# UREDBA (EU) 2019/881 EVROPSKEGA PARLAMENTA IN SVETA

## z dne 17. aprila 2019

## o Agenciji Evropske unije za kibernetsko varnost (ENISA) in o certificiranju informacijske in komunikacijske tehnologije na področju kibernetske varnosti ter razveljavitvi Uredbe (EU) št. 526/2013 (Akt 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 ([1]),

ob upoštevanju mnenja Odbora regij ([2]),

v skladu z rednim zakonodajnim postopkom ([3]),

ob upoštevanju naslednjega:

(1) Omrežja in informacijski sistemi ter elektronska komunikacijska omrežja in storitve imajo ključno vlogo v družbi ter so postali temelj gospodarske rasti. Informacijske in komunikacijske tehnologije (IKT) so osnova za kompleksne sisteme, ki podpirajo vsakodnevne 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 državljani, organizacijami in podjetji po vsej Uniji je vedno bolj razširjena uporaba omrežij in informacijskih sistemov. Digitalizacija in povezljivost postajata poglavitni značilnosti vse večjega števila proizvodov in storitev, s prihodom interneta stvari (IoT) pa naj bi se v naslednjem desetletju po vsej Uniji začelo uporabljati izredno veliko število 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 vodi do nezadostnih informacij za posamezne uporabnike, uporabnike v organizacijah in poslovne uporabnike o lastnostih proizvodov IKT, storitev IKT in postopkov IKT glede kibernetske varnosti, kar spodkopava zaupanje v digitalne rešitve. Omrežja in informacijski sistemi so zmožni podpreti vse vidike našega življenja in poganjajo gospodarsko rast Unije. So ključna podlaga za vzpostavitev enotnega digitalnega trga.

(3) Večja digitalizacija in povezljivost povečujeta 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 tovrstna tveganja za družbo, je treba sprejeti vse potrebne ukrepe, da bi izboljšali kibernetsko varnost v Uniji in tako omrežja in informacijske sisteme, komunikacijska omrežja ter digitalne proizvode, storitve in naprave, ki jih uporabljajo državljani, organizacije in podjetja – od malih in srednjih podjetij (MSP), kot so opredeljena v Priporočilu Komisije 2003/361/ES ([4]), do upravljavcev kritične infrastrukture –, bolje zaščitili pred kibernetskimi grožnjami.

([1]) UL C 227, 28.6.2018, str. 86.
([2]) UL C 176, 23.5.2018, str. 29.
([3]) Stališče Evropskega parlamenta z dne 12. marca 2019 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 9. aprila 2019.
([4]) Priporočilo Komisije z dne 6. maja 2003 o opredelitvi mikro, malih in srednjih podjetij (UL L 124, 20.5.2003, str. 36).

(4) Agencija Evropske unije za varnost omrežij in informacij (v nadaljnjem besedilu: agencija ENISA), ustanovljena z Uredbo (EU) št. 526/2013 Evropskega parlamenta in Sveta ([5]) z dajanjem ustreznih informacij na voljo javnosti pomaga pri razvoju industrije kibernetske varnosti v Uniji, zlasti MSP in zagonskih podjetij. Agencija ENISA bi si morala prizadevati za tesnejše sodelovanje z univerzami in raziskovalnimi ustanovami, da bi prispevala k zmanjšanju odvisnosti od proizvodov in storitev za kibernetsko varnost iz držav zunaj Unije ter okrepila dobavne verige znotraj Unije.

(5) Kibernetski napadi so vse pogostejši, povezana gospodarstvo in družba, ki sta bolj ranljiva za kibernetske grožnje in napade, pa potrebujeta boljšo obrambo. Čeprav so kibernetski napadi pogosto čezmejni, so pristojnosti in odzivi politike organov za kibernetsko varnost ter organov za preprečevanje za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj večinoma nacionalni. Veliki incidenti bi lahko povzročili motnje pri zagotavljanju bistvenih storitev po vsej Uniji. Zato so potrebni učinkoviti in usklajeni odzivi ter krizno upravljanje na ravni Unije, in sicer na podlagi namenskih politik in širših instrumentov za evropsko solidarnost in medsebojno pomoč. Poleg tega je za oblikovalce politike, industrijo 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.

(6) 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 cilji vključujejo nadaljnjo krepitev zmogljivosti in pripravljenosti držav članic in podjetij ter boljše sodelovanje, izmenjavo informacij in usklajevanje med državami članicami ter institucijami, organi, uradi in agencijami Unije. 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 primerih velikih čezmejnih incidentov in kriz, ob upoštevanju pomena ohranjanja in nadaljnjega izboljševanja nacionalnih zmogljivosti za odzivanje na kibernetske grožnje vseh razsežnosti.

(7) Potrebna so tudi dodatna prizadevanja za večjo ozaveščenost državljanov, organizacij in podjetij o vprašanjih kibernetske varnosti. Glede na to, da incidenti zmanjšujejo zaupanje v ponudnike digitalnih storitev in sam enotni digitalni trg, zlasti med potrošniki, bi bilo treba zaupanje poleg tega dodatno okrepiti s tem, da bi se na pregleden način nudile informacije o ravni varnosti proizvodov IKT, storitev IKT in postopkov IKT, ki poudarjajo, da tudi visoka raven certificiranja kibernetske varnosti ne more zagotoviti, da je proizvod IKT, storitev IKT ali postopek IKT povsem varen. Večje zaupanje je mogoče lažje doseči s certificiranjem na ravni Unije, ki bi zagotavljalo skupne zahteve in merila za ocenjevanje glede kibernetske varnosti za vse nacionalne trge in sektorje.

(8) Pri kibernetski varnosti ne gre zgolj za vprašanje, povezano s tehnologijo, ampak za vprašanje, kjer je prav toliko pomembno tudi ravnanje ljudi. Zato bi bilo treba odločno spodbujati „kibernetsko higieno“, in sicer preproste in rutinske ukrepe, ki zmanjšajo izpostavljenost državljanov, organizacij in podjetij tveganjem zaradi kibernetskih groženj, kadar jih ti redno izvajajo.

(9) Za krepitev struktur kibernetske varnosti Unije je pomembno ohranjati in razvijati zmogljivosti držav članic za celovito odzivanje na kibernetske grožnje, vključno s čezmejnimi incidenti.

(10) Podjetja in posamezni potrošniki bi morali imeti točne informacije glede ravni zanesljivosti, s katero so bili certificirani njihovi proizvodi IKT, storitve IKT in postopki IKT. Hkrati pa nista noben proizvod IKT ali storitev IKT v celoti kibernetsko varna in je treba osnovna pravila za kibernetsko higieno spodbujati in jih prednostno obravnavati. Glede na vse večjo dostopnost naprav interneta stvari bi lahko zasebni sektor sprejel vrsto prostovoljnih ukrepov, s katerimi bi okrepil zaupanje v varnost proizvodov IKT, storitev IKT in postopkov IKT.

(11) Sodobni proizvodi in sistemi IKT pogosto vključujejo eno ali več tehnologij in komponent tretjih strani, kot so moduli programske opreme, knjižnice ali vmesniki za aplikacijsko programiranje, ter se nanje opirajo. To opiranje oziroma „odvisnost“ bi lahko povzročilo dodatna tveganja za kibernetsko varnost, saj bi lahko šibke točke, odkrite v komponentah tretje strani, vplivale tudi na varnost proizvodov IKT, storitev IKT in postopkov IKT. Odkrivanje in dokumentiranje takšnih odvisnosti končnim uporabnikom proizvodov IKT, storitev IKT in postopkov IKT pogosto omogoči, da izboljšajo dejavnosti obvladovanja tveganj za kibernetsko varnost, s tem ko na primer izboljšajo postopke uporabniškega obvladovanja šibkih točk na področju kibernetske varnosti in odpravljanja njihovih posledic.

([5]) 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).

(12) Organizacije, proizvajalce ali ponudnike, ki sodelujejo pri zasnovi in razvoju proizvodov IKT, storitev IKT ali postopkov IKT, bi bilo treba spodbuditi, naj v čim zgodnejših fazah zasnove in razvoja izvedejo ukrepe, da bo varnost navedenih proizvodov, storitev in postopkov na najvišji možni ravni, in to na način, da bo predpostavljena možnost kibernetskih napadov, njihove posledice pa predvidljive in čim manjše (v nadaljnjem besedilu: vgrajena varnost). Varnost bi bilo treba zagotoviti v celotni življenjski dobi proizvoda IKT, storitve IKT ali postopka IKT, in sicer z zasnovnimi in razvojnimi postopki, ki se nenehno nadgrajujejo, da se zmanjša tveganje za škodo zaradi zlorab.

(13) Podjetja, organizacije in javni sektor bi morali proizvode IKT, storitve IKT ali postopke IKT, ki so jih zasnovali, konfigurirati tako, da bi zagotovili višjo raven varnosti, kar bi prvemu uporabniku moralo omogočiti, da bi imel privzeto konfiguracijo z najvarnejšimi možnimi nastavitvami (v nadaljnjem besedilu: privzeta varnost), in s tem zmanjšati breme uporabnikov, da morajo poskrbeti za ustrezno konfiguracijo proizvodov IKT, storitev IKT ali postopkov IKT. Pogoj za privzeto varnost ne bi smela biti obsežna konfiguracija oziroma privzeta varnost od uporabnikov ne bi smela zahtevati specifičnega tehničnega znanja ali neintuitivnega ravnanja, ki ni značilno za vsakdanjo uporabo; morala bi delovati preprosto in zanesljivo, kadar koli bi jo uporabljali. Če se na podlagi posameznega primera pri analizi tveganja in uporabnosti ugotovi, da takšna privzeta nastavitev ni izvedljiva, bi bilo treba uporabnike spodbuditi, da se odločijo za najbolj varno nastavitev.

(14) Z Uredbo (ES) št. 460/2004 Evropskega parlamenta in Sveta ([6]) je bila ustanovljena agencija ENISA z namenom prispevanja k ciljema, da se zagotovi visoka in učinkovita raven varnosti omrežij in informacij v Uniji ter razvije kultura varnosti omrežij in informacij v korist državljanov, potrošnikov, podjetij in javnih uprav. Z Uredbo (ES) št. 1007/2008 Evropskega parlamenta in Sveta ([7]) je bil mandat agencije ENISA podaljšan do marca 2012. Z Uredbo (EU) št. 580/2011 Evropskega parlamenta in Sveta ([8]) je bil mandat agencije ENISA podaljšan do 13. septembra 2013. Z Uredbo (EU) št. 526/2013 je bil mandat agencije ENISA podaljšan do 19. junija 2020.

(15) 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 zagotavljala smernice pri oblikovanju odziva Unije, kar zadeva politike, na kibernetske grožnje in tveganja. V prizadevanju za boljšo zaščito državljanov na spletu je Unija leta 2016 sprejela prvi pravni akt na področju kibernetske varnosti, in sicer v obliki Direktive (EU) 2016/1148 Evropskega parlamenta in Sveta ([9]). Direktiva (EU) 2016/1148 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, kot so energetika, promet, oskrba s pitno vodo in njena distribucija, bančništvo, infrastrukture finančnih trgov, zdravstvo, digitalna infrastruktura, in za ponudnike 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. K visoki ravni kibernetske varnosti na enotnem digitalnem trgu prispevajo tudi drugi pravni akti, kot so Uredba (EU) 2016/679 Evropskega parlamenta in Sveta ([10]) in direktivi 2002/58/ES ([11]) in (EU) 2018/1972 ([12]) Evropskega parlamenta in Sveta.

([6]) 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).

([7]) 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).

([8]) 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).

([9]) Direktiva (EU) 2016/1148 Evropskega parlamenta in Sveta z dne 6. julija 2016 o ukrepih za visoko skupno raven varnosti omrežij in informacijskih sistemov v Uniji (UL L 194, 19.7.2016, str. 1).

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

([11]) Direktiva 2002/58/ES evropskega parlamenta in Sveta z dne 12. julija 2002 o obdelavi osebnih podatkov in varstvu zasebnosti na področju elektronskih komunikacij (Direktiva o zasebnosti in elektronskih komunikacijah) (UL L 201, 31.7.2002, str. 37).

([12]) Direktiva (EU) 2018/1972 Evropskega parlamenta in Sveta z dne 11. decembra 2018 o Evropskem zakoniku o elektronskih komunikacijah (UL L 321, 17.12.2018, str. 36).

(16) Po sprejetju strategije Evropske unije za kibernetsko varnost leta 2013 in po zadnji reviziji mandata agencije ENISA se je splošni okvir politike znatno spremenil, saj so svetovne razmere postale bolj negotove in manj varne. Na podlagi tega in ob upoštevanju pozitivnega razvoja vloge agencije ENISA kot referenčne točke za svetovanje in strokovno znanje, kot ustanove, ki podpira sodelovanje in krepitev zmogljivosti, poleg tega pa tudi 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 korenito spremenjenih kibernetskih groženj in za katere, kot je bilo ugotovljeno med ocenjevanjem agencije ENISA, sedanji mandat ne zadostuje.

(17) Agencija ENISA, ustanovljena s to uredbo, bi morala nadomestiti agencijo ENISA, ki je bila ustanovljena z Uredbo (EU) št. 526/2013. Agencija ENISA bi morala izvajati naloge, ki so na njo prenesene s to uredbo in pravnimi akti Unije na področju kibernetske varnosti, med drugim zagotavljati svetovanje in strokovno znanje 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 ter institucijami, organi, uradi in agencijami Unije.

(18) V okviru Soglasnega sklepa (2004/97/ES, Euratom) predstavnikov držav članic, ki so se sestali na ravni voditeljev držav ali vlad ([13]), so se predstavniki držav članic odločili, da bo sedež agencije ENISA v grškem mestu, ki ga določi grška vlada. Država članica gostiteljica agencije ENISA, bi morala zagotoviti najboljše možne pogoje za nemoteno in učinkovito delovanje agencije ENISA. Za pravilno in učinkovito izvajanje njenih nalog, zaposlovanje in ohranitev osebja ter večjo učinkovitost dejavnosti mreženja je nujno, da je sedež agencije ENISA na ustrezni lokaciji, kjer so denimo na voljo ustrezne prometne povezave in infrastruktura za zakonce in otroke, ki spremljajo člane osebja agencije ENISA. Potrebne podrobnosti bi morale biti določene v sporazumu med agencijo ENISA in državo članico gostiteljico, sklenjenem po odobritvi upravnega odbora agencije ENISA.

(19) Glede na vse večja tveganja in izzive na področju kibernetske varnosti, s katerimi se spopada Unija, bi bilo treba finančne in človeške vire, dodeljene agenciji ENISA, povečati, da bi ustrezali njeni okrepljeni vlogi in nalogam kot tudi kritičnemu položaju v ekosistemu organizacij, ki varujejo digitalni ekosistem Unije, kar bi agenciji ENISA omogočilo učinkovito izvajanje nalog, ki so na njo prenesene s to uredbo.

(20) Agencija ENISA bi morala razviti in ohranjati visoko raven strokovnega znanja ter delovati kot referenčna točka, ki vzpostavlja zaupanje v enotni trg zaradi svoje neodvisnosti, kakovosti svetovanja, ki ga zagotavlja, in kakovosti informacij, ki jih razširja, preglednosti svojih postopkov in načina delovanja ter skrbnosti pri izvajanju svojih nalog. Agencija ENISA bi morala dejavno podpirati nacionalna prizadevanja in proaktivno prispevati k prizadevanjem Unije ter obenem opravljati svoje naloge ob popolnem sodelovanju z institucijami, organi, uradi in agencijami Unije ter z državami članicami, pri tem pa preprečevati podvajanje dela in spodbujati sinergijo. Poleg tega bi moralo delo agencije ENISA temeljiti na prispevkih zasebnega sektorja in drugih zadevnih deležnikov ter sodelovanju z njimi. Sklop nalog bi moral določati, kako naj agencija ENISA doseže svoje cilje, ter hkrati dopuščati prožnost pri njenem delovanju.

(21) Da bi lahko ustrezno podpirala operativno sodelovanje med državami članicami, bi morala agencija ENISA še izboljšati svoje tehnične zmogljivosti ter človeške sposobnosti in veščine. Agencija ENISA bi morala povečati svoje strokovno znanje in sposobnosti. Agencija ENISA in države članice bi lahko prostovoljno oblikovale programe za napotitev nacionalnih strokovnjakov v agencijo ENISA, in sicer za vzpostavljanje nabora strokovnjakov in izmenjavo osebja.

(22) Agencija ENISA bi morala Komisiji pomagati s svetovanjem, 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 Unije bolj prilagodili kibernetski razsežnosti in omogočili usklajeno izvajanje teh politik in prava na nacionalni ravni. Agencija ENISA 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. Agencija ENISA bi morala Evropski parlament redno obveščati o svojih dejavnostih.

([13]) Soglasni sklep (2004/97/ES, Euratom) predstavnikov držav članic, ki so se sestali na ravni voditeljev držav ali vlad, z dne 13. decembra 2003 o kraju sedežev nekaterih uradov in agencij Evropske unije (UL L 29, 3.2.2004, str. 15).

(23) Javno jedro odprtega interneta, in sicer njegovi glavni protokoli in infrastruktura, ki so svetovno javno dobro, omogoča uporabo ključnih funkcij interneta kot celote in je podlaga za njegovo normalno delovanje. Agencija ENISA bi morala podpirati varnost javnega jedra odprtega interneta in stabilno delovanje, vključno s ključnimi protokoli (zlasti DNS, BGP in IPv6), ter delovanjem sistema domenskih imen (kot je delovanje vseh vrhnjih domen) in delovanjem korenskega območja.

(24) Temeljna naloga agencije ENISA je, da spodbuja dosledno izvajanje zadevnega pravnega okvira, zlasti učinkovito izvajanje Direktive (EU) 2016/1148 in drugih ustreznih pravnih instrumentov, ki se nanašajo na vidike kibernetske varnosti, 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.

(25) Agencija ENISA bi morala državam članicam ter institucijam, organom, uradom in agencijam Unije pomagati pri njihovih prizadevanjih za vzpostavljanje in krepitev zmogljivosti in pripravljenosti za preprečevanje, odkrivanje in odzivanje na kibernetske grožnje in incidente kot tudi pri zadevah v zvezi z varnostjo omrežij in informacijskih sistemov. Agencija ENISA bi morala zlasti podpirati razvoj in krepitev skupin za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: skupine CSIRT) držav članic in Unije iz Direktive (EU) 2016/1148 za doseganje visoke skupne ravni zrelosti v Uniji. Dejavnosti, ki jih agencija ENISA izvaja v zvezi z operativnimi zmogljivostmi držav članic, bi morale dejavno podpirati ukrepe, ki jih države članice sprejmejo zaradi izpolnjevanja obveznosti iz Direktive (EU) 2016/1148, in jih zato ne bi smele nadomeščati.

(26) Agencija ENISA bi morala pomagati tudi pri oblikovanju in posodabljanju strategij za varnost omrežij in informacijskih sistemov na ravni Unije, na zahtevo pa tudi na ravni držav članic, zlasti na področju kibernetske varnosti, ter spodbujati razširjanje takih strategij in spremljati napredek pri njihovem izvajanju. Poleg tega bi morala agencija ENISA med drugim tudi pomagati pri pokrivanju potreb za usposabljanje in gradivo za usposabljanje, vključno s potrebami javnih organov, ter po potrebi v precejšnjem obsegu „usposabljati izvajalce usposabljanj“ na podlagi okvira digitalnih kompetenc za državljane, da bi državam članicam, institucijam, organom, uradom in agencijam Unije pomagala pri razvoju lastnih zmogljivosti za usposabljanje.

(27) Agencija ENISA bi morala z omogočanjem tesnejšega usklajevanja in izmenjave najboljših praks podpirati države članice na področju ozaveščanja in izobraževanja glede kibernetske varnosti. Taka podpora bi lahko vključevala razvoj mreže nacionalnih kontaktnih točk za izobraževanje in platforme za usposabljanje na področju kibernetske varnosti. Mreža nacionalnih kontaktnih točk za izobraževanje bi lahko delovala v okviru mrežo nacionalnih uradnikov za zvezo in bila izhodišče za prihodnje usklajevanje znotraj držav članic.

(28) Agencija ENISA bi morala skupini za sodelovanje, vzpostavljeni z Direktivo (EU) 2016/1148, pomagati pri izvajanju njenih nalog, zlasti z zagotavljanjem strokovnega znanja in svetovanja ter omogočanjem lažje izmenjave najboljših praks, med drugim glede določitve izvajalcev bistvenih storitev s strani držav članic, ter glede čezmejnih odvisnosti v zvezi s tveganji in incidenti.

(29) Zaradi spodbujanja sodelovanja med javnim in zasebnim sektorjem ter znotraj zasebnega sektorja, zlasti pa, da bi pripomogla k zaščiti kritičnih infrastruktur, bi morala agencija ENISA podpirati znotrajsektorsko in medsektorsko izmenjavo informacij, zlasti v sektorjih iz Priloge II k Direktivi (EU) 2016/1148, in sicer z zagotavljanjem najboljših praks in navodil o razpoložljivih orodjih in o postopku ter navodil o tem, kako obravnavati regulativna vprašanja, povezana z izmenjavo informacij, na primer z omogočanjem lažjega ustanavljanja sektorskih centrov za izmenjavo in analizo informacij.

(30) Negativne posledice šibkih točk proizvodov IKT, storitev IKT in postopkov IKT bodo lahko v prihodnje še hujše, zato sta iskanje in odprava teh šibkih točk zelo pomembna za zmanjšanje splošnih tveganj v zvezi s kibernetsko varnostjo. Kot se je pokazalo, je mogoče s sodelovanjem med organizacijami, proizvajalci ali ponudniki proizvodov IKT, storitev IKT in postopkov IKT, pri katerih obstajajo takšne šibke točke, ter raziskovalci s področja kibernetske varnosti in državnimi organi, ki šibke točke odkrivajo, bistveno povečati stopnjo odkrivanja in odpravljanja šibkih točk proizvodov IKT, storitev IKT in postopkov IKT. Usklajeno razkrivanje šibkih točk je strukturiran proces sodelovanja, v katerem je o šibkih točkah najprej seznanjen lastnik informacijskega sistema, s čimer se organizaciji omogoči diagnoza in odprava šibkih točk, še preden se podrobne informacije o šibkih točkah razkrijejo tretjim osebam ali javnosti. Del tega procesa je tudi usklajevanje med odkriteljem in organizacijo v zvezi z seznanjanjem javnosti o teh šibkih točkah. Politike usklajenega razkrivanja šibkih točk bi lahko imele pomembno vlogo pri prizadevanjih držav članic za izboljšanje kibernetske varnosti.

(31) Agencija ENISA bi morala zbrati in analizirati nacionalna poročila skupin CSIRT in medinstitucionalne skupine za odzivanje na računalniške grožnje za institucije, organe in agencije Unije (v nadaljnjem besedilu: skupina CERT-EU), ustanovljene z Dogovorom med Evropskim parlamentom, Evropskim svetom, Svetom Evropske unije, Evropsko komisijo, Sodiščem Evropske unije, Evropsko centralno banko, Evropskim računskim sodiščem, Evropsko službo za zunanje delovanje, Evropskim ekonomsko-socialnim odborom, Evropskim odborom regij in Evropsko investicijsko banko o organizaciji in delovanju skupine za odzivanje na računalniške grožnje za institucije, organe in agencije Unije (CERT-EU) ([14]), ki so bila prostovoljno dana v skupno rabo, da bi tako pripomogla k določitvi skupnih postopkov, jezika in terminologije za izmenjavo informacij. V tej zvezi bi morala agencija ENISA v okviru Direktive (EU) 2016/1148, ki določa temelje za prostovoljno izmenjavo tehničnih informacij na operativni ravni znotraj mreže skupin za odzivanje na incidente na področju računalniške varnosti (v nadaljnjem besedilu: mreža skupin CSIRT), vzpostavljene z navedeno direktivo, vključiti tudi zasebni sektor.

(32) Agencija ENISA bi morala prispevati k odzivom na ravni Unije v primeru velikih čezmejnih incidentov in kriz, povezanih s kibernetsko varnostjo. To nalogo bi morala izvajati v skladu z mandatom agencije ENISA na podlagi te uredbe in pristopom, o katerem se dogovorijo države članice v smislu Priporočila Komisije (EU) 2017/1584 ([15]) ter sklepov Sveta z dne 26. junija 2018 o usklajenem odzivu EU na velike kibernetske incidente in krize. Ta naloga bi lahko vključevala zbiranje ustreznih informacij ter posredovanje med mrežo skupin CSIRT, tehnično skupnostjo in med nosilci odločitev, pristojnimi za krizno upravljanje. Poleg tega bi morala agencija ENISA, kadar tako zahteva ena ali več držav članic, podpirati operativno sodelovanje med državami članicami pri obvladovanju incidentov s tehničnega vidika, tako da bi olajšala ustrezne izmenjave tehničnih rešitev med državami članicami in zagotavljala informacije za komuniciranje z javnostjo. Agencija ENISA bi morala podpirati operativno sodelovanje s preskušanjem ureditev takšnega sodelovanja v okviru rednih vaj na področju kibernetske varnosti.

(33) Agencija ENISA bi morala pri podpiranju operativnega sodelovanja uporabljati razpoložljivo tehnično in operativno strokovno znanje skupine CERT-EU prek strukturiranega sodelovanja. Takšno strukturirano sodelovanje bi lahko okrepilo strokovno znanje in sposobnosti agencije ENISA. Po potrebi bi bilo treba sprejeti posebne dogovore med tema dvema subjektoma, s katerimi bi določili praktično izvajanje tega sodelovanja in se izogibali podvajanju dejavnosti.

(34) Zaradi podpore operativnemu sodelovanju v mreži skupin CSIRT bi morala agencija ENISA 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 zagotavljanjem analiz kibernetskih groženj in incidentov. Agencija ENISA bi morala olajšati 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 (EU) 2017/1584 priporoča, naj države članice v dobri veri sodelujejo ter si med seboj in z agencijo ENISA izmenjujejo informacije o velikih incidentih in krizah, povezanih s kibernetsko varnostjo, brez nepotrebnega odlašanja. Take informacije bi nadalje pomagale agenciji ENISA pri izvajanju njenih nalog podpiranja operativnega sodelovanja.

(35) Kot del rednega sodelovanja na tehnični ravni za podporo situacijskemu zavedanju v Uniji bi morala agencija ENISA ob tesnem sodelovanju z državami članicami redno pripravljati poglobljeno tehnično poročilo o stanju na področju kibernetske varnosti v EU glede incidentov in kibernetskih groženj, ki bi temeljilo na javno dostopnih informacijah, lastni analizi ter poročilih, ki ji jih pošljejo skupine CSIRT držav članic ali nacionalne enotne kontaktne točke za varnost omrežij in informacijskih sistemov (v nadaljnjem besedilu: enotne kontaktne točke) iz Direktive (EU) 2016/1148, 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 (EU INTCEN) pri Evropski službi za zunanje delovanje. To poročilo bi moralo biti na voljo Svetu, Komisiji, visokemu predstavniku Unije za zunanje zadeve in varnostno politiko ter mreži skupin CSIRT.

(36) Podpora agencije ENISA pri naknadnih tehničnih preiskavah incidentov, ki imajo pomembne ali znatne posledice, opravljenih na zahtevo zadevnih držav članic, bi morala biti usmerjena na preprečevanje prihodnjih incidentov. Da bi agenciji ENISA omogočile, da učinkovito podpre naknadne tehnične preiskave, bi morale zadevne države članice zagotoviti potrebne informacije in pomoč.

([14]) UL C 12, 13.1.2018, str. 1.
([15]) Priporočilo Komisije (EU) 2017/1584 z dne 13. septembra 2017 o usklajenem odzivu na velike kibernetske incidente in krize (UL L 239, 19.9.2017, str. 36).

(37) Države članice lahko podjetja, ki jih je incident prizadel, povabijo, naj sodelujejo z zagotavljanjem potrebnih informacij in pomoči agenciji ENISA, brez poseganja v njihovo pravico do varovanja poslovno občutljivih informacij in informacij, ki so pomembne za javno varnost.

(38) Potrebno je, da Agencija ENISA za boljše razumevanje izzivov na področju kibernetske varnosti in z namenom zagotavljanja dolgoročnega strateškega svetovanja državam članicam in institucijam, organom, uradom in agencijam Unije analizira sedanja in nastajajoča tveganja za kibernetsko varnost. V ta namen bi morala agencija ENISA 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 pričakovanem družbenem, pravnem, gospodarskem in regulativnem vplivu tehnoloških inovacij na varnost omrežij in informacij, zlasti na kibernetsko varnost. Agencija ENISA bi morala poleg tega države članice ter institucije, organe, urade in agencije Unije podpirati pri prepoznavanju novih tveganj za kibernetsko varnost in preprečevanju incidentov z opravljanjem analiz kibernetskih groženj, šibkih točk in incidentov.

(39) Da bi povečali odpornost Unije, bi morala agencija ENISA razvijati strokovno znanje in izkušnje na področju kibernetske varnosti infrastrukture, zlasti za podporo sektorjev iz Priloge II k Direktivi (EU) 2016/1148, ter infrastrukture, ki jo uporabljajo ponudniki digitalnih storitev iz Priloge III k navedeni direktivi, in sicer z zagotavljanjem svetovanja, izdajanjem smernic in izmenjavo najboljših praks. Agencija ENISA bi morala z namenom zagotavljanja lažjega dostopa do bolje strukturiranih informacij o tveganjih glede kibernetske varnosti 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, organov, uradov in agencij Unije in nacionalnih institucij, organov, uradov in agencij. Lažji dostop do bolje strukturiranih informacij o tveganjih za kibernetsko varnost in možnih rešitvah bi lahko državam članicam pomagal tudi pri izboljšanju zmogljivosti in usklajevanju praks, s čimer bi se povečala njihova splošna odpornost na kibernetske napade.

(40) Agencija ENISA bi morala prispevati k ozaveščanju javnosti o tveganjih glede kibernetske varnosti, vključno prek vseevropske kampanje ozaveščanja in s spodbujanjem izobraževanja, ter zagotavljati navodila glede dobrih praks za posamezne uporabnike, ki so namenjene državljanom, organizacijam in podjetjem. Agencija ENISA bi morala prispevati tudi k spodbujanju najboljših praks in rešitev, tudi glede kibernetske higiene in kibernetske pismenosti na ravni državljanov, organizacij in podjetij, in sicer z zbiranjem in analiziranjem javno dostopnih informacij o pomembnih incidentih ter pripravljanjem in objavljanjem poročil in navodil za državljane, organizacije in podjetja ter k izboljšanju splošne ravni pripravljenosti in odpornosti. Agencija ENISA bi si morala prizadevati tudi za to, da bi potrošnikom zagotovila ustrezne informacije o veljavnih certifikacijskih shemah, na primer z zagotavljanjem smernic in priporočil. Agencija ENISA bi morala poleg tega v skladu z akcijskim načrtom za digitalno izobraževanje, določenim s sporočilom Komisije z dne 17. januarja 2018, in v sodelovanju z državami članicami ter institucijami, organi, uradi in agencijami Unije organizirati redne kampanje ozaveščanja in redne javne izobraževalne kampanje za končne uporabnike, katerih namen je spodbujati varnejše ravnanje posameznikov na spletu in digitalno pismenost, da bi povečala ozaveščenost o možnih kibernetskih grožnjah, vključno s spletnimi kriminalnimi dejavnostmi, kot so napadi z zvabljanjem, botneti, finančne in bančne goljufije ter goljufije s podatki, pa tudi spodbujati osnovno svetovanje o večstopenjski avtentikaciji, nameščanju popravkov, šifriranju, anonimizaciji in varstvu podatkov.

(41) Agencija ENISA bi morala imeti osrednjo vlogo pri pospeševanju ozaveščenosti končnih uporabnikov glede varnosti naprav in varne uporabe storitev, in bi morala spodbujati vgrajeno varnost in vgrajeno zasebnost na ravni Unije. Pri doseganju tega cilja bi morala agencija ENISA čim bolje izkoristiti razpoložljive najboljše prakse in izkušnje, zlasti najboljše prakse in izkušnje akademskih ustanov in raziskovalcev na področju varnosti IT.

(42) Agencija ENISA 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 informacij o glavnih trendih na trgu kibernetske varnosti, tako na strani povpraševanja kot na strani ponudbe.

(43) Agencija ENISA bi morala prispevati k prizadevanjem Unije za sodelovanje z mednarodnimi organizacijami, pa tudi znotraj ustreznih mednarodnih okvirov sodelovanja s področja kibernetske varnosti. Agencija ENISA bi morala, kadar je to ustrezno, zlasti prispevati k sodelovanju z organizacijami, kot so OECD, OVSE in NATO. Takšno sodelovanje bi lahko vključevalo skupne vaje na področju kibernetske varnosti in skupno usklajevanje odzivanja na incidente. Navedene dejavnosti je treba izvajati ob doslednem spoštovanju načel vključenosti, vzajemnosti in avtonomije pri odločanju Unije ter brez poseganja v posebno naravo varnostne in obrambne politike katere koli države članice.

(44) Da bi lahko agencija ENISA v celoti izpolnila svoje cilje, bi morala sodelovati z ustreznimi nadzornimi organi Unije in drugimi pristojnimi organi v Uniji, institucijami, organi, uradi in agencijami Unije, vključno s skupino CERT-EU, EC3, Evropsko obrambno agencijo (EDA), Agencijo za evropski globalni satelitski navigacijski sistem (v nadaljnjem besedilu: Agencija za evropski GNSS), Organom evropskih regulatorjev za elektronske komunikacije (BEREC), Evropsko agencijo za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (eu-LISA), Evropsko centralno banko (ECB), Evropskim bančnim organom (EBA), Evropskim odborom za varstvo podatkov, Agencijo za sodelovanje energetskih regulatorjev (ACER), Agencijo Evropske unije za varnost v letalstvu (EASA) in vsemi drugimi agencijami Unije, ki se ukvarjajo s kibernetsko varnostjo. Agencija ENISA bi morala prav tako sodelovati z organi, ki se ukvarjajo z varstvom podatkov, da bi izmenjevala tehnično znanje in izkušnje ter najboljše prakse kot tudi nudila svetovanje glede vprašanj kibernetske varnosti, ki bi lahko vplivala na njihovo delo. Predstavniki organov za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter organov za varstvo podatkov na ravni držav članic in na ravni Unije bi morali imeti možnost, da so zastopani v svetovalni skupini agencije ENISA. Agencija bi morala pri sodelovanju z organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj v zvezi z vprašanji varnosti omrežij in informacij, ki bi lahko vplivala na njihovo delo, upoštevati obstoječe informacijske poti in vzpostavljena omrežja.

(45) Vzpostavila bi se lahko partnerstva z akademskimi ustanovami, ki imajo raziskovalne pobude na ustreznih področjih, hkrati pa bi morali obstajati ustrezni kanali za prispevke potrošniških in drugih organizacij, ki bi jih bilo treba upoštevati.

(46) Agencija ENISA bi morala v vlogi sekretariata za mrežo skupin CSIRT podpirati skupine CSIRT držav članic in skupino CERT-EU pri operativnem sodelovanju v zvezi z ustreznimi nalogah mreže skupin CSIRT, kot so opredeljene v Direktivi (EU) 2016/1148. Nadalje bi morala agencija ENISA 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 so zmožni vključevati najmanj dve skupini CSIRT, ob upoštevanju standardnih operativnih postopkov mreže skupin CSIRT.

(47) Da bi agencija ENISA povečala pripravljenost Unije pri odzivanju na incidente, bi morala organizirati vaje na področju kibernetske varnosti na ravni Unije in, na njihovo zahtevo, podpirati države članice ter institucije, organe, urade in agencije Unije pri organiziranju takih vaj. Obsežne vsestranske vaje, ki bi vključevale tehnične, operativne ali strateške elemente, bi bilo treba organizirati dvakrat letno. Poleg tega bi moralo biti agenciji ENISA omogočeno, da redno organizira manj vsestranske vaje z istim ciljem povečanja pripravljenosti Unije pri odzivanju na incidente.

(48) Agencija ENISA bi morala še naprej razvijati in ohranjati svoje strokovno znanje na področju certificiranja kibernetske varnosti z namenom podpiranja politike Unije na tem področju. Agencija ENISA bi se morala opirati na primere najboljše prakse in bi morala spodbujati uporabo certificiranja kibernetske varnosti v Uniji, vključno s prispevanjem k vzpostavitvi in ohranjanju certifikacijskega okvira za kibernetsko varnost na ravni Unije (v nadaljnjem besedilu: evropski certifikacijski okvir za kibernetsko varnost), da bi tako okrepila preglednost zanesljivosti kibernetske varnosti proizvodov IKT, storitev IKT in postopkov IKT ter s tem okrepila zaupanje v digitalni notranji trg in njegovo konkurenčnost.

(49) 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 ENISA 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 proizvodov, sistemov, omrežij in storitev, ki skupaj s programsko opremo zajemajo omrežja in informacijske sisteme.

(50) Agencija ENISA bi morala države članice, proizvajalce ali ponudnike proizvodov IKT, storitev IKT ali postopkov IKT spodbujati, naj zvišajo svoje splošne varnostne standarde, da bi vsi uporabniki interneta lahko ustrezno poskrbeli za svojo osebno kibernetsko varnost in bi bili spodbujeni k temu. Proizvajalci in ponudniki proizvodov IKT, storitev IKT ali postopkov IKT bi zlasti morali zagotavljati vse potrebne posodobitve ter odpoklicati, umakniti s trga ali reciklirati proizvode IKT, storitve IKT ali postopke IKT, ki ne izpolnjujejo standardov kibernetske varnosti, uvozniki in distributerji pa bi morali zagotoviti, da proizvodi IKT, storitve IKT in postopki IKT, ki jih dajejo na trg Unije, izpolnjujejo veljavne zahteve in ne pomenijo tveganja za potrošnike Unije.

(51) Agenciji ENISA bi moralo biti omogočeno, da lahko v sodelovanju s pristojnimi organi razširja informacije o ravni kibernetske varnosti proizvodov IKT, storitev IKT in postopkov IKT, ki so na voljo na notranjem trgu, ter izdaja opozorila, namenjena proizvajalcem oziroma ponudnikom proizvodov IKT, storitev IKT ali postopkov IKT, in od njih zahteva, da izboljšajo varnost svojih proizvodov IKT, storitev IKT in postopkov IKT, vključno s kibernetsko varnostjo.

(52) Agencija ENISA bi morala v celoti upoštevati tekoče dejavnosti na področju raziskav, razvoja in tehnološkega ocenjevanja, zlasti tiste dejavnosti, ki potekajo v okviru raznih raziskovalnih pobud Unije, da bi lahko svetovala institucijam, organom, uradom in agencijam Unije ter, po potrebi in na njihovo zahtevo, državam članicam glede potreb pri raziskavah in prednostnih nalogah na področju kibernetske varnosti. Zaradi ugotavljanja raziskovalnih potreb in prednostnih nalog bi se morala agencija ENISA posvetovati tudi z ustreznimi skupinami uporabnikov. Natančneje, vzpostavilo bi se lahko sodelovanje z Evropskim raziskovalnim svetom, Evropskim inštitutom za inovacije in tehnologijo ter Inštitutom Evropske unije za varnostne študije.

(53) Agencija ENISA bi se morala pri pripravi evropskih certifikacijskih shem za kibernetsko varnost redno posvetovati z organizacijami za standardizacijo, zlasti z evropskimi organizacijami za standardizacijo.

(54) Kibernetske grožnje imajo svetovno razsežnost. Da bi se izboljšali standardi kibernetske varnosti, je potrebno tesnejše mednarodno sodelovanje, vključno s potrebo po opredelitvi skupnih pravil obnašanja, sprejetjem kodeksov ravnanja, uporabo mednarodnih standardov, izmenjavo informacij, spodbujanjem hitrejše vzpostavitve mednarodnega sodelovanja pri odzivanju na vprašanja varnosti omrežij in informacij, pa tudi spodbujanjem skupnega globalnega pristopa do teh vprašanj. V ta namen bi morala agencija ENISA podpirati nadaljnjo udeležbo in sodelovanje Unije s tretjimi državami in mednarodnimi organizacijami, tako da bi po potrebi ustreznim institucijam, organom, uradom in agencijam Unije zagotavljala potrebno strokovno znanje in izkušnje ter analize.

(55) Agencija ENISA bi morala imeti možnost, da se odzove na *ad hoc* zahteve po svetovanju in pomoči s strani držav članic ter institucij, organov, uradov in agencij Unije o zadevah, za katere je agencija ENISA pooblaščena.

(56) V zvezi z upravljanjem agencije ENISA je smiselno in priporočljivo izvajati nekatera načela za zagotavljanje skladnosti s skupno izjavo in skupnim pristopom, o katerih se je julija 2012 dogovorila medinstitucionalna delovna skupina za decentralizirane agencije EU in ki sta namenjena racionalizaciji dejavnosti decentraliziranih agencij ter izboljšanju njihovega delovanja. Kakor je primerno, bi bilo prav tako treba odraziti priporočila iz skupne izjave in skupnega pristopa v delovnih programih, ocenah ter poročanju in upravnih praksah agencije ENISA..

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

(58) Da bi agencija ENISA 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. Komisija in države članice bi si morale prizadevati tudi za omejitev menjav svojih predstavnikov v upravnem odboru, da bi zagotovile njegovo neprekinjeno delovanje.

(59) Da bi agencija ENISA 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 bi moral svoje naloge opravljati popolnoma neodvisno. Izvršni direktor bi moral po predhodnem posvetovanju s Komisijo pripraviti predlog delovnega programa agencije ENISA ter sprejeti vse ukrepe, potrebne za zagotovitev nemotenega izvajanja tega delovnega programa. Izvršni direktor bi moral pripraviti letno poročilo, ki se predloži upravnemu odboru in zajema izvajanje letnega delovnega programa agencije ENISA, ter osnutek poročila o načrtu prihodkov in odhodkov za agencijo ENISA ter izvrševati proračun. Nadalje bi moral izvršni direktor imeti možnost, da ustanovi *ad hoc* delovne skupine, da preučijo posamezna vprašanja, zlasti vprašanja znanstvene, tehnološke, pravne ali družbeno-gospodarske narave. Treba bi bilo ustanoviti *ad hoc* delovno skupino, zlasti v zvezi s pripravo posebne predloge za evropsko certifikacijsko shemo za kibernetsko varnost (v nadaljnjem besedilu: predloga za shemo). Izvršni direktor bi moral zagotoviti, da so člani *ad hoc* delovnih skupin

izbrani v skladu z najvišjimi strokovnimi standardi, pri čemer bi si moral prizadevati za uravnoteženo zastopanost spolov ter glede na posamezna vprašanja ustrezno ravnovesje med predstavniki javnih uprav držav članic, institucij, organov, uradov in agencij Unije in zasebnega sektorja, vključno z industrijo, uporabniki in znanstveniki s področja varnosti omrežij in informacij.

(60) Izvršni odbor bi moral prispevati k učinkovitemu delovanju upravnega odbora. V okviru pripravljalnega dela v zvezi z odločitvami upravnega odbora bi moral upravni odbor podrobno preučiti ustrezne informacije, raziskati razpoložljive možnosti ter ponuditi nasvete in rešitve za pripravo ustreznih odločitev upravnega odbora.

(61) Agencija ENISA bi morala imeti svetovalno skupino agencije ENISA, ki bi delovala kot svetovalni organ, da bi zagotovila reden dialog z zasebnim sektorjem, organizacijami združenji potrošnikov in drugimi ustreznimi deležniki. Svetovalna skupina agencije ENISA, ki jo na predlog izvršnega direktorja ustanovi upravni odbor, bi morala obravnavati zadeve, ki so pomembne za deležnike, in o njih obvestiti agencijo ENISA. S svetovalno skupino agencije ENISA bi se bilo treba posvetovati zlasti v zvezi z osnutkom letnega delovnega programa agencije ENISA. Sestava svetovalne skupine agencije ENISA in naloge, dodeljene tej skupini, bi morale zagotoviti zadostno zastopanost deležnikov pri delu agencije ENISA.

(62) Treba bi bilo ustanoviti certifikacijsko skupino deležnikov za kibernetsko varnost, ki bi agenciji ENISA in Komisiji olajšala posvetovanje z ustreznimi deležniki. Certifikacijsko skupino deležnikov za kibernetsko varnost bi morali sestavljati člani, ki bi uravnoteženo zastopali industrijo, tako na strani povpraševanja kot na strani ponudbe proizvodov IKT in storitev IKT, ter vključevali zlasti MSP, ponudnike digitalnih storitev, evropske in mednarodne organe za standardizacijo, nacionalne akreditacijske organe, nadzorne organe za varstvo podatkov in organe za ugotavljanje skladnosti na podlagi Uredbe (ES) št. 765/2008 Evropskega parlamenta in Sveta ([16]), znanstveno skupnost in potrošniške organizacije.

(63) Agencija ENISA bi morala sprejeti pravila za preprečevanje in obvladovanje nasprotij interesov. Agencija ENISA bi morala poleg tega uporabljati ustrezne predpise Unije o dostopu javnosti do dokumentov iz Uredbe Evropskega parlamenta in Sveta (ES) št. 1049/2001 ([17]). Agencija ENISA bi morala osebne podatke obdelovati v skladu z Uredbo (EU) 2018/1725 Evropskega parlamenta in Sveta ([18]). Agencija ENISA bi morala spoštovati določbe, ki veljajo za institucije, organe, urade in agencije Unije, in nacionalno zakonodajo o ravnanju s podatki, zlasti občutljivimi netajnimi podatki in tajnimi podatki Evropske unije (EUCI).

(64) Da se agenciji ENISA zagotovita popolna samostojnost in neodvisnost ter se ji omogoči, da lahko opravlja dodatne naloge, tudi nepredvidene nujne naloge, bi bilo treba agenciji ENISA dodeliti zadostna lastna proračunska sredstva, ki bi se morali večinoma zagotoviti s prispevkom Unije in prispevki tretjih držav, ki sodelujejo pri delu agencije ENISA. Za zagotovitev, da ima agencija ENISA zadostno zmogljivost za izvajanje vseh svojih nalog in doseganje ciljev, ki jih je vedno več, je ustrezen proračun bistvenega pomen. Večina osebja agencije ENISA bi morala neposredno sodelovati pri operativnem izvajanju njenega mandata. Državi članici gostiteljici in vsaki drugi državi članici bi moralo biti dovoljeno, da lahko prostovoljno prispeva k proračunu agencije ENISA. Za subvencije v breme splošnega proračuna Unije bi se moral še vedno uporabljati postopek za sprejemanje proračuna Unije. Revizijo zaključnih računov agencije ENISA bi moralo opraviti Računsko sodišče, da bi bili zagotovljeni preglednost in odgovornost.

(65) Certificiranje kibernetske varnosti ima pomembno vlogo pri krepitvi zaupanja v proizvode IKT, storitve IKT in postopke IKT ter njihove varnosti. Enotni digitalni trg, zlasti podatkovno gospodarstvo in internet stvari, lahko uspevajo le, če obstaja splošno zaupanje javnosti, da ti proizvodi, storitve in postopki nudijo določeno raven 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 (EU) 2016/1148, so poleg tega sektorji, v katerih je certificiranje kibernetske varnosti ključno.

([16]) Uredba (ES) št. 765/2008 Evropskega Parlamenta in Sveta z dne 9. julija 2008 o določitvi zahtev za akreditacijo in nadzor trga v zvezi s trženjem proizvodov ter razveljavitvi Uredbe (EGS) št. 339/93 (UL L 218, 13.8.2008, str. 30).

([17]) 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).

([18]) Uredba (EU) 2018/1725 Evropskega parlamenta in Sveta z dne 23. oktobra 2018 o varstvu posameznikov pri obdelavi osebnih podatkov v institucijah, organih, uradih in agencijah Unije in o prostem pretoku takih podatkov ter o razveljavitvi Uredbe (ES) št. 45/2001 in Sklepa št. 1247/2002/ES (UL L 295, 21.11.2018, str. 39).

(66) V sporočilu z naslovom „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 proizvodih in rešitvah na področju kibernetske varnosti. Dobava proizvodov IKT ter opravljanje storitev IKT in postopkov IKT na enotnem trgu sta geografsko še vedno zelo razdrobljena. Razlog za to je, da se je industrija kibernetske varnosti v Evropi razvila predvsem zaradi povpraševanja nacionalnih vlad. Poleg tega so med drugimi vrzelmi, ki vplivajo na enotni trg na področju kibernetske varnosti, pomanjkanje interoperabilnih rešitev (tehničnih standardov), praks in mehanizmov certificiranja na ravni Unije. Evropska podjetja zato težko konkurirajo na nacionalni ravni, ravni Unije in svetovni ravni. Po drugi strani pa se s tem zmanjšuje izbira učinkovitih in uporabnih tehnologij kibernetske varnosti, do katerih imajo dostop posamezniki in podjetja. Podobno je Komisija v sporočilu iz leta 2017 o vmesnem pregledu izvajanja strategije za enotni digitalni trg - Povezani enotni digitalni trg za vse poudarila potrebo po varnih povezanih proizvodih 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 notranjega trga.

(67) Zdaj se certificiranje proizvodov IKT, storitev IKT in postopkov 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. V tem smislu certifikat, ki ga izda nacionalni certifikacijski organ za kibernetsko varnost, praviloma ni priznan v drugih državah članicah. Tako so podjetja lahko prisiljena svoje proizvode IKT, storitve IKT in postopke IKT certificirati v več državah članicah, v katerih poslujejo, da bi na primer lahko sodelovala v nacionalnih postopkih javnega naročanja, zaradi česar imajo višje stroške. Poleg tega se zdi, da ni usklajenega in celovitega pristopa k horizontalnim vidikom kibernetske varnosti, na primer na področju interneta stvari, čeprav se pojavljajo nove sheme. Pri obstoječih shemah se pojavljajo znatne pomanjkljivosti in razlike v smislu pokritosti proizvodov, ravni zanesljivosti, vsebinskih meril in dejanske uporabe, kar ovira delovanje mehanizmov vzajemnega priznavanja znotraj Unije.

(68) Prizadevanja za zagotovitev vzajemnega priznavanja certifikatov v Uniji so že potekala. 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 le nekatere države članice. To dejstvo omejuje učinkovitost SOG-IS MRA z vidika notranjega trga.

(69) Zato je treba sprejeti skupni pristop in vzpostaviti evropski certifikacijski okvir za kibernetsko varnost, ki določa glavne horizontalne zahteve za evropske certifikacijske sheme za kibernetsko varnost, ki jih je treba oblikovati, in omogoča, da se evropski certifikati kibernetske varnosti ter izjave EU o skladnosti za proizvode IKT, storitve IKT in postopke IKT priznavajo in uporabljajo v vseh državah članicah. Pri tem je treba nujno temeljiti na obstoječih nacionalnih in mednarodnih shemah ter sistemih vzajemnega priznavanja, zlasti sistemu SOG-IS, pa tudi omogočiti nemoten prehod z obstoječih shem iz teh sistemov na sheme iz novega evropskega certifikacijskega okvira za kibernetsko varnost. Evropski okvir bi moral imeti dvojni cilj: po eni strani bi moral pripomoči k povečanju zaupanja v proizvode IKT, storitve IKT in postopke IKT, ki so bili certificirani v okviru evropskih certifikacijskih shem za kibernetsko varnost. Kot drugo pa bi moral pomagati preprečevati kopičenje nasprotujočih si ali prekrivajočih se nacionalnih certifikacijskih shem za kibernetsko varnost in tako zmanjšati stroške za podjetja, ki poslujejo na enotnem digitalnem trgu. Evropske certifikacijske sheme za kibernetsko varnost bi morale biti nediskriminatorne in temeljiti na evropskih ali mednarodnih standardih, razen če so ti standardi neučinkoviti ali neprimerni za dosego legitimnih ciljev Unije v tej zvezi.

(70) Evropski certifikacijski okvir za kibernetsko varnost bi moral biti enotno vzpostavljen v vseh državah članicah, da se ne bi zaradi različnih ravni strogosti v različnih državah članicah pojavila praksa „nakupovanja certifikatov“.

(71) Evropske certifikacijske sheme za kibernetsko varnost bi morale temeljiti na že obstoječih sistemih na mednarodni in nacionalni ravni ter po potrebi tehničnih specifikacijah forumov in konzorcijev, pri čemer bi se bilo treba opirati na obstoječe pozitivne lastnosti ter ocenjevati in odpravljati pomanjkljivosti.

(72) Prožne rešitve za kibernetsko varnost so nujno potrebne za to, da bi industrija lahko predvidela kibernetske grožnje, zato bi bilo treba vsako certifikacijsko shemo zasnovati na način, da se prepreči, da bi hitro zastarela.

(73) Komisija bi morala biti pooblaščena za sprejemanje evropskih certifikacijskih shem za kibernetsko varnost za določene skupine proizvodov IKT, storitev IKT in postopkov IKT. Te sheme bi morali izvajati in nadzorovati nacionalni certifikacijski organi za kibernetsko varnost, 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 bi organi, ki izvajajo takšne sheme, morali imeti možnost predlagati Komisiji, naj preuči možnost, da bi te sheme odobrila kot evropsko certifikacijsko shemo za kibernetsko varnost.

(74) Določbe te uredbe ne bi smele posegati v pravo Unije, ki vsebuje posebne predpise o certificiranju proizvodov IKT, storitev IKT in postopkov IKT. Zlasti Uredba (EU) 2016/679 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 proizvodov IKT, storitev IKT in postopkov IKT. Ta uredba ne posega v certificiranje postopkov obdelave podatkov na podlagi Uredbe (EU) 2016/679, vključno kadar so taki postopki vgrajeni v proizvode IKT, storitve IKT in postopke IKT.

(75) Evropske certifikacijske sheme bi morale zagotoviti, da proizvodi IKT, storitve IKT in postopki IKT, ki so bili certificirani v okviru takih shem, izpolnjujejo posebne zahteve, da se zaščitijo razpoložljivost, pristnost, celovitost in zaupnost shranjenih, prenesenih ali obdelanih podatkov ali z njimi povezanih funkcij ali storitev, ki jih ponujajo ali so dostopni prek navedenih proizvodov, storitev in postopkov v celotnem življenjskem ciklu. V tej uredbi ni mogoče podrobno določiti zahtev glede kibernetske varnosti, ki se nanašajo na vse proizvode IKT, storitve IKT in postopke IKT v tej uredbi. Proizvodi IKT, storitve IKT in postopki 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 v vseh okoliščinah. Zato je treba sprejeti širok in splošen pojem kibernetske varnosti za namene certificiranja, ki bi ga moral dopolnjevati 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 proizvodih IKT, storitvah IKT in postopkih IKT, bi bilo treba nadalje podrobno določiti na ravni posamezne certifikacijske sheme, ki jo sprejme Komisija, na primer s sklicem na standarde ali tehnične specifikacije, če ustrezni standardi niso na voljo.

(76) Tehnične specifikacije, ki naj bi bile uporabljene v evropskih certifikacijskih shemah za kibernetsko varnost, bi bilo treba upoštevati zahteve iz Priloge II k Uredbi (EU) št. 1025/2012 Evropskega parlamenta in Sveta ([19]). Toda v ustrezno utemeljenih primerih bi morda bila potrebna nekatera odstopanja od teh zahtev, kadar naj bi bile navedene tehnične specifikacije uporabljene v evropski certifikacijski shemi za kibernetsko varnost, ki se nanaša na „visoko“ raven zanesljivosti. Razlogi za takšna odstopanja bi morali biti objavljeni.

(77) Ugotavljanje skladnosti je postopek ugotavljanja, ali so posebne zahteve glede proizvoda IKT, storitve IKT ali postopka IKT izpolnjene. Ta postopek izvede neodvisna tretja oseba, ki ni proizvajalec proizvoda ali ponudnik proizvodov IKT, storitev IKT ali postopkov IKT, ki se ocenjujejo. Evropski certifikat kibernetske varnosti bi moral biti izdan na podlagi uspešno opravljene ocene proizvoda IKT, storitve IKT ali postopka IKT. Evropski certifikat kibernetske varnosti bi moral veljati kot potrdilo, da je bila ocena ustrezno opravljena. Evropska certifikacijska shema za kibernetsko varnost bi glede na raven zanesljivosti morala določati, ali mora certifikat izdati zasebni ali javni organ. Ugotavljanje skladnosti in certificiranje samo po sebi ne more jamčiti, da so certificirani proizvodi IKT, storitve IKT in postopki IKT kibernetsko varni. Namesto tega obstajajo postopki in tehnična metodologija za potrditev, da so bili proizvodi IKT, storitve IKT in postopki IKT testirani ter da izpolnjujejo nekatere zahteve glede kibernetske varnosti, določene drugje, na primer v tehničnih standardih.

(78) Uporabnik evropskega certifikata kibernetske varnosti bi moral izbrati ustrezno certifikacijo in z njo povezane varnostne zahteve na podlagi analize tveganja, povezanega z uporabo proizvodov IKT, storitev IKT ali postopkov IKT. V skladu s tem bi morala raven zanesljivosti ustrezati stopnji tveganja, povezani s predvideno uporabo proizvoda IKT, storitve IKT ali postopka IKT.

([19]) Uredba (EU) št. 1025/2012 Evropskega parlamenta in Sveta z dne 25. oktobra 2012 o evropski standardizaciji, spremembi direktiv Sveta 89/686/EGS in 93/15/EGS ter direktiv 94/9/ES, 94/25/ES, 95/16/ES, 97/23/ES, 98/34/ES, 2004/22/ES, 2007/23/ES, 2009/23/ES in 2009/105/ES Evropskega parlamenta in Sveta ter razveljavitvi Sklepa Sveta 87/95/EGS in Sklepa št. 1673/2006/ES Evropskega parlamenta in Sveta (UL L 316, 14.11.2012, str. 12).

(79) Evropske certifikacijske sheme za kibernetsko varnost bi lahko omogočale, da se ugotavljanje skladnosti izvede na izključno odgovornost proizvajalca ali ponudnika proizvodov IKT, storitev IKT ali postopkov IKT (v nadaljnjem besedilu: samoocenjevanje skladnosti). V takih primerih bi moralo biti dovolj, da proizvajalec ali ponudnik sam izvede vse preglede da bi zagotovil, da so proizvodi IKT, storitve IKT ali postopki IKT skladni z evropsko certifikacijsko shemo za kibernetsko varnost. Ugotavljanje skladnosti bi moralo šteti kot primerno za manj kompleksne proizvode IKT, storitve IKT ali postopke IKT, ki pomenijo nizko tveganje za javni interes, kot so preprosta zasnova in mehanizmi proizvodnje. Poleg tega bi bilo treba samoocenjevanje skladnosti za proizvode IKT, storitve IKT ali postopke IKT dovoliti samo, kadar ustrezajo „osnovni“ ravni zanesljivosti.

(80) V okviru evropskih certifikacijskih shem za kibernetsko varnost bi se lahko dopustila samoocenjevanja skladnosti in certificiranje proizvodov IKT, storitev IKT ali postopkov IKT. V teh primerih bi morala shema potrošnikom in drugim uporabnikom ponuditi jasne in razumljive načine za razlikovanje med proizvodi IKT, storitvami IKT ali postopki IKT, v zvezi s katerimi je njihov proizvajalec ali ponudnik odgovoren za oceno, in proizvodi IKT, storitvami IKT ali postopki IKT, ki jih je certificirala tretja stran.

(81) Proizvajalec ali ponudnik proizvodov IKT, storitev IKT ali postopkov IKT, ki izvede samoocenjevanje skladnosti, bi moral imeti možnost v okviru postopka ugotavljanja skladnosti izdati in podpisati izjavo EU o skladnosti. Izjava EU o skladnosti je dokument, v katerem je navedeno, da posamezen proizvod IKT, storitev IKT ali postopek IKT izpolnjuje zahteve evropske certifikacijske sheme za kibernetsko varnost. Proizvajalec ali ponudnik z izdajo in podpisom izjave EU o skladnosti prevzame odgovornost za skladnost proizvoda IKT, storitve IKT ali postopka IKT s pravnimi zahtevami evropske certifikacijske sheme za kibernetsko varnost. Kopijo izjave EU o skladnosti bi bilo treba predložiti nacionalnemu certifikacijskemu organu za kibernetsko varnost in agenciji ENISA.

(82) Proizvajalci ali ponudniki proizvodov IKT, storitev IKT ali postopkov IKT bi morali za obdobje, opredeljeno v ustrezni evropski certifikacijski shemi za kibernetsko varnost, hraniti izjavo EU o skladnosti, tehnično dokumentacijo in vse druge ustrezne informacije, ki se nanašajo na skladnost proizvodov IKT, storitev IKT ali postopkov IKT z zadevno shemo, tako da je na voljo pristojnemu nacionalnemu certifikacijskemu organu za kibernetsko varnost. V tehnični dokumentaciji bi morale biti določene zahteve, ki se uporabljajo v okviru sheme in morala bi zajemati zasnovo, proizvodnjo in delovanje proizvoda IKT, storitve IKT ali postopka IKT v obsegu, ki je pomemben za tako ugotavljanje. Tehnična dokumentacija bi morala biti pripravljena tako, da bi omogočala ugotavljanje, ali proizvod IKT oziroma storitev IKT izpolnjuje zahteve, ki se uporabljajo v okviru te sheme.

(83) Pri upravljanju evropskega certifikacijskega okvira za kibernetsko varnost bi bilo treba upoštevati sodelovanje držav članic in ustrezno vključitev deležnikov ter določiti vlogo Komisije med načrtovanjem, vložitvijo predlogov in zahtev ter med pripravo, sprejetjem in pregledovanjem evropskih certifikacijskih shem za kibernetsko varnost.

(84) Komisija bi morala ob podpori evropske certifikacijske skupine za kibernetsko varnost in certifikacijske skupine deležnikov za kibernetsko varnost ter po odprtem in širokem posvetovanju oblikovati tekoči delovni program Unije za evropske certifikacijske sheme za kibernetsko varnost in ga objaviti v obliki pravno nezavezujočega instrumenta. Tekoči delovni program Unije bi moral biti strateški dokument, ki industriji, nacionalnim organom in organom za standardizacijo omogoča, da se pripravijo zlasti na prihodnje evropske certifikacijske sheme za kibernetsko varnost. Tekoči delovni program Unije bi moral vključevati večletni pregled zahtev za pripravo predlog za sheme, ki jih namerava Komisija nasloviti na agencijo ENISA na podlagi posebnih razlogov. Komisija bi morala ta tekoči delovni program Unije upoštevati pri pripravi svojega tekočega načrta za standardizacijo IKT in zahteve za standardizacijo evropskim organizacijam za standardizacijo. Glede na hitro uvajanje novih tehnologij in naraščanja njene uporabe med uporabniki in podjetji, zaradi pojavljanja prej neznanih tveganj glede kibernetske varnosti in zaradi sprememb v zakonodaji in na trgu bi morala Komisija ali evropska certifikacijska skupina za kibernetsko varnost imeti pravico od agencije ENISA zahtevati, naj pripravi predloge za sheme, ki niso bile vključene v tekoči delovni program Unije. Komisija in evropska certifikacijska skupina za kibernetsko varnost bi morali v takih primerih oceniti tudi upravičenost take zahteve, pri čemer bi upoštevali splošne cilje te uredbe in potrebo po zagotavljanju kontinuitete načrtovanja agencije ENISA in njene uporabe virov.

Agencija ENISA bi morala po prejemu take zahteve brez nepotrebnega odlašanja pripraviti predloge za sheme za posamezne proizvode IKT, storitve IKT ali postopke IKT. Komisija bi morala oceniti pozitivni in negativni učinek svoje zahteve na zadevni specifični trg, zlasti njegov vpliv na MSP, inovacije, ovire za vstop na ta trg in stroške za končne uporabnike. Nadalje bi morali Komisijo pooblastiti, da na podlagi predloge za shemo, ki jo pripravi agencija ENISA, sprejme evropsko certifikacijsko shemo za kibernetsko varnost z izvedbenimi akti. Ob upoštevanju splošnega namena in varnostnih ciljev, določenih v tej uredbi, bi moral biti v evropskih certifikacijskih shemah za kibernetsko varnost, ki jih sprejme Komisija, določen minimalni sklop elementov v zvezi z vsebino, področjem uporabe in delovanjem posamezne sheme. Ti elementi bi morali med drugim vključevati področje uporabe in predmet certificiranja kibernetske varnosti, vključno z zajetimi kategorijami proizvodov IKT, storitev IKT in postopkov IKT, podrobno specifikacijo zahtev glede kibernetske varnosti, na primer s sklicem na standarde ali tehnične specifikacije, posebnimi merili in metodami za ocenjevanje ter predvideno raven zanesljivosti („osnovno“, „znatno“ ali „visoko“) in po potrebi stopnjami ocenjevanja. Agencija ENISA bi morala imeti možnost, da zavrne zahtevo evropske certifikacijske skupine za kibernetsko varnost. Takšne odločitve, ki bi morale biti ustrezno obrazložene, bi moral sprejeti upravni odbor.

(85) Agencija ENISA bi morala vzdrževati spletišče, ki zagotavlja informacije o evropskih certifikacijskih shemah za kibernetsko varnost in je namenjeno obveščanju javnosti o teh shemah, ki bi med drugim moralo vključevati zahteve za pripravo predloge za shemo, pa tudi povratne informacije, prejete med posvetovalnim postopkom, ki ga je v pripravljalni fazi izvedla agencija ENISA. Spletišče bi moralo vsebovati tudi informacije o evropskih certifikatih kibernetske varnosti in izjavah EU o skladnosti, izdanih na podlagi te uredbe, vključno v zvezi z njihovim odvzemom in potekom. Na spletišču bi morale biti navedene tudi nacionalne certifikacijske sheme za kibernetsko varnost, ki so bile nadomeščene z evropsko certifikacijsko shemo za kibernetsko varnost.

(86) Raven zanesljivosti evropske certifikacijske sheme za kibernetsko varnost je podlaga za zaupanje, da proizvod IKT, storitev IKT ali postopek IKT izpolnjuje varnostne zahteve določene evropske certifikacijske sheme za kibernetsko varnost. Zaradi skladnosti evropskega certifikacijskega okvira za kibernetsko varnost bi morala evropska certifikacijska shema za kibernetsko varnost določati ravni zanesljivosti za evropske certifikate kibernetske varnosti in izjave EU o skladnosti, izdane v okviru te sheme. Vsak evropski certifikat kibernetske varnosti se morda nanaša na eno od ravni zanesljivosti: „osnovno“, „znatno“, „visoko“, medtem ko bi se izjava EU o skladnosti morda nanašala samo na „osnovno“ raven zanesljivosti. Ravni zanesljivosti bi določale ustrezno strogost in obseg ocene proizvoda IKT, storitve IKT ali postopka IKT in bi bile opredeljene s sklici na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je ublažiti ali preprečiti incidente. Vsaka raven zanesljivosti bi morala biti usklajena s posameznimi sektorskimi področji, v katerih se uporablja certificiranje.

(87) V evropski certifikacijski shemi za kibernetsko varnost bi se lahko določilo več stopenj ocenjevanja, odvisno od strogosti in obsega uporabljene metodologije za ocenjevanje. Stopnje ocenjevanja bi morale ustrezati eni od ravni zanesljivosti in biti povezane z ustrezno kombinacijo elementov zanesljivosti. Proizvod IKT, storitev IKT ali postopek IKT bi moral za vse ravni zanesljivosti vsebovati vrsto varnih funkcij, kot so določene s shemo in ki lahko vključujejo: varno vnaprej določeno konfiguracijo, podpisano kodo, varno posodobitev in ublažitev nevarnosti izkoriščanja ter polne zaščite spomina, organiziranega v skladu ali 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.

(88) Pri „osnovni“ ravni zanesljivosti bi morali biti vodilo ocenjevanja vsaj naslednji elementi zanesljivosti: organ za ugotavljanje skladnosti bi moral pri ocenjevanju najmanj pregledati tehnično dokumentacijo proizvoda IKT, storitve IKT ali postopka IKT. Kadar certifikacija vključuje tudi postopke IKT, bi bilo treba postopek, uporabljen pri zasnovi, razvoju in vzdrževanju proizvoda IKT ali storitve IK podvreči tudi tehničnemu pregledu. Kadar evropska certifikacijska shema za kibernetsko varnost predvideva samoocenjevanje skladnosti, bi moralo zadostovati, da proizvajalec ali ponudnik proizvodov IKT, storitev IKT ali postopkov IKT izvede samooceno skladnosti proizvodov IKT, storitev IKT ali postopkov IKT s certifikacijsko shemo.

(89) Pri „znatni“ ravni zanesljivosti bi moralo biti vodilo ocenjevanja poleg zahtev iz „osnovne“ ravni zanesljivosti vsaj še preverjanje skladnosti varnostnih funkcionalnosti proizvoda IKT, storitve IKT ali postopka IKT s pripadajočo tehnično dokumentacijo.

(90) Pri „visoki“ ravni zanesljivosti bi moralo biti vodilo ocenjevanje poleg zahtev iz „znatne“ ravni zanesljivosti vsaj še testiranje učinkovitosti, s katerim se preveri odpornost varnostnih funkcionalnosti proizvoda IKT, storitve IKT ali postopka IKT proti kompleksnim kibernetskim napadom, ki jih izvedejo osebe, ki imajo precejšnje znanje in vire.

(91) Uporaba evropskega certificiranja za kibernetsko varnost in izjave EU o skladnosti bi morala ostati prostovoljna, razen če je v pravu Unije ali pravu držav članic, sprejetemu v skladu s pravom Unije, določeno drugače. Kadar pravo Unije ni harmonizirano, lahko države članice sprejmejo nacionalne tehnične predpise, ki določajo obvezno certificiranje v okviru evropske certifikacijske sheme za kibernetsko varnost, v skladu z Direktivo (EU) 2015/1535 Evropskega parlamenta in Sveta ([20]). Države članice lahko evropsko certificiranje za kibernetsko varnost uporabijo tudi v okviru javnega naročanja in Direktive 2014/24/EU Evropskega parlamenta in Sveta ([21]).

(92) Za izboljšanje ravni kibernetske varnosti v Uniji bodo posebne zahteve glede kibernetske varnosti in ustreznega certificiranja za nekatere proizvode IKT, storitve IKT ali postopke IKT morda v prihodnosti morale postati obvezne. Komisija bi morala redno spremljati učinek sprejetih evropskih certifikacijskih shem za kibernetsko varnost na razpoložljivost varnih proizvodov IKT, storitev IKT ali postopkov IKT na notranjem trgu ter redno oceniti, v kolikšni meri proizvajalci in ponudniki proizvodov IKT, storitev IKT ali postopkov IKT v Uniji uporabljajo certifikacijske sheme. Učinkovitost evropskih certifikacijskih shem za kibernetsko varnost in vprašanje, ali bi morale določene sheme postati obvezne, bi bilo treba oceniti ob upoštevanju zakonodaje Unije, povezane s kibernetsko varnostjo, zlasti Direktive (EU) 2016/1148, ob upoštevanju varnosti omrežij in informacijskih sistemov, ki jih uporabljajo izvajalci bistvenih storitev.

(93) Evropski certifikati kibernetske varnosti in izjave EU o skladnosti bi morali pomagati končnim uporabnikom pri sprejemanju ozaveščene odločitve. Zato bi bilo treba certificiranim in samoocenjenim proizvodom IKT, storitvam IKT in postopkom IKT, ki so bili certificirani ali za katere je bila izdana izjava EU o skladnosti, priložiti strukturirane informacije, prilagojene pričakovani tehnični ravni predvidenega končnega uporabnika. Vse takšne informacije bi morale biti na voljo na spletu in po potrebi v fizični obliki. Končni uporabnik bi moral imeti dostop do informacij o referenčni številki certifikacijske sheme, ravni zanesljivosti, opisu tveganj za kibernetsko varnost, povezanih s proizvodom IKT, storitvijo IKT ali postopkom IKT, ter o organu izdajatelju ali bi moral imeti možnost pridobiti kopijo evropskega certifikata kibernetske varnosti. Poleg tega bi moral biti končni uporabnik seznanjen s politiko proizvajalca ali ponudnika proizvodov IKT, storitev IKT ali postopkov IKT glede zagotavljanja podpore v zvezi s kibernetsko varnostjo, in sicer kako dolgo lahko končni uporabniki pričakujejo, da bodo prejemali posodobitve ali popravke v zvezi s kibernetsko varnostjo. Po potrebi bi bilo treba zagotoviti tudi navodila glede ukrepanja ali nastavitev, ki jih lahko končni uporabnik izvede za ohranitev ali povečanje kibernetske varnosti proizvoda IKT ali storitve IKT in kontaktne informacije enotne kontaktne točke za poročanje in podporo v primeru kibernetskih napadov (poleg samodejnega poročanja). Te informacije bi bilo treba redno posodabljati in jih objavljati na spletišču, ki zagotavlja informacije o evropskih certifikacijskih shemah za kibernetsko varnost.

(94) Da bi dosegli cilje te uredbe in preprečili razdrobljenost notranjega trga, bi nacionalne certifikacijske sheme ali postopki za kibernetsko varnost za proizvode IKT, storitve IKT ali postopke IKT, ki jih zajema evropska certifikacijska shema za kibernetsko varnost, morali prenehati učinkovati od datuma, ki ga določi Komisija z izvedbenimi akti. Poleg tega države članice ne bi smele uvajati novih nacionalnih certifikacijskih shem za kibernetsko varnost za proizvode IKT, storitve IKT ali postopke 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 kibernetsko varnost za namene nacionalne varnosti. Države članice bi morale Komisijo in evropsko certifikacijsko skupino za kibernetsko varnost obveščati o vsaki nameri priprave novih nacionalnih certifikacijskih shem za kibernetsko varnost. Komisija in evropska certifikacijska skupina za kibernetsko varnost bi morali oceniti, kakšni so učinki novih nacionalnih certifikacijskih shem za kibernetsko varnost na pravilno delovanje notranjega trga, ob upoštevanju kakršnih koli strateških interesov za to, da bi se zahtevalo, da jo nadomesti evropska certifikacijska shema za kibernetsko varnost.

(95) Namen evropskih certifikacijskih shem za kibernetsko varnost je, da pomagajo harmonizirati prakso na področju kibernetske varnosti v Uniji. Prispevale naj bi tudi k povečanju ravni kibernetske varnosti v Uniji. Pri zasnovi evropskih certifikacijskih shem za kibernetsko varnost bi bilo treba upoštevati in omogočiti razvoj inovacij na področju kibernetske varnosti.

([20]) Direktiva (EU) 2015/1535 Evropskega parlamenta in Sveta z dne 9. septembra 2015 o določitvi postopka za zbiranje informacij na področju tehničnih predpisov in pravil za storitve informacijske družbe (UL L 241, 17.9.2015, str. 1).

([21]) Direktiva 2014/24/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o javnem naročanju in razveljavitvi Direktive 2004/18/ES (UL L 94, 28.3.2014, str. 65).

(96) V evropskih certifikacijskih shemah za kibernetsko varnost bi bilo treba upoštevati obstoječe metode razvoja programske in strojne opreme ter zlasti učinek pogostih posodobitev programske ali vdelane programske opreme na posamezne evropske certifikate kibernetske varnosti. V evropskih certifikacijskih shemah za kibernetsko varnost bi bilo treba določiti pogoje, pod katerimi bi se lahko zaradi posodobitve zahtevalo ponovno certificiranje proizvoda IKT, storitve IKT ali postopka IKT ali zmanjšanje obsega posameznega evropskega certifikata kibernetske varnosti, pri čemer bi se upoštevali morebitni škodljivi učinki posodobitve na skladnost z varnostnimi zahtevami tega certifikata.

(97) Ko je evropska certifikacijska shema za kibernetsko varnost sprejeta, bi morali proizvajalci ali ponudniki proizvodov IKT, storitev IKT ali postopkov IKT imeti možnost, da vložijo vlogo za certificiranje svojih proizvodov IKT ali storitev IKT pri organu za ugotavljanje skladnosti po lastni izbiri kjer koli v Uniji. Organe za ugotavljanje skladnosti bi moral akreditirati nacionalni akreditacijski organ, če izpolnjujejo nekatere posebne zahteve, določene v tej uredbi. Akreditacija bi morala biti izdana za obdobje največ petih let in bi se morala pod enakimi pogoji podaljšati, če bi organ za ugotavljanje skladnosti še vedno izpolnjeval določene zahteve. Nacionalni akreditacijski organi bi morali omejiti ali začasno oziroma trajno preklicati akreditacijo organa za ugotavljanje skladnosti, če pogoji za akreditacijo niso bili ali niso več izpolnjeni ali kadar organ za ugotavljanje skladnosti krši to uredbo.

(98) Sklici v nacionalni zakonodaji na nacionalne standarde, ki so prenehali učinkovati zaradi začetka veljavnosti evropske certifikacijske sheme za kibernetsko varnost, lahko povzročijo zmedo. Države članice bi morale zato prilagoditi nacionalno zakonodajo, da se upošteva sprejetje evropske certifikacijske sheme za kibernetsko varnost.

(99) Da bi po vsej Uniji vzpostavili enakovredne standarde, da bi olajšali vzajemno priznavanje ter spodbudili splošno sprejemanje evropskih certifikatov kibernetske varnosti in izjav EU o skladnosti, bi bilo treba vzpostaviti sistem medsebojnih strokovnih pregledov med nacionalnimi certifikacijskimi organi za kibernetsko varnost. Medsebojni strokovni pregled bi moral zajemati postopke za nadzor nad skladnostjo proizvodov IKT, storitev IKT in postopkov IKT z evropskimi certifikati kibernetske varnosti, za spremljanje obveznosti proizvajalcev ali ponudnikov proizvodov IKT, storitev IKT ali postopkov IKT, ki opravljajo samoocenjevanje skladnosti, za spremljanje organov za ugotavljanje skladnosti ter ustreznosti strokovnega znanja osebja v organih, ki izdajajo certifikate za „visoko“ raven zanesljivosti. Komisija bi morala imeti možnost z izvedbenimi akti določiti vsaj petletni načrt za medsebojne strokovne preglede ter merila in metodologijo za izvajanje medsebojnih strokovnih pregledov.

(100) Brez poseganja v splošni sistem medsebojnih strokovnih pregledov, ki bi se v certifikacijskem okviru vzpostavil med vsemi nacionalnimi certifikacijskimi organi za kibernetsko varnost, bi lahko nekatere evropske certifikacijske sheme za kibernetsko varnost vključevale mehanizem medsebojnega strokovnega ocenjevanja za organe, ki v okviru takih shem izdajajo evropske certifikate kibernetske varnosti za proizvode IKT, storitve IKT in postopke IKT z „visoko“ ravnjo zanesljivosti. Evropska certifikacijska skupina za kibernetsko varnost bi morala podpirati izvajanje takšnih mehanizmov medsebojnega strokovnega ocenjevanja. Pri medsebojnem strokovnem ocenjevanju bi bilo treba zlasti oceniti, ali zadevni organi svoje naloge izvajajo harmonizirano, mehanizmi pa lahko vključujejo tudi pritožbene mehanizme. Rezultati medsebojnega strokovnega ocenjevanja bi morali biti javno objavljeni. Ti zadevni organi lahko sprejmejo ustrezne ukrepe za ustrezno prilagoditev svojih praks in strokovnega znanja.

(101) Države članice bi morale imenovati enega ali več nacionalnih certifikacijskih organov za kibernetsko varnost, ki bi nadzoroval skladnost z zahtevami iz te uredbe. Nacionalni certifikacijski organ za kibernetsko varnost je lahko obstoječ ali nov organ. Država članica bi poleg tega morala imeti možnost, da po dogovoru z drugo državo članico imenuje enega ali več nacionalnih certifikacijskih organov za kibernetsko varnost na ozemlju te druge države članice.

(102) Nacionalni certifikacijski organi za kibernetsko varnosti bi morali zlasti spremljati in izvrševati obveznosti proizvajalcev oziroma ponudnikov proizvodov IKT, storitev IKT ali postopkov IKT s sedežem na njihovem ozemlju, ki se nanašajo na izjavo EU o skladnosti, nacionalnim akreditacijskim organom pomagati pri spremljanju in nadziranju dejavnosti organov za ugotavljanje skladnosti, tako da bi jim zagotavljali strokovno znanje in potrebne informacije, pooblastiti organe za ugotavljanje skladnosti za izvajanje svojih nalog, kadar taki organi izpolnjujejo dodatne zahteve iz evropske certifikacijske sheme za kibernetsko varnost, in spremljati ustrezni razvoj na področju certificiranja kibernetske varnosti. Nacionalni certifikacijski organi za kibernetsko varnost bi morali tudi obravnavati pritožbe, ki jih vložijo fizične ali pravne osebe glede evropskih certifikatov kibernetske varnosti, ki jih izdajo ti organi, ali glede evropskih certifikatov kibernetske varnosti, ki jih izdajo organi za ugotavljanje skladnosti in se

nanašajo na „visoko“ raven zanesljivosti, v ustreznem obsegu preučiti vsebino pritožbe ter pritožnika v razumnem roku obvestiti o napredku in izidih preiskave. Poleg tega bi morali nacionalni certifikacijski organi za kibernetsko varnost sodelovati z ostalimi nacionalnimi certifikacijskimi organi za kibernetsko varnost ali drugimi javnimi organi, vključno z izmenjavo informacij o morebitni neskladnosti proizvodov IKT, storitev IKT in postopkov IKT z zahtevami iz te uredbe ali z določenimi evropskimi certifikacijskimi shemami za kibernetsko varnost. Komisija bi morala to izmenjavo informacij omogočiti z vzpostavitvijo splošnega elektronskega sistema informacijske podpore, na primer informacijskega in komunikacijskega sistema za nadzor trga (ICSMS) ter sistema hitrega obveščanja o nevarnih neživilskih proizvodih (RAPEX), ki ju organi za nadzor trga že uporabljajo v skladu z Uredbo (ES) št. 765/2008.

(103) Da bi zagotovili dosledno uporabo evropskega certifikacijskega okvira za kibernetsko varnost, bi bilo treba ustanoviti evropsko certifikacijsko skupino za kibernetsko varnost, ki jo sestavljajo predstavniki nacionalnih certifikacijskih organov za kibernetsko varnost ali drugih ustreznih nacionalnih organov. Glavne naloge evropske certifikacijske skupine za kibernetsko varnost 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 ENISA pri pripravi predlog za certifikacijske sheme za kibernetsko varnost, v ustrezno utemeljenih primerih predlagati, da Komisija od agencije ENISA zahteva, naj pripravi predlogo za shemo, in sprejeti mnenja, naslovljena na agencijo ENISA glede predlog za sheme in na Komisijo glede ohranjanja in pregledovanja obstoječih evropskih certifikacijskih shem za kibernetsko varnost. Evropska certifikacijska skupina za kibernetsko varnost bi morala olajšati izmenjavo dobrih praks in strokovnega znanja med različnimi nacionalnimi certifikacijskimi organi za kibernetsko varnost, ki so pristojni za odobritev organov za ugotavljanje skladnosti in izdajanje evropskih certifikatov kibernetske varnosti.

(104) Da bi Komisija okrepila ozaveščenost in olajšala sprejemljivost prihodnjih evropskih certifikacijskih shem za kibernetsko varnost, lahko izda splošne ali sektorske smernice za kibernetsko varnost, na primer o dobrih praksah ali odgovornem ravnanju na področju kibernetske varnosti, pri čemer poudari pozitivni učinek uporabe certificiranih proizvodov IKT, storitev IKT in postopkov IKT.

(105) Glede na globalni značaj dobavnih verig za IKT bi lahko Unija, da bi še bolj olajšala trgovino, v skladu s členom 218 Pogodbe o delovanju Evropske unije (PDEU) sklepala sporazume o vzajemnem priznavanju glede evropskih certifikatov kibernetske varnosti. Komisija lahko ob upoštevanju mnenja agencije ENISA in evropske certifikacijske skupine za kibernetsko varnost priporoči začetek ustreznih pogajanj. Vsaka evropska certifikacijska shema za kibernetsko varnost bi morala določati posebne pogoje za tako vzajemno priznavanje sporazumov s tretjimi državami.

(106) Da bi zagotovili enotne pogoje izvajanja te uredbe, bi bilo treba na Komisijo prenesti izvedbena pooblastila. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta ([22]).

(107) Postopek pregleda bi bilo treba uporabiti za sprejetje izvedbenih aktov o evropskih certifikacijskih shemah za kibernetsko varnost za proizvode IKT, storitve IKT ali postopke IKT, za sprejetje izvedbenih aktov o načinih izvajanja preiskav s strani agencije ENISA, za sprejetje izvedbenih aktov o načrtu medsebojnih strokovnih pregledov nacionalnih certifikacijskih organov za kibernetsko varnost ter za sprejetje izvedbenih aktov o okoliščinah, oblikah in postopkih priglasitve akreditiranih organov za ugotavljanje skladnosti Komisiji s strani nacionalnih certifikacijskih organov za kibernetsko varnost.

(108) Dejavnosti agencije ENISA bi bilo treba redno in neodvisno ocenjevati. Pri tej oceni bi bilo treba upoštevati uspešnost agencije ENISA pri doseganju ciljev, njene delovne prakse in relevantnost njenih nalog, zlasti tistih, ki so povezane z operativnim sodelovanjem na ravni Unije. Oceniti pa bi bilo treba tudi učinek, uspešnost in učinkovitost evropskega certifikacijskega okvira za kibernetsko varnost. V primeru pregleda bi morala Komisija oceniti, kako bi bilo mogoče še utrditi vlogo agencije ENISA kot referenčne točke za svetovanje in strokovno znanje, oceniti pa bi morala tudi možnost vloge agencije ENISA pri podpori ocenjevanju proizvodov IKT, storitev IKT in postopkov IKT, ki vstopajo na trg Unije, vendar ne izpolnjujejo predpisov Unije.

([22]) Uredba (EU) št. 182/2011 Evropskega parlamenta in Sveta z dne 16. februarja 2011 o določitvi splošnih pravil in načel, na podlagi katerih države članice nadzirajo izvajanje izvedbenih pooblastil Komisije (UL L 55, 28.2.2011, str. 13).

(109) Ker ciljev te uredbe države članice ne morejo zadovoljivo doseči, temveč se ti cilji zaradi njenega obsega in učinkov lažje dosežejo na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji (PEU). V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseganje navedenih ciljev.

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

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 določa:

(a) cilje, naloge in organizacijske zadeve, povezane z Agencijo Evropske unije za kibernetsko varnost (v nadaljnjem besedilu: agencija ENISA), ter

(b) okvir za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost za namene zagotavljanja ustrezne ravni kibernetske varnosti za proizvode IKT, storitve IKT in postopke IKT v Uniji, pa tudi za namene preprečevanja razdrobljenosti notranjega trga v zvezi s certifikacijskimi shemami za kibernetsko varnost v Uniji.

Okvir iz točke (b) prvega pododstavka se uporablja brez poseganja v posebne določbe v drugih pravnih aktih Unije glede prostovoljnega ali obveznega certificiranja.

2. Ta uredba ne posega v pristojnosti držav članic v zvezi z dejavnostmi, 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“ pomeni dejavnosti, ki so potrebne za zaščito omrežij in informacijskih sistemov, uporabnikov takih sistemov in drugih oseb, na katere vplivajo kibernetske grožnje;

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

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

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

(5) „ponudnik digitalnih storitev“ pomeni ponudnika digitalnih storitev, kot je opredeljen v točki 6 člena 4 Direktive (EU) 2016/1148;

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

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

(8) „kibernetska grožnja“ pomeni vsako potencialno okoliščino, dogodek ali dejanje, ki bi lahko poškodovalo, prekinilo ali drugače škodljivo vplivalo na omrežja in informacijske sisteme, uporabnike takih sistemov in druge osebe;

(9) „evropska certifikacijska shema za kibernetsko varnost“ pomeni celovit sklop pravil, tehničnih zahtev, standardov in postopkov, ki so vzpostavljeni na ravni Unije in se uporabljajo za certificiranje ali ugotavljanje skladnosti posameznih proizvodov IKT, storitev IKT ali postopkov IKT;

(10) „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 proizvodov IKT, storitev IKT in postopkov IKT, ki spadajo na področje uporabe določene sheme;

(11) „evropski certifikat kibernetske varnosti“ pomeni dokument, ki ga izda ustrezen organ in potrjuje, da je bil zadevni proizvod IKT, storitev IKT ali postopek IKT ocenjen glede skladnosti s posebnimi varnostnimi zahtevami, določenimi v evropski certifikacijski shemi za kibernetsko varnost;

(12) „proizvod IKT“ pomeni element ali skupino elementov omrežja ali informacijskega sistema;

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

(14) „postopek IKT“ pomeni sklop dejavnosti, ki se izvaja za zasnovo, razvoj, dobavo ali vzdrževanje proizvoda IKT ali storitve IKT;

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

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

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

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

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

(20) „tehnična specifikacija“ pomeni dokument, ki določa tehnične zahteve, ki jih mora izpolnjevati proizvod IKT, storitev IKT ali postopek IKT, ali postopke ugotavljanja skladnosti v zvezi s proizvodom IKT, storitvijo IKT ali postopkom IKT;

(21) „raven zanesljivosti“ pomeni podlago za zaupanje, da proizvod IKT, storitev IKT ali postopek IKT izpolnjuje varnostne zahteve določene evropske certifikacijske sheme za kibernetsko varnost, navaja pa tudi raven, na kateri je bil proizvod IKT, storitev IKT ali postopek IKT ocenjen, vendar kot taka ne meri varnosti zadevnega proizvoda IKT, storitve IKT ali postopka IKT;

(22) „samoocenjevanje skladnosti“ pomeni dejavnost proizvajalca ali ponudnika proizvodov IKT, storitev IKT ali postopkov IKT s katero se oceni, ali ti proizvodi IKT, storitve IKT ali postopki IKT izpolnjujejo zahteve iz določene evropske certifikacijske sheme za kibernetsko varnost.

NASLOV II

**Agencija ENISA**

*POGLAVJE I*

***Mandat in cilji***

*Člen 3*

**Mandat**

1. Agencija ENISA opravlja naloge, ki so ji dodeljene na podlagi te uredbe, da bi se dosegla visoka skupna raven kibernetske varnosti v vsej Uniji, vključno z dejavnim podpiranjem držav članic ter institucij, organov, uradov in agencij Unije za izboljšanje kibernetske varnosti. Agencija ENISA deluje kot referenčna točka za svetovanje in strokovno znanje v zvezi s kibernetsko varnostjo za institucije, organe, urade in agencije Unije ter za druge ustrezne deležnike Unije.

Agencija ENISA z opravljanjem nalog, ki so ji dodeljene na podlagi te uredbe, prispeva k zmanjšanju razdrobljenosti notranjega trga.

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

3. Agencija ENISA pri opravljanju svojih nalog deluje neodvisno, pri tem pa se izogiba podvajanju dejavnosti držav članic in upošteva že obstoječe strokovno znanje držav članic.

4. Agencija ENISA pridobi lastne vire, vključno s tehničnimi zmogljivostmi ter človeškimi sposobnostmi in veščinami, potrebnimi za opravljanje nalog, ki so ji dodeljene s to uredbo.

*Člen 4*

**Cilji**

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

2. Agencija ENISA institucijam, organom, uradom in agencijam 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 ENISA podpira krepitev zmogljivosti in pripravljenosti v vsej Uniji, tako da institucijam, organom, uradom in agencijam 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 znanja in spretnosti na področju kibernetske varnosti.

4. Agencija ENISA pri vprašanjih, ki se nanašajo na kibernetsko varnost, spodbuja sodelovanje, vključno z izmenjavo informacij, in usklajevanje na ravni Unije med državami članicami, institucijami, organi, uradi in agencijami Unije ter ustreznimi zasebnimi in javnimi deležniki.

5. Agencija ENISA prispeva h krepitvi zmogljivosti na področju kibernetske varnosti na ravni Unije, da bi podprla dejavnosti držav članic pri preprečevanju kibernetskih groženj in odzivanju nanje, zlasti v primeru čezmejnih incidentov.

6. Agencija ENISA spodbuja uporabo evropskega certificiranja na področju kibernetske varnosti, da se prepreči razdrobljenost notranjega trga. Agencija ENISA prispeva k vzpostavitvi in vzdrževanju evropskega certifikacijskega okvira za kibernetsko varnost v skladu z naslovom III te uredbe, da bi se izboljšala preglednost kibernetske varnosti proizvodov IKT, storitev IKT in postopkov IKT ter s tem okrepila zaupanje v digitalni notranji trg in njegova konkurenčnost.

7. Agencija ENISA spodbuja visoko raven ozaveščenosti o kibernetski varnosti, vključno s kibernetsko higieno in kibernetsko pismenostjo med državljani, organizacijami in podjetji.

*POGLAVJE II*

***Naloge***

*Člen 5*

**Oblikovanje in izvajanje politike in prava Unije**

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

(1) pomočjo in svetovanjem glede oblikovanja in pregleda politike in prava Unije na področju kibernetske varnosti ter glede sektorske politike in pravnih pobud, kadar gre za zadeve, povezane s kibernetsko varnostjo, zlasti z zagotavljanjem neodvisnega mnenja in analize ter z izvajanjem pripravljalnega dela;

(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 izdajo mnenj, smernic, svetovanjem in najboljšimi praksami na področjih, kot so obvladovanje tveganj, poročanje o incidentih in izmenjava informacij, ter z omogočanjem lažje izmenjave najboljših praks med pristojnimi organi v zvezi s tem;

(3) pomočjo državam članicam ter institucijam, organom, uradom in agencijam Unije pri oblikovanju in spodbujanju politik kibernetske varnosti, povezanih z ohranjanjem splošne dostopnosti oziroma celovitosti javnega jedra odprtega interneta;

(4) prispevanjem k delu skupine za sodelovanje na podlagi člena 11 Direktive (EU) 2016/1148, in sicer z zagotavljanjem strokovnega znanja in pomoči;

(5) podporo:

(a) oblikovanju in izvajanju politike Unije na področju elektronske identifikacije in storitev zaupanja, zlasti z zagotavljanjem svetovanja in izdajo tehničnih smernic, ter z omogočanjem lažje izmenjave najboljših praks med pristojnimi organi;

(b) spodbujanju višje ravni varnosti elektronskih komunikacij, vključno z zagotavljanjem svetovanja in strokovnega znanja, ter z omogočanjem lažje izmenjave najboljših praks med pristojnimi organi;

(c) državam članicam pri izvajanju posebnih vidikov kibernetske varnosti v okviru politike in prava Unije v zvezi z varstvom podatkov in zasebnostjo, vključno s svetovanjem Evropskemu odboru za varstvo podatkov na njegovo zahtevo;

(6) podpiranjem rednega pregleda dejavnosti politike Unije s pripravo letnega poročila o stanju izvajanja zadevnega pravnega okvira glede:

(a) informacij o priglasitvah incidentov s strani držav članic, ki jih skupini za sodelovanje zagotovijo enotne kontaktne točke na podlagi člena 10(3) Direktive (EU) 2016/1148;

(b) povzetkov uradnih obvestil o kršitvi varnosti ali izgubi celovitosti, prejetih od ponudnikov storitev zaupanja, ki jih agenciji ENISA zagotovijo nadzorni organi na podlagi člena 19(3) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta ([23]);

(c) uradnih obvestil o varnostnih incidentih, ki jih pošljejo ponudniki javnih elektronskih komunikacijskih omrežij ali javno dostopnih elektronskih komunikacijskih storitev, agenciji ENISA pa jih predložijo pristojni organi na podlagi člena 40 Direktive (EU) 2018/1972.

([23]) Uredba (EU) št. 910/2014 Evropskega parlamenta in Sveta z dne 23. julija 2014 o elektronski identifikaciji in storitvah zaupanja za elektronske transakcije na notranjem trgu in o razveljavitvi Direktive 1999/93/ES (UL L 257, 28.8.2014, str. 73).

*Člen 6*

**Krepitev zmogljivosti**

1. Agencija ENISA pomaga:

(a) državam članicam pri njihovih prizadevanjih za izboljšanje preprečevanja, odkrivanja in analiziranja kibernetskih groženj in incidentov ter zmogljivosti odzivanja nanje, tako da jim zagotavlja potrebno strokovno znanje in izkušnje;

(b) državam članicam ter institucijam, organom, uradom in agencijam Unije pri vzpostavljanju in izvajanju politik razkrivanja šibkih točk na prostovoljni podlagi;

(c) institucijam, organom, uradom in agencijam Unije pri njihovih prizadevanjih za izboljšanje preprečevanja, odkrivanja in analiziranja kibernetskih groženj in incidentov ter izboljšanje zmogljivosti odzivanja na take kibernetske grožnje in incidente, zlasti z ustrezno podporo skupini CERT-EU;

(d) državam članicam pri oblikovanju nacionalnih skupin CSIRT, kadar za to zaprosijo na podlagi člena 9(5) Direktive (EU) 2016/1148;

(e) državam članicam pri oblikovanju nacionalnih strategij za varnost omrežij in informacijskih sistemov, kadar za to zaprosijo na podlagi člena 7(2) Direktive (EU) 2016/1148, ter spodbuja razširjanje teh strategij in se seznanja z napredkom pri njihovem izvajanju po vsej Uniji, da bi spodbujala najboljše prakse;

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

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

(h) državam članicam z rednim organiziranjem vaj na področju kibernetske varnosti na ravni Unije iz člena 7(5) vsaj na vsaki dve leti in z oblikovanjem političnih priporočil, ki temeljijo na postopku ocenjevanja vaj in izkušnjah, pridobljenih z njimi;

(i) ustreznim javnim organom z zagotavljanjem usposabljanja na področju kibernetske varnosti, po potrebi v sodelovanju z deležniki;

(j) skupini za sodelovanje pri izmenjavi najboljših praks, zlasti glede določitve izvajalcev bistvenih storitev s strani držav članic na podlagi točke (l) člena 11(3) Direktive (EU) 2016/1148,vključno glede čezmejnih odvisnosti v zvezi s tveganji in incidenti.

2. Agencija ENISA 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 navodil v zvezi z razpoložljivimi orodji in postopki ter glede tega, kako obravnavati regulativna vprašanja, povezana z izmenjavo informacij.

*Člen 7*

**Operativno sodelovanje na ravni Unije**

1. Agencija ENISA podpira operativno sodelovanje med državami članicami ter institucijami, organi, uradi in agencijami Unije ter med deležniki.

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

(a) izmenjavo strokovnega znanja in najboljših praks;

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

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

3. Agencija ENISA zagotovi sekretariat mreže skupin CSIRT na podlagi člena 12(2) Direktive (EU) 2016/1148 ter v tej funkciji dejavno podpira izmenjavo informacij in sodelovanje med njenimi člani.

4. Agencija ENISA podpira države članice v zvezi z operativnim sodelovanjem v mreži skupin CSIRT, in sicer s:

(a) svetovanjem o načinih za izboljšanje njihovih zmogljivosti za preprečevanje in odkrivanje incidentov ter odzivanje nanje, na zahtevo ene ali več držav članic pa tudi s svetovanjem v zvezi s specifično kibernetsko grožnjo;

(b) pomočjo, na zahtevo ene ali več držav članic, pri ocenjevanju incidentov, ki imajo pomembne ali znatne posledice, z zagotavljanjem strokovnega znanja in omogočanjem lažjega tehničnega obvladovanja takih incidentov, med drugim zlasti s podpiranjem prostovoljne izmenjave zadevnih informacij in tehničnih rešitev med državami članicami;

(c) analiziranjem šibkih točk in incidentov na podlagi javno dostopnih informacij ali informacij, ki jih v ta namen prostovoljno sporočijo države članice, ter

(d) zagotavljanjem podpore, na zahtevo ene ali več držav članic, v zvezi z naknadnimi tehničnimi preiskavami incidentov, ki imajo pomembne ali znatne posledice, v smislu Direktive (EU) 2016/1148.

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

5. Agencija ENISA redno organizira vaje na področju kibernetske varnosti na ravni Unije ter države članice in institucije, organe, urade in agencije Unije podpira pri organiziranju vaj na področju kibernetske varnosti na podlagi njihovih zahtev. Takšne vaje na področju kibernetske varnosti na ravni Unije lahko vključujejo tehnične, operativne ali strateške elemente. Agencija ENISA vsaj na vsaki dve leti organizira obsežno vsestransko vajo.

Po potrebi agencija ENISA prispeva tudi k sektorskim vajam na področju kibernetske varnosti in jih pomaga organizirati skupaj z ustreznimi organizacijami, ki prav tako sodelujejo pri vajah na področju kibernetske varnosti na ravni Unije.

6. Agencija ENISA v tesnem sodelovanju z državami članicami pripravi redno poglobljeno tehnično poročilo o stanju na področju kibernetske varnosti v EU glede incidentov in kibernetskih groženj, in sicer na podlagi javno dostopnih informacij, lastne analize in poročil, ki jih med drugim predložijo skupine CSIRT držav članic ali enotne kontaktne točke, vzpostavljene z Direktivo (EU) 2016/1148, v obeh primerih na prostovoljni podlagi, EC3 ter skupine CERT-EU.

7. Agencija ENISA 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 in analiziranjem poročil iz nacionalnih virov, ki so dostopna javnosti ali so bila prostovoljno dana v skupno rabo, da bi prispevala k vzpostavitvi skupnega situacijskega zavedanja;

(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, tehničnega obravnavanja takih incidentov ali kriz, vključno zlasti s podpiranjem prostovoljne izmenjave tehničnih rešitev med državami članicami;

(d) podpiranjem institucij, organov, uradov in agencij Unije, na njihovo zahtevo pa tudi držav članic, pri komuniciranju z javnostjo v zvezi s takimi incidenti ali krizami;

(e) preskušanjem načrtov za sodelovanje za odzivanje na take incidente ali krize na ravni Unije, na zahtevo pa tudi podpiranjem držav članic pri preskušanju takih načrtov na nacionalni ravni.

*Člen 8*

**Trg, certificiranje kibernetske varnosti in standardizacija**

1. Agencija ENISA podpira in spodbuja oblikovanje in izvajanje politike Unije o certificiranju proizvodov IKT, storitev IKT in postopkov IKT glede kibernetske varnosti, kot je določeno v naslovu III te uredbe, in sicer s:

(a) stalnim spremljanjem razvoja na področjih, povezanih s standardizacijo, in dajanjem priporočil glede ustreznih tehničnih specifikacij, namenjenih razvoju evropske certifikacijske sheme za kibernetsko varnost na podlagi točke (c) člena 54(1), kadar standardi niso na voljo;

(b) pripravo predlog za evropske certifikacijske sheme za kibernetsko varnost (v nadaljnjem besedilu: predloge za sheme) za proizvode IKT, storitve IKT in postopke IKT v skladu s členom 49;

(c) ocenjevanjem sprejetih evropskih certifikacijskih shem za kibernetsko varnost v skladu s členom 49(8);

(d) sodelovanjem pri medsebojnih strokovnih pregledih na podlagi člena 59(4);

(e) podporo Komisiji pri zagotavljanju sekretariata evropski certifikacijski skupini za kibernetsko varnost na podlagi člena 62(5).

2. Agencija ENISA zagotovi sekretariat certifikacijski skupini deležnikov za kibernetsko varnost na podlagi člena 22(4).

3. Agencija ENISA pripravi in objavi smernice ter razvije dobre prakse glede zahtev na področju kibernetske varnosti za proizvode IKT, storitve IKT in postopke IKT v sodelovanju z nacionalnimi certifikacijskimi organi za kibernetsko varnost in industrijo na formalen, strukturiran in pregleden način.

4. Agencija ENISA podpira krepitev zmogljivosti v zvezi s postopki ocenjevanja in certificiranja, tako da pripravi in izda smernice, ter s podpiranjem držav članic na njihovo zahtevo.

5. Agencija ENISA omogoča lažjo vzpostavitev in uvedbo evropskih in mednarodnih standardov za obvladovanje tveganja in za varnost proizvodov IKT, storitev IKT in postopkov IKT.

6. Agencija ENISA v sodelovanju z državami članicami in industrijo 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, na podlagi člena 19(2) Direktive (EU) 2016/1148.

7. Agencija ENISA 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 ENISA:

(a) izvaja analize nastajajočih tehnologij 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 incidentov;

(c) v sodelovanju s strokovnjaki iz organov držav članic in ustreznimi deležniki zagotavlja svetovanje, navodila in najboljše prakse za varnost omrežij in informacijskih sistemov, zlasti za varnost infrastruktur, ki podpirajo sektorje, navedene v Prilogi II k Direktivi (EU) 2016/1148, in infrastruktur, ki jih uporabljajo ponudniki digitalnih storitev, navedeni v Prilogi III k navedeni direktivi;

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

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

*Člen 10*

**Ozaveščanje in izobraževanje**

Agencija ENISA:

(a) javnost ozavešča o tveganjih za kibernetsko varnost in zagotavlja navodila o dobrih praksah za posamezne uporabnike, ki so namenjene državljanom, organizacijam in podjetjem, vključno s kibernetsko higieno in kibernetsko pismenostjo;

(b) v sodelovanju z državami članicami, institucijami, organi, uradi in agencijami Unije ter industrijo organizira redne kampanje ozaveščanja za izboljšanje kibernetske varnosti in njene prepoznavnosti v Uniji ter spodbuja široko javno razpravo;

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

(d) podpira tesnejše usklajevanje in izmenjavo najboljših praks med državami članicami na področju ozaveščenosti o kibernetski varnosti in izobraževanja.

*Člen 11*

**Raziskave in inovacije**

Agencija ENISA v zvezi z raziskavami in inovacijami:

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

(b) sodeluje v fazi izvajanja programov za financiranje raziskav in inovacij ali kot upravičenec, kadar je Komisija nanjo prenesla ustrezna pooblastila;

(c) prispeva k strateškemu načrtu raziskav in inovacij na ravni Unije na področju kibernetske varnosti.

*Člen 12*

**Mednarodno sodelovanje**

Agencija ENISA prispeva k prizadevanjem Unije za sodelovanje s tretjimi državami in mednarodnimi organizacijami, pa tudi znotraj ustreznih mednarodnih okvirov sodelovanja, ter tako spodbuja mednarodno sodelovanje o zadevah, ki se nanašajo na kibernetsko varnost, in sicer s:

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

(b) olajševanjem izmenjave najboljših praks, na zahtevo Komisije;

(c) zagotavljanjem strokovnega znanja Komisiji na njeno zahtevo;

(d) svetovanjem in pomočjo Komisiji pri zadevah, povezanih s sporazumi o vzajemnem priznavanju certifikatov kibernetske varnosti s tretjimi državami, v sodelovanju z evropsko certifikacijsko skupino za kibernetsko varnost, ustanovljeno na podlagi člena 62.

*POGLAVJE III*

***Organizacija agencije ENISA***

*Člen 13*

**Struktura agencije ENISA**

Upravno in vodstveno strukturo agencije ENISA sestavljajo:

(a) upravni odbor;

(b) izvršni odbor;

(c) izvršni direktor;

(d) svetovalna skupina agencije ENISA;

(e) mreža nacionalnih uradnikov za zvezo.

Oddelek 1

**Upravni odbor**

*Člen 14*

**Sestava upravnega odbora**

1. Upravni odbor sestavljajo po en član, ki ga imenuje vsaka država članica, ter dva člana, ki ju imenuje Komisija. Vsi člani imajo glasovalno pravico.

2. Vsak član upravnega odbora ima namestnika. Ta člana predstavlja 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 upravnega 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 15*

**Funkcije upravnega odbora**

1. Upravni odbor:

(a) oblikuje splošno usmeritev delovanja agencije ENISA in zagotavlja, da agencija ENISA deluje v skladu s pravili in načeli iz te uredbe. Prav tako zagotovi, da je delo agencije ENISA v skladu z dejavnostmi držav članic in dejavnostmi na ravni Unije;

(b) sprejme osnutek enotnega programskega dokumenta agencije ENISA iz člena 24, preden ga predloži Komisiji, ki o njem poda mnenje;

(c) sprejme enotni programski dokument agencije ENISA, pri čemer upošteva mnenje Komisije;

(d) nadzira izvajanje večletnega in letnega programa dejavnosti, vključenega v enotni programski dokument;

(e) sprejme letni proračun agencije ENISA in izvaja druge funkcije, povezane s proračunom agencije ENISA, v skladu s poglavjem IV;

(f) oceni in sprejme konsolidirano letno poročilo o dejavnostih agencije ENISA, vključno z zaključnim računom in opisom, kako je agencija ENISA dosegla svoje kazalnike uspešnosti, letno poročilo in njegovo oceno do 1. julija naslednjega leta predloži Evropskemu parlamentu, Svetu, Komisiji in Računskemu sodišču ter objavi letno poročilo;

(g) sprejme finančna pravila, ki se uporabljajo za agencijo ENISA v skladu s členom 32;

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

(i) sprejme pravila za preprečevanje in upravljanje nasprotij interesov, ki se uporabljajo za njegove člane;

(j) 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;

(k) sprejme svoj poslovnik, vključno s pravili za začasne odločitve o prenosu posameznih nalog v skladu s členom 19(7);

(l) v zvezi z osebjem agencije ENISA izvaja pooblastila, ki jih Kadrovski predpisi za uradnike (v nadaljnjem besedilu: Kadrovski predpisi za uradnike) in Pogoji za zaposlitev drugih uslužbencev Evropske unije (v nadaljnjem besedilu: Pogoji za zaposlitev drugih uslužbencev), določeni v Uredbi Sveta (EGS, Euratom, ESPJ) št. 259/68 ([24]) podeljujejo organu za imenovanja in organu, pooblaščenemu za sklenitev pogodbe o zaposlitvi (v nadaljnjem besedilu: pooblastila organa za imenovanja) v skladu z odstavkom 2 tega člena;

(m) sprejme izvedbena pravila za Kadrovske predpise za uradnike in Pogoje za zaposlitev drugih uslužbencev v skladu s postopkom iz člena 110 Kadrovskih predpisov za uradnike;

(n) imenuje izvršnega direktorja in po potrebi podaljša njegov mandat ali ga razreši s položaja v skladu s členom 36;

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

(p) sprejme vse odločitve glede vzpostavitve notranjih struktur agencije ENISA in po potrebi sprememb teh notranjih struktur, pri čemer upošteva potrebe pri dejavnostih agencije ENISA in dobro proračunsko upravljanje;

(q) odobri vzpostavitev delovnih dogovorov v skladu s členom 7;

(r) odobri vzpostavitev ali sklenitev delovnih dogovorov v skladu s členom 42.

2. Upravni odbor v skladu s členom 110 Kadrovskih predpisov ter na podlagi člena 2(1) Kadrovskih predpisov za uradnike in člena 6 Pogojev za zaposlitev drugih uslužbencev sprejme odločitev o prenosu ustreznih pooblastil organa za imenovanja na izvršnega direktorja in določitvi pogojev, pod katerimi se lahko ta prenos pooblastil začasno prekliče. Izvršni direktor lahko nadalje prenese ta pooblastila.

([24]) UL L 56, 4.3.1968, str. 1.

3. Zaradi izjemnih okoliščin lahko upravni odbor sprejme odločitev o začasnem preklicu prenosa pooblastil organa za imenovanja na izvršnega direktorja in njegovega morebitnega nadaljnjega prenosa pooblastil organa za imenovanja ter jih namesto tega izvaja sam ali jih prenese na enega od svojih članov ali uslužbenca, ki ni izvršni direktor.

*Člen 16*

**Predsednik upravnega odbora**

Upravni odbor izmed članov izvoli predsednika in njegovega namestnika z dvotretjinsko večino glasov članov. Njun mandat traja štiri leta z možnostjo enkratnega podaljšanja. Če njuno članstvo v upravnem odboru preneha kadar koli 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 17*

**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 svojih članov se sestane tudi na izrednih sejah.

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

4. Člani svetovalne skupine agencije ENISA lahko na povabilo predsednika sodelujejo na sejah upravnega odbora, vendar nimajo glasovalne pravice.

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

6. Agencija ENISA upravnemu odboru zagotovi sekretariat.

*Člen 18*

**Pravila glasovanja v upravnem odboru**

1. Upravni odbor sprejema odločitve z večino svojih članov.

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

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

4. Predsednik upravnega odbora se udeleži glasovanja.

5. Izvršni direktor se glasovanja ne udeleži.

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

Oddelek 2

## Izvršni odbor

*Člen 19*

### 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 ustrezne nadaljnje ukrepe v zvezi z ugotovitvami in priporočili na podlagi preiskav urada OLAF ter različnih notranjih ali zunanjih revizijskih poročil in ocen;

(c) brez poseganja v odgovornosti izvršnega direktorja iz člena 20 pomaga in svetuje izvršnemu direktorju pri izvajanju odločitev upravnega odbora o upravnih in proračunskih zadevah na podlagi člena 20.

3. Izvršni odbor sestavlja pet članov. Ti so imenovani izmed članov upravnega odbora. Eden od članov je predsednik upravnega odbora, ki lahko predseduje tudi izvršnemu odboru, eden od članov pa je predstavnik Komisije. Pri imenovanju članov izvršnega odbora se prizadeva zagotoviti uravnoteženo zastopanost spolov v izvršnem odboru. Izvršni direktor se udeležuje sej izvršnega odbora, vendar nima glasovalne pravice.

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

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

6. Upravni odbor določi poslovnik izvršnega odbora.

7. Izvršni odbor lahko po potrebi in v nujnih primerih sprejme določene začasne odločitve v imenu upravnega odbora, zlasti o zadevah v zvezi z upravnim poslovodenjem, vključno z začasnim preklicem prenosa pooblastil organa za imenovanja in proračunskimi zadevami. Vse takšne začasne odločitve se brez nepotrebnega odlašanja sporočijo upravnemu odboru. Upravni odbor se potem odloči, ali odobri oziroma zavrne začasno odločitev, najpozneje tri mesece po sprejetju odločitve. Izvršni odbor v imenu upravnega odbora ne sprejema odločitev, za sprejetje katerih je potrebna dvotretjinska večina članov upravnega odbora.

Oddelek 3

## Izvršni direktor

*Člen 20*

### Dolžnosti izvršnega direktorja

1. Agencijo ENISA upravlja izvršni direktor, ki svoje dolžnosti opravlja neodvisno. Izvršni direktor odgovarja upravnemu odboru.

2. Izvršni direktor na poziv 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 ENISA;

(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 ENISA, 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 urada OLAF ter poročanje o napredku, in sicer Komisiji dvakrat letno, upravnemu odboru pa redno;

(h) pripravo osnutka finančnih pravil, ki se uporabljajo za agencijo ENISA iz člena 32;

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

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

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

(l) vzpostavljanje in ohranjanje stika s poslovno skupnostjo in potrošniškimi organizacijami za zagotavljanje rednega dialoga z ustreznimi deležniki;

(m) redno izmenjavo mnenj in informacij z institucijami, organi, uradi in agencijami Unije v zvezi z njihovimi dejavnostmi, povezanimi s kibernetsko varnostjo, da se zagotovi skladnost pri razvoju in izvajanju politike Unije;

(n) izvajanje drugih nalog, ki so izvršnemu direktorju dodeljene s to uredbo.

4. Izvršni direktor lahko po potrebi ter v okviru s cilji in nalogami agencije ENISA ustanovi *ad hoc* delovne skupine, ki jih sestavljajo strokovnjaki, vključno s strokovnjaki iz pristojnih organov držav članic. Izvršni direktor o tem vnaprej obvesti upravni odbor. Postopki, ki se nanašajo zlasti na sestavo delovnih skupin, imenovanje strokovnjakov delovnih skupin s strani izvršnega direktorja in delovanje delovnih skupin, se določijo v statutu agencije ENISA.

5. Izvršni direktor lahko za učinkovito in uspešno izvajanje nalog agencije ENISA ter na podlagi ustrezne analize stroškov in koristi po potrebi odloči, da se ustanovi 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 ENISA, 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. Skupno število zaposlenih v vseh lokalnih uradih mora biti čim manjše in ne sme presegati 40 % skupnega števila osebja agencije ENISA v državi članici, v kateri je sedež agencije ENISA. Število zaposlenih v posameznem lokalnem uradu ne sme presegati 10 % skupnega števila osebja agencije ENISA v državi članici, v kateri je sedež agencije ENISA.

Z odločitvijo o ustanovitvi lokalnega urada se določi obseg dejavnosti, ki naj bi se izvajale v zadevnem lokalnem uradu, in sicer tako, da se preprečijo nepotrebni stroški in podvajanje upravnih funkcij agencije ENISA.

Oddelek 4

## Svetovalna skupina agencije ENISA, certifikacijska skupina deležnikov za kibernetsko varnost in mreža nacionalnih uradnikov za zvezo

*Člen 21*

### Svetovalna skupina agencije ENISA

1. Na predlog izvršnega direktorja upravni odbor na pregleden način ustanovi svetovalno skupino agencije ENISA, ki jo sestavljajo priznani strokovnjaki, ki zastopajo ustrezne deležnike, kot so predstavniki industrije IKT, ponudniki elektronskih komunikacijskih omrežij ali storitev, dostopnih javnosti, MSP, izvajalci bistvenih storitev, skupine potrošnikov, znanstveniki s področja kibernetske varnosti in predstavniki pristojnih organov, ki so uradno obveščeni v skladu z Direktivo (EU) 2018/1972, evropske organizacije za standardizacijo ter organi za preprečevanje, odkrivanje in preiskovanje kaznivih dejanj ter nadzorni organi za varstvo podatkov. Upravni odbor si prizadeva zagotoviti uravnoteženo zastopanost spolov in geografskih območij, pa tudi ravnovesje med različnimi skupinami deležnikov.

2. Postopki svetovalne skupine agencije ENISA, ki se nanašajo zlasti na njeno sestavo, predlog s strani izvršnega direktorja iz odstavka 1, število in imenovanje njenih članov ter delovanje svetovalne skupine ENISA, se določijo v statutu agencije ENISA in objavijo.

3. Svetovalni skupini agencije ENISA predseduje izvršni direktor ali katera koli oseba, ki jo izvršni direktor imenuje za vsak primer posebej.

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

5. Svetovalna skupina agencije ENISA svetuje agenciji ENISA v zvezi z opravljanjem njenih nalog, razen glede uporabe določb naslova III te uredbe. Zlasti svetuje izvršnemu direktorju pri pripravi predloga letnega delovnega programa agencije ENISA in pri komuniciranju z ustreznimi deležniki o zadevah, ki se nanašajo na letni delovni program.

6. Svetovalna skupina agencije ENISA o svojih dejavnostih redno obvešča upravni odbor.

*Člen 22*

### Certifikacijska skupina deležnikov za kibernetsko varnost

1. Ustanovi se certifikacijska skupina deležnikov za kibernetsko varnost.

2. Certifikacijsko skupino deležnikov za kibernetsko varnost sestavljajo člani, izbrani izmed priznanih strokovnjakov, ki zastopajo ustrezne deležnike. Komisija člane certifikacijske skupine deležnikov za kibernetsko varnost izbere na predlog agencije ENISA prek preglednega in odprtega razpisa, pri čemer zagotovi ravnovesje med različnimi skupinami deležnikov ter uravnoteženo zastopanost spolov in geografskih območij.

3. Certifikacijska skupina deležnikov za kibernetsko varnost:

(a) svetuje Komisiji glede strateških vprašanj v zvezi z evropskim certifikacijskim okvirom za kibernetsko varnost;

(b) agenciji ENISA na zahtevo svetuje glede splošnih in strateških vprašanj v zvezi z nalogami agencije ENISA, ki se nanašajo na trg, certificiranje kibernetske varnosti in standardizacijo;

(c) Komisiji pomaga pri pripravi tekočega delovnega programa Unije iz člena 47;

(d) izda mnenje o tekočem delovnem programu Unije na podlagi člena 47(4) in

(e) v nujnih primerih svetuje Komisiji in evropski certifikacijski skupini za kibernetsko varnost glede potrebe po dodatnih certifikacijskih shemah, ki niso vključene v tekoči delovni program Unije, kot je navedeno v členih 47 in 48.

4. Certifikacijski skupini deležnikov sopredsedujeta predstavnika Komisije in agencije ENISA, sekretariat pa zagotovi agencija ENISA.

*Člen 23*

**Mreža nacionalnih uradnikov za zvezo**

1. Upravni odbor na predlog izvršnega direktorja ustanovi mrežo nacionalnih uradnikov za zvezo, ki jo sestavljajo predstavniki vseh držav članic (v nadaljnjem besedilu: nacionalni uradniki za zvezo). Vsaka država članica imenuje enega predstavnika v mrežo nacionalnih uradnikov za zvezo. Sestanki mreže nacionalnih uradnikov za zvezo lahko potekajo v različnih sestavah strokovnjakov.

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

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

4. Medtem ko nacionalni uradniki za zvezo tesno sodelujejo s predstavniki svojih držav članic v upravnem odboru, pa mreža nacionalnih uradnikov za zvezo sama ne podvaja dela upravnega odbora ali drugih forumov Unije.

5. Funkcije in postopki mreže nacionalnih uradnikov za zvezo se določijo v statutu agencije ENISA in se objavijo.

Oddelek 5

**Delovanje**

*Člen 24*

**Enotni programski dokument**

1. Agencija ENISA deluje v skladu z enotnim programskim dokumentom, ki zajema letni in večletni program dejavnosti ter vsebuje vse načrtovane dejavnosti.

2. Izvršni direktor vsako leto pripravi osnutek enotnega programskega dokumenta, ki zajema letni in večletni program dejavnosti ter ustrezno načrtovanje finančnih in človeških virov v skladu s členom 32 Delegirane uredbe Komisije (EU) št. 1271/2013 ([25]), pri čemer upošteva smernice Komisije.

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

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

([25]) 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).

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

6. Upravni odbor spremeni sprejeti letni delovni program, kadar se agenciji ENISA dodeli nova naloga. Vse bistvene spremembe letnega delovnega programa se sprejmejo 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, 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 67.

*Člen 25*

**Izjava o interesih**

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

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

*Člen 26*

**Preglednost**

1. Agencija ENISA svoje dejavnosti izvaja z visoko stopnjo preglednosti in v skladu s členom 28.

2. Agencija ENISA zagotovi, da javnost in vse zainteresirane strani dobijo ustrezne, objektivne, zanesljive in lahko dostopne informacije, zlasti glede rezultatov njenega dela. Objavi tudi izjave o interesih, ki so bile podane v skladu s členom 25.

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

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

*Člen 27*

**Zaupnost**

1. Brez poseganja v člen 28 Agencija ENISA tretjim stranem ne razkrije informacij, ki jih obdeluje ali prejme in v zvezi s katerimi je bilo z obrazložitvijo zahtevano, da se z njimi ravna zaupno.

2. Člani upravnega odbora, izvršni direktor, člani svetovalne skupine agencije ENISA, zunanji strokovnjaki, ki sodelujejo v *ad hoc* delovnih skupinah, in osebje agencije ENISA, vključno z iz držav članic začasno napoteni uradniki, upoštevajo zahteve glede zaupnosti v skladu s členom 339 PDEU tudi po prenehanju opravljanja svojih dolžnosti.

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

4. Upravni odbor agenciji ENISA dovoli, da ravna z zaupnimi informacijami, če je to potrebno za izvajanje nalog agencije ENISA. V tem primeru agencija ENISA v soglasju s Komisijo sprejme varnostna pravila, pri čemer upošteva varnostna načela iz sklepov Komisije (EU, Euratom) 2015/443 ([26]) in 2015/444 ([27]). Navedena varnostna pravila vključujejo določbe za izmenjavo, obdelavo in hrambo tajnih podatkov.

*Člen 28*

**Dostop do dokumentov**

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

2. Upravni odbor do 28. decembra 2019 sprejme ureditev za izvajanje Uredbe (ES) št. 1049/2001.

3. Zoper odločitve, ki jih agencija ENISA sprejme na podlagi člena 8 Uredbe (ES) št. 1049/2001, je v skladu s členom 228 PDEU možna pritožba pri Evropskem varuhu človekovih pravic ali tožba pred Sodiščem Evropske unije v skladu s členom 263 PDEU.

*POGLAVJE IV*

***Določitev in sestava proračuna agencije ENISA***

*Člen 29*

**Določitev proračuna agencije ENISA**

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

2. Upravni odbor vsako leto na podlagi osnutka poročila o oceni pripravi poročilo o oceni prihodkov in odhodkov agencije ENISA za naslednje proračunsko leto.

3. Upravni odbor vsako leto do 31. januarja pošlje poročilo o oceni, ki je del osnutka enotnega programskega dokumenta, Komisiji in tretjim državam, s katerimi je Unija sklenila sporazume, kot je določeno v členu 42(2).

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

5. Evropski parlament in Svet odobrita proračunska sredstva za prispevek Unije, namenjen agenciji ENISA.

6. Evropski parlament in Svet sprejmeta kadrovski načrt agencije ENISA.

([26]) Sklep Komisije (EU, Euratom) 2015/443 z dne 13. marca 2015 o varnosti v Komisiji (UL L 72, 17.3.2015, str. 41).
([27]) 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).

7. Upravni odbor sprejme proračun agencije ENISA skupaj z enotnim programskim dokumentom. Proračun agencije ENISA je dokončen po dokončnem sprejetju splošnega proračuna Unije. Upravni odbor po potrebi prilagodi proračun in enotni programski dokument agencije ENISA v skladu s splošnim proračunom Unije.

*Člen 30*

**Sestava proračuna agencije ENISA**

1. Prihodki agencije ENISA brez poseganja v druge vire zajemajo:

(a) prispevek iz splošnega proračuna Unije;

(b) prihodke, dodeljene za posebne odhodkovne postavke v skladu z njenimi finančnimi pravili iz člena 32;

(c) sredstva Unije v obliki sporazumov o prenosu pooblastil ali *ad hoc* nepovratnih sredstev v skladu z njenimi finančnimi pravili iz člena 32 in določbami zadevnih instrumentov, ki podpirajo politike Unije;

(d) prispevke iz tretjih držav, ki sodelujejo pri delu agencije ENISA, kot je določeno v členu 42;

(e) vse prostovoljne prispevke držav članic, denarne ali v naravi.

Države članice, ki zagotovijo prostovoljne prispevke v skladu s točko (e) prvega pododstavka, v zameno za to ne smejo zahtevati nobenih posebnih pravic ali storitev.

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

*Člen 31*

**Izvrševanje proračuna agencije ENISA**

1. Za izvrševanje proračuna agencije ENISA je odgovoren izvršni direktor.

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

3. Računovodja agencije ENISA do 1. marca po vsakem proračunskem letu (leto N + 1) računovodji Komisije in Računskemu sodišču pošlje začasni zaključni račun za proračunsko leto (leto N).

4. Računovodja agencije ENISA po prejemu pripomb Računskega sodišča k začasnemu zaključnemu računu agencije ENISA v skladu s členom 246 Uredbe (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta ([28]) pripravi končni zaključni račun agencije ENISA na lastno odgovornost in ga predloži v mnenje upravnemu odboru.

5. Upravni odbor izda mnenje o zaključnem računu agencije ENISA.

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 agencije ENISA do 1. julija leta N + 1 Evropskemu parlamentu, Svetu, računovodji Komisije in Računskemu sodišču pošlje končni zaključni račun agencije ENISA skupaj z mnenjem upravnega odbora.

([28]) Uredba (EU, Euratom) 2018/1046 Evropskega parlamenta in Sveta z dne 18. julija 2018 o finančnih pravilih, ki se uporabljajo za splošni proračun Unije, spremembi uredb (EU) št. 1296/2013, (EU) št. 1301/2013, (EU) št. 1303/2013, (EU) št. 1304/2013, (EU) št. 1309/2013, (EU) št. 1316/2013, (EU) št. 223/2014, (EU) št. 283/2014 in Sklepa št. 541/2014/EU ter razveljavitvi Uredbe (EU, Euratom) št. 966/2012 (UL L 193, 30.7.2018, str. 1).

8. Računovodja agencije ENISA pošlje Računskemu sodišču in v vednost računovodji Komisije na isti dan, ko pošlje končni zaključni račun agencije ENISA, tudi spremni dopis z dodatnimi obrazložitvami k temu računu.

9. Izvršni direktor do 15. novembra leta N + 1 objavi končni zaključni račun agencije ENISA v *Uradnem listu Evropske unije*.

10. Izvršni direktor do 30. septembra leta N + 1 Računskemu sodišču 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 261(3) Uredbe (EU, Euratom) 2018/1046 predloži vse informacije, potrebne za nemoten potek postopka razrešnice za zadevno proračunsko leto.

12. Na priporočilo Sveta Evropski parlament izvršnemu direktorju pred 15. majem leta N + 2 podeli razrešnico za izvrševanje proračuna za leto N.

*Člen 32*

**Finančna pravila**

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

*Člen 33*

**Boj proti goljufijam**

1. Da bi olajšali boj proti goljufijam, korupciji in drugim nezakonitim dejavnostim v skladu z Uredbo (EU, Euratom) št. 883/2013 Evropskega parlamenta in Sveta ([29]) agencija ENISA do 28. decembra 2019 pristopi k Medinstitucionalnemu sporazumu z dne 25. maja 1999 med Evropskim parlamentom, Svetom Evropske unije in Komisijo Evropskih skupnosti notranjih preiskavah Evropskega urada za boj proti goljufijam (OLAF) ([30]). Agencija ENISA sprejme ustrezne predpise, ki se uporabljajo za vse zaposlene agencije ENISA, pri čemer uporabi obrazec iz Priloge k navedenemu sporazumu.

2. Računsko sodišče je pooblaščeno za izvajanje revizij na podlagi dokumentacije in inšpekcij na kraju samem pri vseh upravičencih do nepovratnih sredstev, izvajalcih in podizvajalcih, ki so od agencije ENISA prejeli sredstva Unije.

3. Urad OLAF lahko izvaja preiskave, vključno s pregledi in inšpekcijami na kraju samem, v skladu z določbami in postopki iz Uredbe (EU, Euratom) št. 883/2013 ter Uredbe Sveta (Euratom, ES) št. 2185/96 ([31]), da bi ugotovil, ali je prišlo do goljufije, korupcije ali katere koli druge nezakonite dejavnosti, ki vpliva na finančne interese Unije v povezavi z nepovratnimi sredstvi ali pogodbo, ki jo je financirala agencija ENISA.

4. Brez poseganja v odstavke 1, 2 in 3 sporazumi o sodelovanju s tretjimi državami ali mednarodnimi organizacijami, pogodbe, sporazumi in sklepi o nepovratnih sredstvih agencije ENISA vsebujejo določbe, s katerimi Računsko sodišče in urad OLAF izrecno pooblaščajo za izvajanje takšnih revizij in preiskav v skladu z njunimi pristojnostmi.

([29]) 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).

([30]) UL L 136, 31.5.1999, str. 15.

([31]) 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).

*POGLAVJE V*

***Osebje***

*Člen 34*

**Splošne določbe**

Za osebje agencije ENISA veljajo Kadrovski predpisi za uradnike in Pogoji za zaposlitev drugih uslužbencev ter pravila za izvajanje Kadrovskih predpisov za uradnike in Pogojev za zaposlitev drugih uslužbencev, sprejeta z dogovorom med institucijami Unije.

*Člen 35*

**Privilegiji in imunitete**

Za agencijo ENISA in njeno osebje se uporablja Protokol št. 7 o privilegijih in imunitetah Evropske unije, ki je priložen PEU in PDEU.

*Člen 36*

**Izvršni direktor**

1. Izvršni direktor je zaposlen kot začasni uslužbenec agencije ENISA v skladu s točko (a) člena 2 Pogojev za zaposlitev drugih uslužbencev.

2. Izvršnega direktorja na podlagi odprtega in preglednega izbirnega postopka imenuje upravni odbor s seznama kandidatov, ki ga predlaga Komisija.

3. Agencijo ENISA pri sklenitvi pogodbe o zaposlitvi 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 poslancev.

5. Mandat izvršnega direktorja traja pet let. Komisija do konca tega obdobja pripravi oceno uspešnosti dela izvršnega direktorja ter prihodnjih nalog in izzivov agencije ENISA.

6. Upravni odbor sprejme odločitve o imenovanju, podaljšanju mandata ali razrešitvi izvršnega direktorja v skladu s členom 18(2).

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

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

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

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

*Člen 37*

**Napoteni nacionalni strokovnjaki in drugo osebje**

1. Agencija ENISA lahko uporabi napotene nacionalne strokovnjake ali drugo osebje, ki ni zaposleno v agenciji ENISA. Za to osebje ne veljajo Kadrovski predpisi za uradnike in Pogoji za zaposlitev drugih uslužbencev.

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

*POGLAVJE VI*

***Splošne določbe v zvezi z agencijo ENISA***

*Člen 38*

**Pravni status agencije ENISA**

1. Agencija ENISA je organ Unije in ima pravno osebnost.

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

3. Agencijo ENISA zastopa izvršni direktor.

*Člen 39*

**Odgovornost agencije ENISA**

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

2. Za odločanje na podlagi katere koli arbitražne klavzule iz pogodb, ki jih sklene agencija ENISA, je pristojno Sodišče Evropske unije.

3. Pri nepogodbeni odgovornosti agencija ENISA povrne vsakršno škodo, ki jo pri opravljanju nalog povzroči sama ali jo povzročijo njeni uslužbenci, v skladu s splošnimi načeli, ki so skupni zakonodaji držav članic.

4. Sodišče Evropske unije je pristojno za odločanje v vseh odškodninskih sporih za škodo iz odstavka 3.

5. Osebno odgovornost uslužbencev agencije ENISA do agencije ENISA urejajo ustrezni pogoji, ki se uporabljajo za osebje agencije ENISA.

*Člen 40*

**Jezikovna ureditev**

1. Za agencijo ENISA se uporablja Uredba Sveta št. 1 ([32]). Države članice in drugi organi, ki jih imenujejo države članice, lahko pišejo agenciji ENISA in prejmejo odgovor v uradnem jeziku institucij Unije, ki ga izberejo.

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

*Člen 41*

**Varstvo osebnih podatkov**

1. Agencija ENISA obdeluje osebne podatke v skladu z Uredbo (EU) 2018/1725.

2. Upravni odbor sprejme izvedbena pravila iz člena 45(3) Uredbe (EU) 2018/1725. Upravni odbor lahko sprejme dodatne ukrepe, ki so potrebni, da agencija ENISA uporablja Uredbo (EU) 2018/1725.

([32]) Uredba Sveta št. 1 o določitvi jezikov, ki se uporabljajo v Evropski gospodarski skupnosti (UL 17, 6.10.1958, str. 385/58).

*Člen 42*

**Sodelovanje s tretjimi državami in mednarodnimi organizacijami**

1. Agencija ENISA 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 ENISA na podlagi predhodne odobritve Komisije vzpostavi delovne dogovore z organi tretjih držav in mednarodnimi organizacijami. Ti delovni dogovori ne ustvarjajo novih pravnih obveznosti za Unijo in njene države članice.

2. Agencija ENISA je odprta za udeležbo tretjih držav, ki so v ta namen z Unijo sklenile sporazume. Na podlagi ustreznih določb teh sporazumov se vzpostavijo delovni dogovori, v katerih so določeni zlasti značaj, obseg in način udeležbe vsake izmed teh tretjih držav pri delu agencije ENISA, ter vključujejo določbe glede udeležbe pri pobudah agencije ENISA, finančnih prispevkov in osebja. Glede kadrovskih zadev so ti delovni dogovori v vseh pogledih skladni s Kadrovskimi predpisi za uradnike in Pogoji za zaposlitev drugih uslužbencev..

3. Upravni odbor sprejme strategijo o odnosih s tretjimi državami in mednarodnimi organizacijami glede vprašanj, ki so v pristojnosti agencije ENISA. Komisija zagotovi, da agencija ENISA deluje v skladu s svojim mandatom in veljavnim institucionalnim okvirom, tako da z izvršnim direktorjem sklene ustrezne delovne dogovore.

*Člen 43*

**Varnostni predpisi za varovanje občutljivih netajnih podatkov in tajnih podatkov**

Agencija ENISA po posvetovanju s Komisijo sprejme varnostne predpise, ki upoštevajo varnostna načela, vsebovana v varnostnih predpisih Komisije za varovanje občutljivih netajnih podatkov in tajnih podatkov Evropske unije, kot so določeni v sklepih (EU, Euratom) 2015/443 in 2015/444. Varnostni predpisi agencije ENISA vsebujejo določbe o izmenjavi, obdelavi in hrambi takih podatkov.

*Člen 44*

**Sporazum o sedežu in pogoji delovanja**

1. Potrebni dogovori glede namestitve, ki jo je treba agenciji ENISA 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 ENISA in njihove družinske člane, so določeni v sporazumu o sedežu, ki ga agencija ENISA in država članica gostiteljica skleneta po pridobitvi odobritve upravnega odbora.

2. Država članica gostiteljica agencije ENISA zagotovi optimalne pogoje za zagotovitev uspešnega delovanja agencije ENISA, ob upoštevanju dostopnosti lokacije, obstoja ustreznih šol za otroke uslužbencev ter ustreznega dostopa do trga dela, socialne varnosti in zdravstvenega varstva za otroke in zakonce članov osebja.

*Člen 45*

**Upravni nadzor**

Delovanje agencije ENISA nadzoruje Evropski varuh človekovih pravic v skladu s členom 228 PDEU.

NASLOV III

**CERTIFIKACIJSKI OKVIR ZA KIBERNETSKO VARNOST**

*Člen 46*

**Evropski certifikacijski okvir za kibernetsko varnost**

1. Evropski certifikacijski okvir za kibernetsko varnost se vzpostavi za izboljšanje pogojev za delovanje notranjega trga z zvišanjem ravni kibernetske varnosti v Uniji in omogočanjem harmoniziranega pristopa na ravni Unije glede evropskih certifikacijskih shem za kibernetsko varnost, da bi se oblikoval enotni digitalni trg za proizvode IKT, storitve IKT in postopke IKT.

2. Evropski certifikacijski okvir za kibernetsko varnost zagotavlja mehanizem za vzpostavitev evropskih certifikacijskih shem za kibernetsko varnost in za potrjevanje, da proizvodi IKT, storitve IKT in postopki IKT, ki so bili ocenjeni v skladu s takimi shemami, izpolnjujejo določene varnostne zahteve, da se zaščitijo razpoložljivost, pristnost, celovitost ali zaupnost shranjenih, prenesenih ali obdelanih podatkov ali funkcij ali storitev, ki jih ti proizvodi, storitve in postopki ponujajo ali so prek njih dostopni v celotnem življenjskem ciklu.

*Člen 47*

**Tekoči delovni program Unije za evropsko certificiranje kibernetske varnosti**

1. Komisija objavi tekoči delovni program Unije za evropsko certificiranje kibernetske varnosti (v nadaljnjem besedilu: tekoči delovni program Unije), v katerem so opredeljene strateške prednostne naloge za prihodnje evropske certifikacijske sheme za kibernetsko varnost.

2. Tekoči delovni program Unije vključuje predvsem seznam proizvodov IKT, storitev IKT in postopkov IKT ali njihovih kategorij, za katere je lahko koristno, če so vključeni v področje uporabe evropske certifikacijske sheme za kibernetsko varnost.

3. Vključitev posameznih proizvodov IKT, storitev IKT in postopkov IKT ali njihovih kategorij v tekoči delovni program Unije se utemelji z enim ali več od naslednjih razlogov:

(a) razpoložljivost in oblikovanje nacionalnih certifikacijskih shem za kibernetsko varnost, ki zajemajo posamezno kategorijo proizvodov IKT, storitev IKT ali postopkov IKT, zlasti kar zadeva tveganje razdrobljenosti;

(b) ustrezna politika ali pravo Unije ali nacionalna politika ali pravo;

(c) povpraševanje na trgu;

(d) razvoj kibernetskih groženj;

(e) zahteva za pripravo posebne predloge sheme, ki jo predlaga evropska certifikacijska skupina za kibernetsko varnost.

4. Komisija ustrezno upošteva mnenja, ki jih glede osnutka tekočega delovnega programa Unije izdata evropska certifikacijska skupina za kibernetsko varnost in certifikacijska skupina deležnikov.

5. Prvi tekoči delovni program Unije se objavi do 28. junija 2020. Posodablja se vsaj vsaka tri leta in, če je potrebno, pogosteje.

*Člen 48*

**Zahteva za evropsko certifikacijsko shemo za kibernetsko varnost**

1. Komisija lahko od agencije ENISA zahteva, naj pripravi predlogo za shemo ali pregleda obstoječo evropsko certifikacijsko shemo za kibernetsko varnost na podlagi tekočega delovnega programa Unije.

2. Komisija ali evropska certifikacijska skupina za kibernetsko varnost lahko v ustrezno utemeljenih primerih od agencije ENISA zahteva, naj pripravi predlogo za shemo ali pregleda obstoječo shemo, ki ni vključena v tekoči delovni program Unije. Tekoči delovni program Unije se ustrezno posodobi.

*Člen 49*

**Priprava, sprejetje in pregled evropske certifikacijske sheme za kibernetsko varnost**

1. Agencija ENISA na zahtevo Komisije na podlagi člena 48 pripravi predlogo za shemo, ki izpolnjuje zahteve iz členov 51, 52 in 54.

2. Agencija ENISA lahko na zahtevo evropske certifikacijske skupine za kibernetsko varnost na podlagi člena 48(2) pripravi predlogo za shemo, ki izpolnjuje zahteve iz členov 51, 52 in 54. Če agencija ENISA takšno zahtevo zavrne, mora to obrazložiti. Vsako odločitev o zavrnitvi take zahteve sprejme upravni odbor.

3. Pri pripravi predloge za shemo se agencija ENISA posvetuje z vsemi ustreznimi deležniki v okviru formalnega, odprtega, preglednega in vključujočega posvetovanja.

4. Agencija ENISA za vsako predlogo za shemo ustanovi *ad hoc* delovno skupino v skladu s členom 20(4), da agenciji ENISA pomaga s specifičnimi nasveti ter strokovnim znanjem in izkušnjami.

5. Agencija ENISA tesno sodeluje z evropsko certifikacijsko skupino za kibernetsko varnost. Ta skupina agenciji ENISA zagotavlja pomoč in strokovno svetovanje pri pripravi predloge za shemo ter sprejme mnenje o predlogi za shemo.

6. Agencija ENISA v največji možni meri upošteva mnenje evropske certifikacijske skupine za kibernetsko varnost, preden predlogo za shemo, pripravljeno v skladu z odstavki 3, 4 in 5, pošlje Komisiji. Mnenje evropske certifikacijske skupine za kibernetsko varnost za agencijo ENISA ni zavezujoče in agencija ENISA lahko predlogo za shemo pošlje Komisiji tudi brez takega mnenja.

7. Komisija lahko na podlagi predloge za shemo, ki jo pripravi agencija ENISA, sprejme izvedbene akte, ki določajo evropsko certifikacijsko shemo za kibernetsko varnost za proizvode IKT, storitve IKT in postopke IKT, ki izpolnjujejo zahteve iz členov 51, 52 in 54. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 66(2).

8. Agencija ENISA najmanj vsakih pet let oceni vsako sprejeto evropsko certifikacijsko shemo za kibernetsko varnost ob upoštevanju povratnih informacij, ki jih prejme od zainteresiranih strani. Komisija ali evropska certifikacijska skupina za kibernetsko varnost lahko po potrebi zaprosi agencijo ENISA, da začne postopek oblikovanja revidirane predloge za shemo v skladu s členom 48 in tem členom.

*Člen 50*

**Spletišče evropskih certifikacijskih shem za kibernetsko varnost**

1. Agencija ENISA vzdržuje posebno spletišče, namenjeno informiranju in obveščanju javnosti o evropskih certifikacijskih shemah za kibernetsko varnost, evropskih certifikatih kibernetske varnosti in izjavah EU o skladnosti, vključno z informacijami v zvezi z evropskimi certifikacijskimi shemami za kibernetsko varnost, ki niso več veljavne, odvzetimi in poteklimi evropskimi certifikati kibernetske varnosti in izjavami EU o skladnosti ter repozitorijem povezav do informacij o kibernetski varnosti, zagotovljenih v skladu s členom 55.

2. Na spletišču iz odstavka 1 so po potrebi navedene tudi nacionalne certifikacijske sheme za kibernetsko varnost, ki so bile nadomeščene z evropsko certifikacijsko shemo za kibernetsko varnost.

*Člen 51*

**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 proizvoda IKT, storitve IKT ali postopka IKT;

(b) zaščititi shranjene, prenesene ali kako drugače obdelane podatke pred naključnim ali nepooblaščenim uničenjem, izgubo ali spremembo ali slabo razpoložljivostjo med celotnim življenjskim ciklom proizvoda IKT, storitve IKT ali postopka IKT;

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

(d) opredeliti in evidentirati znane odvisnosti in šibke točke;

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

(f) omogočiti preverjanje, 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 oziroma jih je uporabljal ali obdeloval;

(g) preveriti, da proizvodi IKT, storitve IKT in postopki IKT ne vsebujejo znanih šibkih točk;

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

(i) proizvodi IKT, storitve IKT in postopki IKT so razviti v skladu z načelom privzete in vgrajene varnosti;

(j) proizvodi IKT, storitve IKT in postopki 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.

*Člen 52*

**Ravni zanesljivosti evropskih certifikacijskih shem za kibernetsko varnost**

1. Evropska certifikacijska shema za kibernetsko varnost lahko določa eno ali več naslednjih ravni zanesljivosti za proizvode IKT, storitve IKT in postopke IKT: „osnovno“, „znatno“ ali „visoko“. Raven zanesljivosti ustreza stopnji tveganja, povezani s predvideno uporabo proizvoda IKT, storitve IKT ali postopka IKT v smislu verjetnosti in vpliva incidenta.

2. Evropski certifikati kibernetske varnosti in izjave EU o skladnosti se nanašajo na katero koli raven zanesljivosti, določeno v evropski certifikacijski shemi za kibernetsko varnost, v okviru katere se evropski certifikat kibernetske varnosti ali izjava EU o skladnosti izda.

3. Varnostne zahteve, ki ustrezajo vsaki ravni zanesljivosti, so določene v ustrezni evropski certifikacijski shemi za kibernetsko varnost, vključno z ustreznimi varnostnimi funkcionalnostmi in ustrezno strogostjo in obsegom ocenjevanja, ki se izvede za proizvod IKT, storitev IKT ali postopek IKT.

4. Certifikat ali izjava EU o skladnosti se nanaša na zadevne tehnične specifikacije, standarde in postopke, vključno s tehničnim nadzorom, katerih namen je zmanjšati tveganje za incidente, povezane s kibernetsko varnostjo, ali jih preprečiti.

5. Evropski certifikat kibernetske varnosti ali izjava EU o skladnosti, ki se nanaša na „osnovno“ raven zanesljivosti, zagotavlja, da proizvodi IKT, storitve IKT in postopki IKT, za katere se izda ta certifikat ali ta izjava EU o skladnosti, izpolnjujejo ustrezne varnostne zahteve, vključno z varnostnimi funkcionalnostmi, in da so bili ocenjeni na ravni za kar najbolj zmanjšana znana osnovna tveganja incidentov in kibernetskih napadov. Ocenjevalne dejavnosti, ki se izvedejo, vključujejo vsaj pregled tehnične dokumentacije. Kadar tak pregled ni primeren, se izvedejo nadomestne ocenjevalne dejavnosti z enakovrednim učinkom.

6. Evropski certifikat kibernetske varnosti, ki se nanaša na „znatno“ raven zanesljivosti, zagotavlja, da proizvodi IKT, storitve IKT in postopki IKT, za katere se izda ta certifikat, izpolnjujejo ustrezne varnostne zahteve, vključno z varnostnimi funkcionalnostmi, in da so bili ocenjeni na ravni za kar najbolj zmanjšana znana kibernetska tveganja ter tveganja incidentov in kibernetskih napadov, ki jih izvajajo akterji z omejenim znanjem in viri. Ocenjevalne dejavnosti, ki se izvedejo, vključujejo najmanj naslednje: pregled za dokazovanje, da se javno znane šibke točke ne pojavljajo, in testiranje za dokazovanje, da se pri proizvodih IKT, storitvah IKT ali postopkih IKT pravilno izvajajo potrebne varnostne funkcionalnosti. Kadar katera izmed takih ocenjevalnih dejavnost ni primerna, se izvedejo nadomestne ocenjevalne dejavnosti z enakovrednim učinkom.

7. Evropski certifikat kibernetske varnosti, ki se nanaša na „visoko“ raven zanesljivosti, zagotavlja, da proizvodi IKT, storitve IKT in postopki IKT, za katere se izda ta certifikat, izpolnjujejo ustrezne varnostne zahteve, vključno z varnostnimi funkcionalnostmi, in da so bili ocenjeni na ravni za kar najbolj zmanjšano tveganje naprednih kibernetskih napadov, ki jih izvajajo akterji z obsežnim znanjem in viri. Ocenjevalne dejavnosti, ki se izvedejo, vključujejo najmanj naslednje: pregled za dokazovanje, da se javno znane šibke točke ne pojavljajo, ter testiranje za dokazovanje, da se pri proizvodih IKT, storitvah IKT ali postopkih IKT pravilno izvajajo potrebne najsodobnejše varnostne funkcionalnosti, in ocenjevanje njihove odpornosti proti izurjenim napadalcem z uporabo penetracijskega testiranja. Kadar katera izmed takih ocenjevalnih dejavnosti ni primerna, se izvedejo nadomestne dejavnosti z enakovrednim učinkom.

8. V evropski certifikacijski shemi za kibernetsko varnost se lahko določi več stopenj ocenjevanja, odvisno od strogosti in obsega metodologije za ocenjevanje, ki se uporabi. Vsaka od stopenj ocenjevanja ustreza eni od ravni zanesljivosti in je opredeljena z ustrezno kombinacijo elementov zanesljivosti.

*Člen 53*

**Samoocenjevanje skladnosti**

1. V okviru evropske certifikacijske sheme za kibernetsko varnost se lahko dopusti samoocenjevanje skladnosti, za katero je v celoti odgovoren proizvajalec ali ponudnik proizvodov IKT, storitev IKT ali postopkov IKT. Samoocenjevanje se dopusti samo v zvezi s proizvodi IKT, storitvami IKT in postopki IKT, ki predstavljajo nizko tveganje, ki ustreza „osnovni“ ravni zanesljivosti.

2. Proizvajalec ali ponudnik proizvodov IKT, storitev IKT ali postopkov 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 proizvodov IKT, storitev IKT ali postopkov IKT prevzame odgovornost za skladnost proizvoda IKT, storitve IKT ali postopka IKT z zahtevami iz te sheme.

3. Proizvajalec ali ponudnik proizvodov IKT, storitev IKT ali postopkov IKT za obdobje, določeno v ustrezni evropski certifikacijski shemi za kibernetsko varnost, nacionalnemu certifikacijskemu organu za kibernetsko varnost iz člena 58 da na voljo izjavo EU o skladnosti, tehnično dokumentacijo in vse druge ustrezne informacije. Kopija izjave EU o skladnosti se predloži nacionalnemu certifikacijskemu organu za kibernetsko varnost in agenciji ENISA.

4. Izjava EU o skladnosti se izda prostovoljno, razen če je v pravu Unije ali države članice določeno drugače.

5. Izjave EU o skladnosti se priznajo v vseh državah članicah.

*Člen 54*

**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 proizvodov IKT, storitev IKT in postopkov IKT;

(b) jasen opis namena sheme ter tega, kako izbrani standardi, metode za ocenjevanje in ravni zanesljivosti ustrezajo potrebam predvidenih uporabnikov sheme;

(c) sklic na mednarodne, evropske ali nacionalne standarde, uporabljene pri ocenjevanju, ali, kadar taki standardi niso na voljo ali niso ustrezni, sklic na tehnične specifikacije, ki izpolnjujejo zahteve iz Priloge II k Uredbi (EU) št. 1025/2012, ali, če take specifikacije niso na voljo, sklic na tehnične specifikacije ali druge zahteve glede kibernetske varnosti, določene v evropski certifikacijski shemi za kibernetsko varnost;

(d) eno ali več ravni zanesljivosti, kadar je to ustrezno;

(e) navedbo, ali je samoocenjevanje skladnosti dovoljeno v okviru sheme;

(f) 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;

(g) posebna merila in metode za ocenjevanje, vključno z vrstami ocene, ki se uporabljajo za dokazovanje, da so varnostni cilji iz člena 51 doseženi;

(h) kadar je ustrezno, informacije, ki so potrebne za certificiranje in ki jih vložnik predloži ali kako drugače da na voljo organom za ugotavljanje skladnosti;

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

(j) pravila za spremljanje skladnosti proizvodov IKT, storitev IKT in postopkov IKT z zahtevami evropskih certifikatov kibernetske varnosti ali izjave EU o skladnosti, vključno z mehanizmi za dokazovanje stalnega izpolnjevanja določenih zahtev glede kibernetske varnosti;

(k) kadar je ustrezno, pogoje za izdajo, ohranitev, nadaljevanje in obnovitev evropskih certifikatov kibernetske varnosti ter pogojev za razširitev ali zmanjšanje področja uporabe certificiranja;

(l) pravila glede posledic za proizvode IKT, storitve IKT in postopke IKT, ki so bili certificirani ali za katere se je izdala izjava EU o skladnosti, vendar niso skladni z zahtevami sheme;

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

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

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

(p) vsebino in obliko evropskih certifikatov kibernetske varnosti in izjav EU o skladnosti, ki jih je treba izdati;

(q) obdobje razpoložljivosti izjave EU o skladnosti, tehnične dokumentacije in vseh drugih ustreznih informacij, ki jih da na voljo proizvajalec ali ponudnik proizvodov IKT, storitev IKT ali postopkov IKT;

(r) najdaljši rok veljavnosti evropskih certifikatov kibernetske varnosti, izdanih v okviru sheme;

(s) politiko razkritja za evropske certifikate kibernetske varnosti, izdane, spremenjene oziroma odvzete v okviru sheme;

(t) pogoje za vzajemno priznavanje certifikacijskih shem s tretjimi državami;

(u) kadar je ustrezno, pravila glede vsakršnega mehanizma medsebojnega strokovnega ocenjevanja, vzpostavljenega s shemo, za organe, ki izdajajo evropske certifikate kibernetske varnosti, za „visoko“ raven zanesljivosti v skladu s členom 56(6). Takšen mehanizem ne vpliva na medsebojni strokovni pregled iz člena 59;

(v) obliko in postopke, ki jih morajo upoštevati proizvajalci in ponudniki proizvodov IKT, storitev IKT ali postopkov IKT pri zagotavljanju in posodabljanju dodatnih informacij o kibernetski varnosti v skladu s členom 55.

2. Določene zahteve evropske certifikacijske sheme za kibernetsko varnost so v skladu z veljavnimi pravnimi zahtevami, zlasti zahtevami, ki izhajajo iz harmoniziranega prava Unije.

3. Kadar tako določa posebni pravni akt Unije, se certifikat ali izjava EU o skladnosti, izdana v okviru evropske certifikacijske sheme za kibernetsko varnost lahko uporabi za dokazovanje domneve o skladnosti z zahtevami navedenega pravnega akta.

4. Če ni harmoniziranega prava Unije, lahko pravo države članice določa tudi, da se evropska certifikacijska shema za kibernetsko varnost lahko uporabi za oblikovanje domneve o skladnosti s pravnimi zahtevami.

*Člen 55*

**Dodatne informacije o kibernetski varnosti za certificirane proizvode IKT, storitve IKT in postopke IKT**

1. Proizvajalec ali ponudnik certificiranih proizvodov IKT, storitev IKT in postopkov IKT ali proizvodov IKT, storitev IKT in postopkov IKT, za katere je bila izdala izjava EU o skladnosti, da na voljo naslednje dodatne informacije o kibernetski varnosti:

(a) navodila in priporočila za pomoč končnim uporabnikom pri varni konfiguraciji, namestitvi, uvajanju, delovanju in vzdrževanju proizvodov IKT ali storitev IKT;

(b) obdobje, v katerem bo končnim uporabnikom na voljo varnostna podpora, zlasti kar zadeva razpoložljivost posodobitev, povezanih s kibernetsko varnostjo;

(c) kontaktne informacije proizvajalca ali ponudnika in sprejete metode za prejemanje informacij o šibkih točkah od končnih uporabnikov in raziskovalcev na področju varnosti;

(d) o dostopu do spletnih seznamov javno znanih šibkih točk v zvezi s proizvodom IKT, storitvijo IKT ali postopkom IKT in ustreznih nasvetov s področja kibernetske varnosti.

2. Informacije iz odstavka 1 so na voljo v elektronski obliki ter ostanejo na voljo in se po potrebi posodabljajo vsaj do izteka veljavnosti ustreznega evropskega certifikata kibernetske varnosti ali izjave EU o skladnosti.

*Člen 56*

**Certificiranje kibernetske varnosti**

1. Za proizvode IKT, storitve IKT in postopke IKT, ki so bili certificirani na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete na podlagi člena 49, se domneva, da so skladni z zahtevami take sheme.

2. Certificiranje za kibernetsko varnost je prostovoljno, razen če je v pravu Unije ali države članice določeno drugače.

3. Komisija redno ocenjuje učinkovitost in uporabo sprejetih evropskih certifikacijskih shem za kibernetsko varnost ter ali bi morala posamezna evropska certifikacijska shema za kibernetsko varnost postati obvezna na podlagi ustreznega prava Unije, da bi zagotovili ustrezno raven kibernetske varnosti proizvodov IKT, storitev IKT in postopkov IKT v Uniji ter izboljšali delovanje notranjega trga. Prva taka ocena se izvede do 31. decembra 2023, poznejše ocene pa se izvedejo vsaj vsaki dve leti po tem. Komisija na podlagi rezultatov teh ocen opredeli proizvode IKT, storitve IKT in postopke IKT, zajete v obstoječi certifikacijski shemi, ki bi morali biti zajeti v obvezni certifikacijski shemi.

Komisija se prednostno osredotoča na sektorje iz Priloge II k Direktivi (EU) 2016/1148, ki jih je treba oceniti najpozneje dve leti po sprejetju prve evropske certifikacijske sheme za kibernetsko varnost.

Komisija pri pripravi ocene:

(a) upošteva učinek ukrepov na proizvajalce ali ponudnike takšnih proizvodov IKT, storitev IKT ali postopkov IKT ter na uporabnike v smislu stroška teh ukrepov, pa tudi družbene ali gospodarske koristi zaradi pričakovane višje ravni varnosti ciljnih proizvodov IKT, storitev IKT ali postopkov IKT;

(b) upošteva obstoj in izvajanje ustreznega prava države članice in prava tretje države;

(c) izvede odprto, pregledno in vključujoče posvetovanje z vsemi ustreznimi deležniki in državami članicami;

(d) upošteva roke za izvajanje, prehodne ukrepe in obdobja, zlasti glede morebitnega učinka ukrepov na proizvajalce ali ponudnike proizvodov IKT, storitev IKT ali postopkov IKT, vključno z MSP;

(e) predlaga najhitrejši in najučinkovitejši način za izvedbo prehoda s prostovoljnih na obvezne certifikacijske sheme.

4. Organi za ugotavljanje skladnosti iz člena 60 na podlagi tega člena izdajo evropski certifikat kibernetske varnosti, ki se nanaša na „osnovno“ ali „znatno“ raven zanesljivosti, na podlagi meril, vključenih v evropsko certifikacijsko shemo za kibernetsko varnost, ki jo je na podlagi člena 49 sprejela Komisija.

5. Z odstopanjem od odstavka 4 in v ustrezno utemeljenih primerih lahko evropska certifikacijska shema za kibernetsko varnost določa, da mora evropske certifikate kibernetske varnosti, ki izhajajo iz te sheme, izdati le javni organ. Tak organ je eden od naslednjih:

(a) nacionalni organ za certificiranje kibernetske varnosti, kot je določen v členu 58(1), ali

(b) javni organ, ki je akreditiran kot organ za ugotavljanje skladnosti na podlagi člena 60(1).

6. Kadar evropska certifikacijska shema za kibernetsko varnost na podlagi člena 49 zahteva „visoko“ raven zanesljivosti, lahko evropski certifikat kibernetske varnosti na podlagi te sheme izda samo nacionalni certifikacijski organ za kibernetsko varnost, v naslednjih primerih pa tudi organ za ugotavljanje skladnosti:

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

(b) na podlagi splošnega prenosa naloge izdajanja takih evropskih certifikatov kibernetske varnosti na organ za ugotavljanje skladnosti s strani nacionalnega certifikacijskega organa za kibernetsko varnost.

7. Fizična ali pravna oseba, ki predloži proizvode IKT, storitve IKT ali postopke IKT za certifikacijo, nacionalnemu certifikacijskemu organu za kibernetsko varnost iz člena 58, če je to organ, ki je izdal evropski certifikat kibernetske varnosti, ali organu za ugotavljanje skladnosti iz člena 60 da na voljo vse informacije, ki so potrebne za izvedbo certifikacije.

8. Imetnik evropskega certifikata kibernetske varnosti obvesti nacionalni certifikacijski organ za kibernetsko varnost ali organ za ugotavljanje skladnosti iz odstavka 7 o vseh pozneje odkritih šibkih točkah ali nepravilnostih v zvezi z varnostjo certificiranega proizvoda IKT, storitve IKT ali postopka IKT, ki bi lahko vplivale na njegovo skladnost z zahtevami, povezanimi s certifikacijo. Navedeni organ te informacije brez nepotrebnega odlašanja posreduje zadevnemu nacionalnemu certifikacijskemu organu za kibernetsko varnost.

9. Evropski certifikat kibernetske varnosti se izda za obdobje, določeno v evropski certifikacijski shemi za kibernetsko varnost, in se lahko podaljša, če so zadevne zahteve še vedno izpolnjene.

10. Evropski certifikat kibernetske varnosti, izdan na podlagi tega člena, se prizna v vseh državah članicah.

*Člen 57*

**Nacionalne certifikacijske sheme za kibernetsko varnost in nacionalni certifikati kibernetske varnosti**

1. Brez poseganja v odstavek 3 tega člena nacionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za proizvode IKT, storitve IKT in postopke IKT, ki so zajeti v evropski certifikacijski shemi za kibernetsko varnost, prenehajo učinkovati z datumom, določenim v izvedbenem aktu, sprejetem na podlagi člena 49(7). Nacionalne certifikacijske sheme za kibernetsko varnost ter z njimi povezani postopki za proizvode IKT, storitve IKT in postopke IKT, ki niso zajeti v evropski certifikacijski shemi za kibernetsko varnost, še naprej obstajajo.

2. Države članice ne uvedejo novih nacionalnih certifikacijskih shem za kibernetsko varnost za proizvode IKT, storitve IKT in postopke IKT, ki so zajeti v veljavni evropski certifikacijski shemi za kibernetsko varnost.

3. Obstoječi certifikati, ki so bili izdani na podlagi nacionalnih certifikacijskih shem za kibernetsko varnost in so zajeti v evropski certifikacijski shemi za kibernetsko varnost, ostanejo veljavni do datuma izteka veljavnosti.

4. Države članice z namenom preprečevanja razdrobljenosti notranjega trga Komisijo in evropsko certifikacijsko skupino za kibernetsko varnost obveščajo o kakršnih koli pobudah za pripravo novih nacionalnih certifikacijskih shem za kibernetsko varnost.

*Člen 58*

**Nacionalni certifikacijski organi za kibernetsko varnost**

1. Vsaka država članica na svojem ozemlju imenuje enega ali več nacionalnih certifikacijskih organov za kibernetsko varnost ali pa v dogovoru z drugo državo članico imenuje enega ali več nacionalnih certifikacijskih organov za kibernetsko varnost 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 nacionalnih certifikacijskih organov za kibernetsko varnost. Kadar država članica imenuje več kot en organ, pa Komisijo obvesti tudi o nalogah, ki so dodeljene vsakemu posameznemu organu.

3. Vsak nacionalni certifikacijski organ za kibernetsko varnost je brez poseganja v točko (a) člena 56(5) in člen 56(6) glede svoje organizacije, odločitev o financiranju, pravne strukture in sprejemanja odločitev neodvisen od subjektov, ki jih nadzoruje.

4. Države članice zagotovijo, da so dejavnosti nacionalnega certifikacijskega organu za kibernetsko varnost, ki se nanašajo na izdajanje evropskih certifikatov kibernetske varnosti iz točke (a) člena 56(5) in člena 56(6), strogo ločene od njihovih nadzornih dejavnosti iz tega člena ter da se te dejavnosti izvajajo neodvisno druga od druge.

5. Države članice zagotovijo, da imajo nacionalni certifikacijski organi za kibernetsko varnost ustrezne vire za izvajanje svojih pooblastil ter učinkovito in uspešno izvajanje svojih nalog.

6. Za učinkovito izvajanje te uredbe je primerno, da nacionalni certifikacijski organi za kibernetsko varnost sodelujejo v evropski certifikacijski skupini za kibernetsko varnost na dejaven, učinkovit, uspešen in varen način.

7. Nacionalni organi za certificiranje kibernetske varnosti:

(a) nadzirajo in uveljavljajo pravila iz evropskih certifikacijskih shem za kibernetsko varnost na podlagi točke (j) člena 54(1) za spremljanje skladnosti proizvodov IKT, storitev IKT in postopkov IKT z zahtevami evropskih certifikatov kibernetske varnosti, ki so bili izdani na njihovem ozemlju, v sodelovanju z drugimi zadevnimi organi za nadzor trga;

(b) spremljajo izpolnjevanje obveznosti proizvajalcev ali ponudnikov proizvodov IKT, storitev IKT ali postopkov IKT, ki imajo sedež na njihovem ozemlju in izvajajo samoocenjevanje skladnosti, in jih izvršujejo, ter zlasti spremljajo izpolnjevanje obveznosti takih proizvajalcev ali ponudnikov, določenih v členu 53(2) in (3) in v ustrezni evropski certifikacijski shemi za kibernetsko varnost, in jih izvršujejo;

(c) brez poseganja v člen 60(3) nacionalnim akreditacijskim organom dejavno pomagajo in jih podpirajo pri spremljanju in nadziranju dejavnosti organov za ugotavljanje skladnosti za namene te uredbe;

(d) spremljajo in nadzirajo dejavnosti javnih organov iz člena 56(5);

(e) kadar je ustrezno, pooblastijo organe za ugotavljanje skladnosti v skladu s členom 60(3) ter omejijo, začasno prekličejo ali odvzamejo obstoječe pooblastilo, kadar organi za ugotavljanje skladnosti kršijo zahteve iz te uredbe;

(f) obravnavajo pritožbe fizičnih ali pravnih oseb glede evropskih certifikatov kibernetske varnosti, ki jih izdajo nacionalni certifikacijski organi za kibernetsko varnost, ali glede evropskih certifikatov kibernetske varnosti, ki jih izdajo organi za ugotavljanje skladnosti v skladu s členom 56(6), ali glede izjav EU o skladnosti, izdanih na podlagi člena 53, ter v ustreznem obsegu preučijo vsebino takih pritožb ter pritožnika v razumnem roku obvestijo o napredku in izidih preiskave;

(g) agenciji ENISA in evropski certifikacijski skupini za kibernetsko varnost posredujejo letno zbirno poročilo o dejavnostih, izvedenih na podlagi točk (b), (c) in (d) tega odstavka ali na podlagi odstavka 8;

(h) sodelujejo z drugimi nacionalnimi certifikacijskimi organi za kibernetsko varnost ali drugimi javnimi organi, vključno z izmenjavo informacij o morebitni neskladnosti proizvodov IKT, storitev IKT in postopkov IKT z zahtevami iz te uredbe ali z zahtevami posameznih evropskih certifikacijskih shem za kibernetsko varnost, ter

(i) spremljajo ustrezen razvoj na področju certificiranja kibernetske varnosti.

8. Vsak nacionalni certifikacijski organ za kibernetsko varnost ima vsaj naslednja pooblastila:

(a) od organov za ugotavljanje skladnosti, imetnikov evropskih certifikatov kibernetske varnosti in izdajateljev izjav 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 evropskih certifikatov kibernetske varnosti in izdajateljev izjav EU o skladnosti, da preveri njihovo skladnost s tem naslovom;

(c) v skladu z nacionalnim pravom sprejme ustrezne ukrepe, da zagotovi, da organi za ugotavljanje skladnosti, imetniki evropskih certifikatov kibernetske varnosti certifikata in izdajatelji izjav EU o skladnosti izpolnjujejo zahteve iz te uredbe ali evropske certifikacijske sheme za kibernetsko varnost;

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

(e) v skladu z nacionalnim pravom odvzame evropske certifikate kibernetske varnosti, ki jih izdajo nacionalni certifikacijski organi za kibernetsko varnost, ali evropske certifikate kibernetske varnosti, ki jih izdajo organi za ugotavljanje skladnosti v skladu s členom 56(6), kadar taki certifikati niso skladni s to uredbo ali z evropsko certifikacijsko shemo za kibernetsko varnost;

(f) v skladu z nacionalnim pravom izreče kazni, kot je določeno v členu 65, in zahteva takojšnje prenehanje kršitev obveznosti iz te uredbe.

9. Nacionalni certifikacijski organi za kibernetsko varnost sodelujejo med seboj in s Komisijo, zlasti z izmenjavo informacij, izkušenj in dobrih praks glede certificiranja kibernetske varnosti in tehničnih vprašanj, ki zadevajo kibernetsko varnost proizvodov IKT, storitev IKT in postopkov IKT.

*Člen 59*

**Medsebojni strokovni pregled**

1. Da bi po vsej Uniji vzpostavili enakovredne standarde v zvezi z evropskimi certifikati kibernetske varnosti in izjavami EU o skladnosti, se za nacionalne certifikacijske organe za kibernetsko varnost izvajajo medsebojni strokovni pregledi.

2. Medsebojni strokovni pregled se izvede na podlagi zanesljivih in preglednih meril in postopkov vrednotenja, zlasti v zvezi z zahtevami glede strukture, človeških virov in postopkov, zaupnosti ter pritožb.

3. Z medsebojnim strokovnim pregledom se ocenjuje:

(a) kadar je ustrezno, ali so dejavnosti nacionalnih certifikacijskih organov za kibernetsko varnost, ki se nanašajo na izdajanje evropskih certifikatov kibernetske varnosti iz točke (a) člena 56(5) in člena 56(6), strogo ločene od njihovih nadzornih dejavnosti iz člena 58 ter ali se te dejavnosti izvajajo neodvisno druga od druge;

(b) postopke za nadziranje in uveljavljanje pravil za spremljanje skladnosti proizvodov IKT, storitev IKT in postopkov IKT z evropskimi certifikati kibernetske varnosti v na podlagi točke (a) člena 58(7);

(c) postopke za spremljanje in izvrševanje obveznosti proizvajalcev ali ponudnikov proizvodov IKT, storitev IKT ali postopkov IKT na podlagi točke (b) člena 58(7);

(d) postopke za spremljanje, odobritev in nadziranje dejavnosti organov za ugotavljanje skladnosti;

(e) kadar je ustrezno, ali ima osebje organov, ki izdajajo certifikate za „visoko“ raven zanesljivosti v skladu s členom 56(6), ustrezno strokovno znanje in izkušnje.

4. Medsebojni strokovni pregled opravijo vsaj dva nacionalna certifikacijska organa za kibernetsko varnost iz drugih držav članic in Komisija, izvede pa se najmanj vsakih pet let. Pri medsebojnem strokovnem pregledu lahko sodeluje agencija ENISA.

5. Komisija lahko sprejme izvedbene akte za določitev načrta medsebojnih strokovnih pregledov, ki zajema vsaj petletno obdobje, ter določa merila v zvezi s sestavo skupine za medsebojni strokovni pregled, zanj uporabljeno metodologijo, roke, pogostost in druge naloge, povezane z njim. Komisija pri sprejemanju izvedbenih aktov ustrezno upošteva mnenja evropske certifikacijske skupine za kibernetsko varnost. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 66(2).

6. Rezultate medsebojnih strokovnih pregledov preuči evropska certifikacijska skupina za kibernetsko varnost, ki pripravi povzetke, ki se lahko objavijo, ter po potrebi izda smernice ali priporočila za ukrepe, ki naj bi jih sprejeli zadevni subjekti.

*Člen 60*

**Organi za ugotavljanje skladnosti**

1. Organe za ugotavljanje skladnosti akreditirajo nacionalni akreditacijski organi, imenovani na podlagi Uredbe (ES) št. 765/2008. Taka akreditacija se izda samo, kadar organ za ugotavljanje skladnosti izpolnjuje zahteve, določene v Prilogi k tej uredbi.

2. Kadar evropski certifikat kibernetske varnosti izda nacionalni certifikacijski organ za kibernetsko varnost na podlagi točke (a) člena 56(5) in člena 56(6), se certifikacijski organ nacionalnega certifikacijskega organa za kibernetsko varnost akreditira kot organ za ugotavljanje skladnosti na podlagi odstavka 1 tega člena.

3. Kadar evropske certifikacijske sheme za kibernetsko varnost določajo posebne ali dodatne zahteve na podlagi točke (f) člena 54(1), lahko nacionalni certifikacijski organ za kibernetsko varnost za izvajanje nalog iz takih shem pooblasti samo organe za ugotavljanje skladnosti, ki izpolnjujejo navedene zahteve.

4. Akreditacija iz odstavka 1 se izda organom za ugotavljanje skladnosti za največ pet let in se lahko pod enakimi pogoji podaljša, če organ za ugotavljanje skladnosti še vedno izpolnjuje zahteve iz tega člena. Nacionalni akreditacijski organi sprejmejo vse ustrezne ukrepe, da v razumnem roku omejijo ali začasno oziroma trajno prekličejo akreditacijo organa za ugotavljanje skladnosti, izdano na podlagi odstavka 1, kadar pogoji za akreditacijo niso bili izpolnjeni ali niso več izpolnjeni ali kadar organ za ugotavljanje skladnosti krši to uredbo.

*Člen 61*

**Priglasitev**

1. Nacionalni certifikacijski organi za kibernetsko varnost za vsako evropsko certifikacijsko shemo za kibernetsko varnost, Komisiji priglasijo organe za ugotavljanje skladnosti, ki so bili akreditirani in po potrebi pooblaščeni na podlagi člena 60(3), za izdajo evropskih certifikatov kibernetske varnosti na določenih ravneh zanesljivosti iz člena 52. Nacionalni certifikacijski organi za kibernetsko varnost Komisiji brez nepotrebnega odlašanja priglasijo kakršne koli naknadne spremembe glede njih.

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

3. Če Komisija prejme priglasitev po izteku obdobja iz odstavka 2, objavi spremembe seznama priglašenih organov za ugotavljanje skladnosti v *Uradnem listu Evropske unije* v dveh mesecih od datuma prejema priglasitve.

4. Nacionalni certifikacijski organ za kibernetsko varnost lahko Komisiji predloži zahtevek za črtanje organa za ugotavljanje skladnosti, ki ga je priglasil ta organ, s seznama iz odstavka 2. Komisija objavi ustrezne spremembe tega seznama v *Uradnem listu Evropske unije* v enem mesecu po datumu prejema zahtevka nacionalnega certifikacijskega organa za kibernetsko varnost.

5. Komisija lahko sprejme izvedbene akte, s katerimi se določijo okoliščine, oblike in postopki za priglasitev iz odstavka 1 tega člena. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 66(2).

*Člen 62*

**Evropska certifikacijska skupina za kibernetsko varnost**

1. Ustanovi se evropska certifikacijska skupina za kibernetsko varnost.

2. Evropsko certifikacijsko skupino za kibernetsko varnost sestavljajo predstavniki nacionalnih certifikacijskih organov za kibernetsko varnost ali predstavniki drugih ustreznih nacionalnih organov. Član skupine ne sme zastopati več kot dveh držav članic.

3. Na seje evropske certifikacijske skupine za kibernetsko varnost so lahko povabljeni deležniki in zadevne tretje strani, ki lahko tudi sodelujejo pri njenem delu.

4. Evropska certifikacijska skupina za kibernetsko varnost opravlja naslednje naloge:

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

(b) podpira in svetuje agenciji ENISA ter z njo sodeluje pri pripravi predloge za shemo na podlagi člena 49;

(c) sprejme mnenje o predlogah za sheme, ki jih pripravi agencija ENISA na podlagi člena 49;

(d) od agencije ENISA zahteva, naj pripravi predloge za sheme na podlagi člena 48(2);

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

(f) preuči ustrezni razvoj na področju certificiranja kibernetske varnosti ter izmenjuje informacije in primere dobrih praks na področju certifikacijskih shem za kibernetsko varnost;

(g) olajšuje sodelovanje med nacionalnimi certifikacijskimi organi za kibernetsko varnost na podlagi tega naslova s krepitvijo zmogljivosti in izmenjavo informacij, zlasti z določitvijo metod za učinkovito izmenjavo informacij o vprašanjih v zvezi s certificiranjem kibernetske varnosti;

(h) podpira izvajanje mehanizmov medsebojnega strokovnega ocenjevanja v skladu s pravili, določenimi v evropski certifikacijski shemi za kibernetsko varnost na podlagi točke (u) člena 54(1);

(i) pospešuje usklajevanje evropskih certifikacijskih shem za kibernetsko varnost z mednarodno priznanimi standardi, vključno s pregledom obstoječih evropskih certifikacijskih shem za kibernetsko varnost, in po potrebi daje priporočila agenciji ENISA v zvezi s sodelovanjem z ustreznimi mednarodnimi organizacijami za standardizacijo, da bi odpravili pomanjkljivosti ali vrzeli v razpoložljivih mednarodno priznanih standardih;

5. Ob pomoči agencije ENISA Komisija predseduje evropski certifikacijski skupini za kibernetsko varnost in ji zagotovi sekretariat v skladu s točko (e) člena 8(1).

*Člen 63*

**Pravica do vložitve pritožbe**

1. Fizične in pravne osebe imajo pravico, da vložijo pritožbo pri izdajatelju evropskega certifikata kibernetske varnosti ali, kadar se pritožba nanaša na evropski certifikat kibernetske varnosti, ki ga je izdal organ za ugotavljanje skladnosti v skladu s členom 56(6), pri zadevnem nacionalnem certifikacijskem organu za kibernetsko varnost.

2. Organ, pri katerem je bila vložena pritožba, obvesti pritožnika o napredku postopka in sprejeti odločitvi ter obvesti pritožnika o pravici do učinkovitega sodnega pravnega sredstva iz člena 64.

*Člen 64*

**Pravica do učinkovitega sodnega pravnega sredstva**

1. Ne glede na morebitna upravna ali druga izvensodna pravna sredstva imajo fizične in pravne osebe pravico do učinkovitega sodnega pravnega sredstva v zvezi z:

(a) odločitvami, ki jih sprejme organ iz člena 63(1), po potrebi tudi v zvezi z nepravilno izdajo, opustitvijo izdaje ali priznanjem evropskega certifikata kibernetske varnosti, ki ga imajo v lasti zadevne fizične ali pravne osebe;

(b) opustitvijo ukrepanja glede pritožbe, vložene pri organu iz člena 63(1).

2. Za postopke v skladu s tem členom so pristojna sodišča države članice, v kateri ima sedež organ, zoper katerega je bilo sodno pravno sredstvo vloženo.

*Člen 65*

**Kazni**

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

NASLOV IV

**KONČNE DOLOČBE**

*Člen 66*

**Postopek v odboru**

1. Komisiji pomaga odbor. Ta odbor je odbor v smislu Uredbe (EU) št. 182/2011.

2. Pri sklicevanju na ta odstavek se uporablja točka (b) člena 5(4) Uredbe (EU) št. 182/2011.

*Člen 67*

**Ocena in pregled**

1. Komisija do 28. junija 2024, nato pa vsakih pet let oceni učinek, uspešnost in učinkovitost agencije ENISA in njenih delovnih praks ter morebitno potrebo po spremembi mandata agencije ENISA kot tudi finančne posledice vsake take spremembe. Pri oceni se upoštevajo vse povratne informacije, ki jih agencija ENISA prejme kot odziv na svoje dejavnosti. Kadar Komisija meni, da nadaljnje delovanje agencije ENISA glede na dodeljene cilje, mandat in naloge ni več upravičen, lahko predlaga spremembo določb te uredbe, ki se nanašajo na agencijo ENISA.

2. Oceni se tudi vpliv, učinkovitost in uspešnost določb naslova III te uredbe glede ciljev zagotavljanja ustrezne ravni kibernetske varnosti proizvodov IKT, storitev IKT in postopkov IKT v Uniji ter izboljšanja delovanja notranjega trga.

3. Med ocenjevanjem se presodi, ali so za dostop do notranjega trga potrebne bistvene zahteve glede kibernetske varnosti, da se prepreči vstop proizvodov IKT, storitev IKT in postopkov IKT, ki ne izpolnjujejo osnovnih zahtev glede kibernetske varnosti, na trg Unije.

4. Komisija do 28. junija 2024, nato pa vsakih pet let pošlje poročilo o oceni skupaj s svojimi zaključki Evropskemu parlamentu, Svetu in upravnemu odboru. Ugotovitve iz poročila o oceni se objavijo.

*Člen 68*

**Razveljavitev in nasledstvo**

1. Uredba (EU) št. 526/2013 se razveljavi z učinkom od 27. junija 2019.

2. Sklici na Uredbo (EU) št. 526/2013 in agencijo ENISA, kot je ustanovljena z navedeno uredbo, se štejejo kot sklici na to uredbo in agencijo ENISA, kot je ustanovljena s to uredbo.

3. Agencija ENISA, kot je ustanovljena s to uredbo, je pravna naslednica agencije ENISA, kot je bila ustanovljena z Uredbo (EU) št. 526/2013, kar zadeva lastništvo, dogovore, pravne obveznosti, pogodbe o zaposlitvi, finančne obveznosti in odgovornosti. Vse obstoječe odločitve upravnega odbora in izvršnega odbora, sprejete v skladu z Uredbo (EU) št. 526/2013, ostanejo veljavne, če so skladne s to uredbo.

4. Agencija ENISA se ustanovi za nedoločeno obdobje od 27. junija 2019.

5. Izvršni direktor, imenovan na podlagi člena 24(4) Uredbe (EU) št. 526/2013, ostane na položaju in izvaja svoje naloge iz člena 20 te uredbe do konca svojega mandata. Drugi pogoji njegove pogodbe ostanejo nespremenjeni.

6. Člani in namestniki članov upravnega odbora, imenovani na podlagi člena 6 Uredbe (EU) št. 526/2013, ostanejo na položaju in izvajajo naloge upravnega odbora iz člena 15 te uredbe do konca svojega mandata.

*Člen 69*

**Začetek veljavnosti**

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

2. Členi 58, 60, 61, 63, 64 in 65 se uporabljajo od 28. junija 2021.

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

V Strasbourgu, 17. aprila 2019

| *Za Evropski parlament* | *Za Svet* |
|---|---|
| *Predsednik* | *Predsednik* |
| A. TAJANI | G. CIAMBA |

*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 ali proizvoda IKT, storitve IKT ali postopka IKT, katerega skladnost ugotavlja.

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

4. Organi za ugotavljanje skladnosti, njihovo najvišje vodstvo in osebe, odgovorne za izvajanje nalog ugotavljanja skladnosti, niso snovalci, proizvajalci, dobavitelji oziroma ponudniki, monterji, kupci, lastniki, uporabniki ali vzdrževalci proizvoda IKT, storitve IKT ali postopka IKT, katerega skladnost ugotavljajo, niti niso pooblaščeni zastopniki katere koli od navedenih strani. Ta prepoved ne onemogoča uporabe proizvodov IKT, za katere ugotavlja skladnost in ki so nujni za delovanje organa za ugotavljanje skladnosti, ali uporabe takšnih proizvodov IKT za osebne namene.

5. Organi za ugotavljanje skladnosti, njihovo najvišje vodstvo in osebe, odgovorne za izvajanje nalog ugotavljanja skladnosti, ne sodelujejo neposredno pri snovanju, proizvodnji ali izdelavi, trženju, montaži, uporabi ali vzdrževanju proizvodov IKT, storitev IKT ali postopkov IKT, katerih skladnost ugotavljajo, niti ne zastopajo strani, ki sodelujejo pri teh dejavnostih. Organi za ugotavljanje skladnosti, njihovo najvišje vodstvo in osebe, odgovorne za izvajanje nalog ugotavljanja skladnosti, ne sodelujejo pri nobenih dejavnostih, ki bi lahko bile v nasprotju z njihovo neodvisno presojo ali integriteto v zvezi z njihovimi dejavnostmi za ugotavljanje skladnosti. Ta prepoved velja zlasti za svetovalne storitve.

6. Če je organ za ugotavljanje skladnosti v lasti ali upravljanju javne osebe ali ustanove, sta zagotovljeni in dokumentirani neodvisnost in odsotnost morebitnega nasprotja interesov med nacionalnim certifikacijskim organom za kibernetsko varnost in organom za ugotavljanje skladnosti.

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

8. 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, ki bi lahko vplivali na njihovo presojo ali rezultate njihovih dejavnosti za ugotavljanje skladnosti, vključno s pritiski in spodbudami finančne narave, zlasti od oseb ali skupin oseb, za katere so rezultati navedenih dejavnosti pomembni.

9. 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. Vsako podizvajanje s strani zunanjega oseba ali posvetovanje z zunanjim osebjem se ustrezno dokumentira, ne vključuje posrednikov in je predmet pisnega sporazuma, ki med drugim zajema zaupnost in nasprotja interesov. Zadevni organ za ugotavljanje skladnosti prevzame polno odgovornost za opravljene naloge.

10. Vedno ter za vsak postopek ugotavljanja skladnosti in vsako vrsto, kategorijo ali podkategorijo proizvoda IKT, storitve IKT ali postopka IKT ima organ za ugotavljanje skladnosti na razpolago:

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

    (b) opise postopkov, v skladu s katerimi se mora izvajati ugotavljanje skladnosti, za zagotovitev preglednost in zmožnost reprodukcije navedenih postopkov. Izvaja ustrezne politike in postopke, na podlagi katerih se ločijo naloge, ki jih izvaja kot organ, priglašen na podlagi člena 61, in njegove druge dejavnosti;

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

11. 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.

12. Osebe, odgovorne za izvajanje dejavnosti za ugotavljanje skladnosti, imajo:

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

(b) zadovoljivo znanje o zahtevah glede ugotavljanja 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.

13. Zagotovi se nepristranskost organa za ugotavljanje skladnosti, njegovega najvišjega vodstva in oseb, odgovornih za izvajanje dejavnosti ugotavljanja skladnosti ter kakršnih koli podizvajalcev.

14. Plačilo najvišjega vodstva in oseb, odgovornih za dejavnosti ugotavljanja skladnosti, ni odvisno od števila opravljenih ugotavljanj skladnosti ali rezultatov navedenih ugotavljanj skladnosti.

15. Organi za ugotavljanje skladnosti sklenejo zavarovanje odgovornosti, razen če odgovornost prevzame država članica v skladu z nacionalnim pravom ali če je država članica sama neposredno odgovorna za ugotavljanje skladnosti.

16. Organ za ugotavljanje skladnosti in njegovo osebje, odbori, odvisne družbe, podizvajalci ter povezani organi ali osebje zunanjih organov organa za ugotavljanje skladnosti spoštujejo zaupnost informacij in so zavezani k poklicni molčečnosti v zvezi z vsemi informacijami, pridobljenimi med izvajanjem nalog ugotavljanja skladnosti iz te uredbe ali na podlagi katere koli določbe nacionalnega prava za izvajanje te uredbe, razen kadar njihovo razkritje zahteva pravo Unije ali države članice, ki velja za te osebe, in razen pred pristojnimi organi držav članic, v katerih se izvajajo njegove dejavnosti. Pravice intelektualne lastnine so zaščitene. Organ za ugotavljanje skladnosti vzpostavi dokumentirane postopke v zvezi z zahtevami iz te točke.

17. Z izjemo točke 16 zahteve iz te priloge ne izključujejo izmenjave tehničnih informacij in regulativnih navodil med organom za ugotavljanje skladnosti in osebo, ki zaprosi za certifikacijo ali preučuje možnost, da bi to storila.

18. Organi za ugotavljanje skladnosti delujejo v skladu z vrsto doslednih, poštenih in razumnih pogojev, ob upoštevanju interesov MSP v zvezi s pristojbinami.

19. Organi za ugotavljanje skladnosti izpolnjujejo zahteve ustreznega standarda, harmoniziranega na podlagi Uredbe (ES) št. 765/2008, za akreditacijo organov za ugotavljanje skladnosti, ki izvajajo certificiranje proizvodov IKT, storitev IKT ali postopkov IKT.

20. Organi za ugotavljanje skladnosti zagotovijo, da preskuševalni laboratoriji, v katerih se izvaja ugotavljanje skladnosti, izpolnjujejo zahteve ustreznega standarda, harmoniziranega na podlagi Uredbe (ES) št. 765/2008, za akreditacijo laboratorijev, ki izvajajo preskuse.