, sektor, v katerem deluje, njegova struktura, stopnja zahtevnosti zadevne tehnologije izdelka ali storitve IKT in masovna ali serijska narava proizvodnega postopka.

10. Organ za ugotavljanje skladnosti ima potrebna sredstva za ustrezno izvajanje tehničnih in upravnih nalog, povezanih z dejavnostmi za ugotavljanje skladnosti, ter dostop do vse potrebne opreme in prostorov.

11. Osebje, odgovorno za izvajanje dejavnosti za ugotavljanje skladnosti, ima:

(a) dobro tehnično in poklicno usposobljenost, ki zajema vse dejavnosti za ugotavljanje skladnosti;

(b) zadovoljivo znanje o zahtevah glede ugotavljanj skladnosti, ki jih izvaja, in ustrezna pooblastila za izvedbo teh ugotavljanj skladnosti;

(c) primerno znanje in razumevanje veljavnih zahtev in standardov preskušanja;

(d) zmožnost, ki je potrebna za pripravo certifikatov, zapisov in poročil, ki dokazujejo, da so bila ugotavljanja skladnosti izvedena.

12. Zagotovi se nepristranskost organa za ugotavljanje skladnosti, njegovega najvišjega vodstva in osebja za ugotavljanje skladnosti.

13. Plačilo najvišjega vodstva in osebja organa za ugotavljanje skladnosti, ki ugotavlja skladnost, ni odvisno od števila opravljenih ugotavljanj skladnosti ali rezultatov navedenih ugotavljanj skladnosti.

14. Organ za ugotavljanje skladnosti sklene zavarovanje odgovornosti, razen če odgovornost prevzame država v skladu z nacionalnim pravom ali če je država članica sama neposredno odgovorna za ugotavljanje skladnosti.

15. Osebje organa za ugotavljanje skladnosti je zavezano k poklicni molčečnosti v zvezi z vsemi informacijami, pridobljenimi med izvajanjem nalog v skladu s to uredbo ali katero koli izvedbeno določbo nacionalne zakonodaje, razen pred pristojnimi organi držav članic, v katerih se izvajajo njegove dejavnosti.

16. Organi za ugotavljanje skladnosti izpolnjujejo zahteve **ustreznega** standarda**, harmoniziranega v skladu z Uredbo (ES) št. 765/2008 za akreditacijo organov za ugotavljanje skladnosti, ki izvajajo certificiranje postopkov, izdelkov ali storitev**[...].

17. Organi za ugotavljanje skladnosti zagotovijo, da preskuševalni laboratoriji, v katerih se izvaja ugotavljanje skladnosti, izpolnjujejo zahteve **ustreznega** standarda**, harmoniziranega v skladu z Uredbo (ES) št. 765/2008 za akreditacijo laboratorijev, ki izvajajo preskuse**[...].