Uradni list
Evropske unije

SL
Serija L

2024/2847

20.11.2024

UREDBA (EU) 2024/2847 EVROPSKEGA PARLAMENTA IN SVETA

z dne 23. oktobra 2024

o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti)

(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]),

po posvetovanju z Odborom regij,

v skladu z rednim zakonodajnim postopkom ([2]),

ob upoštevanju naslednjega:

(1) Kibernetska varnost je eden od ključnih izzivov za Unijo. Število in raznolikost povezanih naprav se bosta v prihodnjih letih eksponentno povečevala. Kibernetski napadi so vprašanje javnega interesa, saj lahko odločilno vplivajo ne le na gospodarstvo Unije, temveč tudi na demokracijo ter varnost in zdravje potrošnikov. Zato je treba okrepiti pristop Unije h kibernetski varnosti, obravnavati kibernetsko odpornost na ravni Unije ter izboljšati delovanje notranjega trga z določitvijo enotnega pravnega okvira za bistvene zahteve glede kibernetske varnosti za dajanje izdelkov z digitalnimi elementi na trg Unije. Obravnavati bi bilo treba dve glavni težavi, zaradi katerih imajo uporabniki in družba dodatne stroške: nizko raven kibernetske varnosti izdelkov z digitalnimi elementi, ki se odraža v splošno razširjenih ranljivostih ter nezadostnem in nedoslednem zagotavljanju varnostnih posodobitev za njihovo odpravljanje, ter nezadostno razumevanje in nezadosten dostop uporabnikov do informacij, ki preprečujeta izbiro izdelkov z ustreznimi lastnostmi kibernetske varnosti ali njihovo varno uporabo.

(2) Namen te uredbe je določiti mejne pogoje za razvoj varnih izdelkov z digitalnimi elementi z zagotovitvijo, da se na trg dajejo izdelki strojne in programske opreme z manj ranljivostmi ter da proizvajalci v celotnem življenjskem ciklu izdelka resno obravnavajo vprašanje varnosti. Poleg tega je njen namen ustvariti pogoje, ki uporabnikom omogočajo upoštevanje kibernetske varnosti pri izbiri in uporabi izdelkov z digitalnimi elementi, na primer z izboljšanjem preglednosti v zvezi z obdobjem podpore za izdelke z digitalnimi elementi, dostopne na trgu.

(3) Veljavno ustrezno pravo Unije obsega več sklopov horizontalnih pravil, ki z različnih zornih kotov obravnavajo določene vidike, povezane s kibernetsko varnostjo, vključno z ukrepi za izboljšanje varnosti digitalne dobavne verige. Vendar obstoječe pravo Unije v zvezi s kibernetsko varnostjo, vključno z Uredbo (EU) 2019/881 Evropskega parlamenta in Sveta ([3]) in Direktivo (EU) 2022/2555 Evropskega parlamenta in Sveta ([4]), ne zajema neposredno obveznih zahtev za varnost izdelkov z digitalnimi elementi.

([1]) UL C 100, 16.3.2023, str. 101.
([2]) Stališče Evropskega parlamenta z dne 12. marca 2024 (še ni objavljeno v Uradnem listu) in odločitev Sveta z dne 10. oktobra 2024.
([3]) 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) (UL L 151, 7.6.2019, str. 15).
([4]) Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80).

(4) Medtem ko se obstoječe pravo Unije uporablja za nekatere izdelke z digitalnimi elementi, horizontalnega regulativnega okvira Unije, ki določa celovite zahteve glede kibernetske varnosti za vse izdelke z digitalnimi elementi, ni. Z različnimi akti in pobudami, ki so bili doslej sprejeti na ravni Unije in nacionalni ravni, se le delno obravnavajo ugotovljene težave in tveganja, povezana s kibernetsko varnostjo, pri čemer ustvarjajo zakonodajni mozaik na notranjem trgu, povečujejo pravno negotovost za proizvajalce in uporabnike teh izdelkov ter dodajajo nepotrebno breme za podjetja in organizacije zaradi izpolnjevanja številnih zahtev in obveznosti za podobne vrste izdelkov. Kibernetska varnost teh izdelkov ima posebno jasno čezmejno razsežnost, saj izdelke z digitalnimi elementi, izdelane v eni državi članici ali v tretji državi, pogosto uporabljajo organizacije in potrošniki na celotnem notranjem trgu. Zato je treba to področje urejati na ravni Unije, da bi zagotovili harmoniziran regulativni okvir in pravno varnost za uporabnike, organizacije in podjetja, vključno z mikropodjetji ter malimi in srednjimi podjetji, kot so opredeljena v Prilogi k Priporočilu Komisije 2003/361/ES ([5]). Regulativno okolje Unije bi bilo treba harmonizirati z uvedbo horizontalnih zahtev glede kibernetske varnosti za izdelke z digitalnimi elementi. Poleg tega bi bilo treba po vsej Uniji zagotoviti pravno varnost za gospodarske subjekte in uporabnike ter boljšo uskladitev notranjega trga in sorazmernost za mikro-, mala in srednja podjetja, s tem pa ustvariti bolj uresničljive pogoje za gospodarske subjekte, ki nameravajo vstopiti na trg Unije.

(5) Kar zadeva mikropodjetja ter mala in srednja podjetja, bi bilo treba pri določanju kategorije, v katero spada podjetje, določbe Priloge k Priporočilu 2003/361/ES uporabljati v celoti. Zato bi bilo treba pri izračunu števila zaposlenih in finančnih zgornjih mej, ki določajo kategorije podjetij, uporabiti tudi določbe člena 6 Priloge k Priporočilu 2003/361/ES o vzpostavitvi podatkov o podjetju ob upoštevanju posebnih vrst podjetij, kot so partnerska podjetja ali povezana podjetja.

(6) Komisija bi morala zagotoviti usmeritve za pomoč gospodarskim subjektom, zlasti mikropodjetjem ter malim in srednjim podjetjem, pri uporabi te uredbe. Take usmeritve bi morale med drugim zajemati področje uporabe te uredbe, zlasti obdelavo podatkov na daljavo in njene posledice za razvijalce proste in odprtokodne programske opreme, uporabo meril, ki se uporabljajo za določitev obdobij podpore za izdelke z digitalnimi elementi, interakcijo med to uredbo in drugim pravom Unije ter konceptom bistvene spremembe.

(7) Na ravni Unije so različni programski in politični dokumenti, kot so Skupno sporočilo Komisije in visokega predstavnika Unije za zunanje zadeve in varnostno politiko z dne 16. decembra 2020 z naslovom „Strategija EU za kibernetsko varnost v digitalnem desetletju“, sklep Sveta z dne 2. decembra 2020 o kibernetski varnosti povezanih naprav in z dne 23. maja 2022 o oblikovanju stališča Evropske unije glede kibernetskih vprašanj ter resolucija Evropskega parlamenta z dne 10. junija 2021 o strategiji EU za kibernetsko varnost v digitalnem desetletju ([6]), pozivali k uvedbi posebnih zahtev Unije glede kibernetske varnosti za digitalne ali povezane izdelke, pri čemer je več tretjih držav na lastno pobudo uvedlo ukrepe za obravnavo tega vprašanja. V končnem poročilu Konference o prihodnosti Evrope so državljani pozvali k „večji vlogi EU pri preprečevanju kibernetskih groženj“. Da bi Unija imela vodilno mednarodno vlogo na področju kibernetske varnosti, je pomembno določiti ambiciozen regulativni okvir.

(8) Za izboljšanje splošne ravni kibernetske varnosti vseh izdelkov z digitalnimi elementi, danih na notranji trg, je treba za te izdelke uvesti tehnološko nevtralne bistvene zahteve glede kibernetske varnosti, usmerjene v cilje, ki se uporabljajo horizontalno.

(9) Pod določenimi pogoji se lahko vsi izdelki z digitalnimi elementi, vgrajeni v večji elektronski informacijski sistem ali povezani z njim, uporabijo kot napadni vektor za zlonamerne akterje. Tako lahko tudi strojna in programska oprema, ki velja za manj kritično, olajša prvotno ogrožanje naprave ali omrežja in zlonamernim akterjem omogoči, da pridobijo privilegiran dostop do sistema ali se pomikajo lateralno med sistemi. Zato bi morali proizvajalci zagotoviti, da se vsi izdelki z digitalnimi elementi načrtujejo in razvijajo v skladu z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe. Ta obveznost zadeva izdelke z možnostjo fizične povezave prek vmesniške strojne opreme in izdelke z možnostjo logične povezave, na primer prek omrežnih vtičnic, cevovodov, datotek, vmesnikov za aplikacijsko programje ali katere koli druge vrste programskih vmesnikov. Kibernetske grožnje se lahko širijo prek različnih izdelkov z digitalnimi elementi, dokler ne dosežejo določenega cilja, na primer s povezovanjem več izrab ranljivosti, zato bi morali proizvajalci zagotoviti tudi kibernetsko varnost izdelkov z digitalnimi elementi, ki so zgolj posredno povezani z drugimi napravami ali omrežji.

([5]) Priporočilo Komisije 2003/361/ES z dne 6. maja 2003 o opredelitvi mikro, malih in srednje velikih podjetij (UL L 124, 20.5.2003, str. 36).

([6]) UL C 67, 8.2.2022, str. 81.

(10) Z določitvijo zahtev glede kibernetske varnosti za dajanje izdelkov z digitalnimi elementi na trg naj bi se izboljšala kibernetska varnost teh izdelkov za potrošnike in podjetja. S temi zahtevami se bo tudi zagotovilo, da se bo kibernetska varnost upoštevala v celotnih dobavnih verigah in se bo s tem dosegla večja varnost končnih izdelkov z digitalnimi elementi in njihovih sestavnih delov. To vključuje tudi zahteve za dajanje potrošniških izdelkov z digitalnimi elementi, ki so namenjeni ranljivim potrošnikom, kakor so igrače in sistemi za spremljanje dojenčkov, na trg. Potrošniški izdelki z digitalnimi elementi, ki so v tej uredbi razvrščeni kot pomembni izdelki z digitalnimi elementi, pomenijo večje tveganje za kibernetsko varnost, saj opravljajo funkcijo, pri kateri obstaja znatno tveganje škodljivih učinkov v smislu intenzivnosti in zmožnosti škodovanja zdravju, zaščiti ali varnosti uporabnikov takih izdelkov, ter bi morali biti predmet strožjega postopka ugotavljanja skladnosti. To velja za izdelke, kot so izdelki za pametni dom z varnostnimi funkcijami, vključno s pametnimi ključavnicami, sistemi za spremljanje dojenčkov in alarmni sistemi, povezanimi igračami in osebno nosljivo zdravstveno tehnologijo. Poleg tega bodo strožji postopki ugotavljanja skladnosti, ki jih morajo prestati drugi izdelki z digitalnimi elementi, ki so v tej uredbi razvrščeni kot pomembni ali kritični izdelki z digitalnimi elementi, prispevali k preprečevanju morebitnih negativnih učinkov izkoriščanja ranljivosti na potrošnike.

(11) Namen te uredbe je zagotoviti visoko raven kibernetske varnosti izdelkov z digitalnimi elementi in njihovih vgrajenih rešitev za daljinsko obdelavo podatkov. Take rešitve za daljinsko obdelavo podatkov bi bilo treba opredeliti kot obdelavo podatkov na daljavo, za katero je programsko opremo zasnoval in razvil proizvajalec zadevnega izdelka z digitalnimi elementi ali je bila zasnovana in razvita v njegovem imenu ter brez katere izdelek z digitalnimi elementi ne bi mogel opravljati ene od svojih funkcij. Ta pristop zagotavlja, da proizvajalci take izdelke v celoti ustrezno zavarujejo, ne glede na to, ali se podatki obdelujejo ali shranjujejo lokalno na napravi uporabnika ali na daljavo s strani proizvajalca. Hkrati obdelava ali shranjevanje na daljavo spada na področje uporabe te uredbe le, če je to potrebno, da izdelek z digitalnimi elementi opravlja svoje funkcije. Taka obdelava ali shranjevanje na daljavo vključuje primere, kadar mobilna aplikacija zahteva dostop do vmesnika za aplikacijsko programiranje ali do podatkovne zbirke, zagotovljene s storitvijo, ki jo razvije proizvajalec. V takem primeru storitev spada na področje uporabe te uredbe kot rešitev za daljinsko obdelavo podatkov. Zahteve v zvezi z rešitvami za daljinsko obdelavo podatkov, ki spadajo na področje uporabe te uredbe, zato ne vključujejo tehničnih, operativnih ali organizacijskih ukrepov za obvladovanje tveganj za varnost omrežij in informacijskih sistemov proizvajalca kot celote.

(12) Rešitve v oblaku so rešitve za obdelavo podatkov na daljavo v smislu te uredbe le, če ustrezajo opredelitvi iz te uredbe. Na primer, funkcije, ki jih omogočajo storitve v oblaku in jih zagotavlja proizvajalec naprav za pametne domove, ki uporabnikom omogočajo upravljanje naprave na daljavo, bi morale spadati na področje uporabe te uredbe. Po drugi strani spletna mesta, ki ne podpirajo funkcionalnosti izdelka z digitalnimi elementi, ali storitve v oblaku, zasnovane in razvite zunaj odgovornosti proizvajalca izdelka z digitalnimi elementi, ne spadajo na področje uporabe te uredbe. Direktiva (EU) 2022/2555 se uporablja za storitve računalništva v oblaku in modele storitev tega računalništva, kot so programska oprema kot storitev, platforma kot storitev ali infrastruktura kot storitev. Subjekti, ki zagotavljajo storitve računalništva v oblaku v Uniji in se štejejo za srednja podjetja na podlagi člena 2 Priloge k Priporočilu 2003/361/ES ali presegajo zgornje meje za srednja podjetja iz odstavka 1 navedenega člena, spadajo na področje uporabe navedene direktive.

(13) V skladu s ciljem te uredbe, da se odpravijo ovire za prosto gibanje izdelkov z digitalnimi elementi, države članice za zadeve, zajete v tej uredbi, ne bi smele ovirati omogočanja dostopnosti izdelkov z digitalnimi elementi, ki so skladni s to uredbo, na trgu. Zato države članice za zadeve, harmonizirane s to uredbo, ne morejo naložiti dodatnih zahtev glede kibernetske varnosti za omogočanje dostopnosti izdelkov z digitalnimi elementi na trgu. Vendar lahko vsak javni ali zasebni subjekt poleg zahtev iz te uredbe določi dodatne zahteve za javno naročanje ali uporabo izdelkov z digitalnimi elementi za posebne namene, zato se lahko odloči za uporabo izdelkov z digitalnimi elementi, ki izpolnjujejo strožje ali bolj specifične zahteve glede kibernetske varnosti od tistih, ki se uporabljajo za omogočanje dostopnosti na trgu na podlagi te uredbe. Brez poseganja v direktivi 2014/24/EU ([7]) in 2014/25/EU ([8]) Evropskega parlamenta in Sveta bi morale države članice pri naročanju izdelkov z digitalnimi elementi, ki morajo izpolnjevati bistvene zahteve glede kibernetske varnosti iz te uredbe, vključno s tistimi v zvezi z obravnavanjem ranljivosti,

([7]) 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).

([8]) Direktiva 2014/25/EU Evropskega parlamenta in Sveta z dne 26. februarja 2014 o javnem naročanju naročnikov, ki opravljajo dejavnosti v vodnem, energetskem in prometnem sektorju ter sektorju poštnih storitev ter o razveljavitvi Direktive 2004/17/ES (UL L 94, 28.3.2014, str. 243).

zagotoviti, da se take zahteve upoštevajo v postopku javnega naročanja in da se upošteva tudi zmožnost proizvajalcev za učinkovito uporabo ukrepov za kibernetsko varnost in obvladovanje kibernetskih groženj. Poleg tega Direktiva (EU) 2022/2555 določa ukrepe za obvladovanje tveganj za kibernetsko varnost za bistvene in pomembne subjekte iz člena 3 navedene direktive, ki bi lahko vključevali ukrepe v zvezi z varnostjo dobavne verige, ki zahtevajo, da taki subjekti uporabljajo izdelke z digitalnimi elementi, ki izpolnjujejo strožje zahteve glede kibernetske varnosti od tistih iz te uredbe. V skladu z Direktivo (EU) 2022/2555 in njenim načelom minimalne harmonizacije lahko države članice zato naložijo dodatne zahteve glede kibernetske varnosti za uporabo izdelkov informacijsko-komunikacijske tehnologije (IKT) s strani bistvenih ali pomembnih subjektov na podlagi navedene direktive, da se zagotovi višja raven kibernetske varnosti, če so take zahteve skladne z obveznostmi držav članic, določenimi v pravu Unije. Zadeve, ki niso zajete v tej uredbi, lahko vključujejo netehnične dejavnike v zvezi z izdelki z digitalnimi elementi in njihovimi proizvajalci. Države članice lahko zato določijo nacionalne ukrepe, vključno z omejitvami za izdelke z digitalnimi elementi ali dobavitelje takih izdelkov, pri katerih se upoštevajo netehnični dejavniki. Za nacionalne ukrepe v zvezi s takimi dejavniki se zahteva, da so v skladu s pravom Unije.

(14) Ta uredba ne bi smela posegati v pristojnosti držav članic, da zaščitijo nacionalno varnost v skladu s pravom Unije. Države članice bi morale imeti možnost, da za izdelke z digitalnimi elementi, ki se naročijo ali uporabljajo za namene nacionalne varnosti ali obrambe, uvedejo dodatne ukrepe, če so taki ukrepi skladni z obveznostmi držav članic, določenimi v pravu Unije.

(15) Ta uredba se uporablja za gospodarske subjekte samo v zvezi z izdelki z digitalnimi elementi, ki so dostopni na trgu in se zato dobavljajo za distribucijo ali uporabo na trgu Unije v okviru gospodarske dejavnosti. Za dobavo v okviru gospodarske dejavnosti je poleg zaračunavanja cene za izdelek z digitalnimi elementi značilno tudi zaračunavanje cene za storitve tehnične podpore, kadar to ne služi le povrnitvi dejanskih stroškov, z namero monetizacije, na primer z zagotavljanjem platforme programske opreme, prek katere proizvajalec monetizira druge storitve, tako da kot pogoj za uporabo zahteva obdelavo osebnih podatkov za druge namene kot izključno za izboljšanje varnosti, združljivosti ali interoperabilnosti programske opreme, ali da sprejema donacije, ki presegajo stroške, povezane z zasnovo, razvojem in zagotavljanjem izdelka z digitalnimi elementi. Sprejemanje donacij brez namena ustvarjanja dobička se ne bi smelo šteti za gospodarsko dejavnost.

(16) Izdelki z digitalnimi elementi, ki se zagotavljajo kot del izvajanja storitve, za katero se zaračuna pristojbina izključno za povračilo dejanskih stroškov, neposredno povezanih z opravljanjem te storitve, kot je lahko v primeru nekaterih izdelkov z digitalnimi elementi, ki jih zagotavljajo subjekti javne uprave, zgolj iz teh razlogov ne bi smeli šteti za komercialno dejavnost za namene te uredbe. Poleg tega se za izdelke z digitalnimi elementi, ki jih subjekt javne uprave razvije ali spremeni izključno za lastno uporabo, ne bi smelo šteti, da so dostopni na trgu v smislu te uredbe.

(17) Programska oprema in podatki, ki se prosto izmenjujejo in pri katerih lahko uporabniki prosto dostopajo do njih ali njihovih spremenjenih različic, jih uporabljajo, spreminjajo in ponovno distribuirajo, lahko prispevajo k raziskavam in inovacijam na trgu. Da bi spodbudili razvoj in uvedbo proste in odprtokodne programske opreme, zlasti pri mikropodjetjih ter malih in srednjih podjetjih, vključno z zagonskimi podjetji, posamezniki neprofitnimi organizacijami in akademskimi raziskovalnimi organizacijami, bi bilo treba pri uporabi te uredbe za izdelke z digitalnimi elementi, ki štejejo za prosto in odprtokodno programsko opremo, ki se dobavlja za distribucijo ali uporabo v okviru gospodarske dejavnosti, upoštevati naravo različnih razvojnih modelov programske opreme, ki se distribuira in razvija na podlagi licenc proste in odprtokodne programske opreme.

(18) Prosta in odprtokodna programska oprema se razume kot programska oprema, katere izvorna koda se odprto deli in katere licenca zagotavlja vse pravice, da postane prosto dostopna in uporabna ter da jo je mogoče spremeniti in prerazporediti. Prosta in odprtokodna programska oprema se razvija, vzdržuje in distribuira odprto, vključno prek spletnih platform. V zvezi z gospodarskimi subjekti, ki spadajo na področje uporabe te uredbe, bi morala na področje uporabe te uredbe spadati le prosta in odprtokodna programska oprema, ki je dostopna na trgu in se zato dobavlja za distribucijo ali uporabo v okviru gospodarske dejavnosti. Pri določanju komercialne ali nekomercialne narave te dejavnosti se zato ne bi smele upoštevati zgolj okoliščine, v katerih je bil izdelek z digitalnimi elementi razvit, ali način financiranja razvoja. Natančneje, se za namene te uredbe in v zvezi z gospodarskimi subjekti, ki spadajo na njeno področje uporabe, da se zagotovi jasno razlikovanje med razvojno fazo in fazo dobave, zagotavljanje izdelkov z digitalnimi elementi, ki štejejo za prosto in odprtokodno programsko opremo, ki jih njihovi

proizvajalci ne monetizirajo, ne bi smelo šteti za komercialno dejavnost. Poleg tega bi se morala dobava izdelkov z digitalnimi elementi, ki se štejejo za sestavne dele proste in odprtokodne programske opreme in ki so namenjeni temu, da jih drugi proizvajalci vključijo v svoje izdelke z digitalnimi elementi, šteti za omogočanje dostopnosti na trgu le, če komponento monetizira njen prvotni proizvajalec. Zgolj dejstvo, da odprtokodni programski izdelek z digitalnimi elementi prejema finančno podporo proizvajalcev ali da proizvajalci prispevajo k razvoju takega izdelka, na primer samo po sebi ne bi smelo določati, da je dejavnost komercialne narave. Poleg tega zgolj redno izdajanje novih različic samo po sebi ne bi smelo privesti do sklepa, da se izdelek z digitalnimi elementi dobavlja v okviru gospodarske dejavnosti. Nazadnje, se za namene te uredbe razvoj izdelkov z digitalnimi elementi, ki štejejo za prosto in odprtokodno programsko opremo, s strani neprofitnih organizacij ne bi smel šteti za komercialno dejavnost, če je organizacija ustanovljena na način, ki zagotavlja, da se vsi prihodki po stroških uporabijo za doseganje neprofitnih ciljev. Ta uredba se ne uporablja za fizične ali pravne osebe, ki z izvorno kodo prispevajo k izdelkom z digitalnimi elementi, ki se štejejo za prosto in odprtokodno programsko opremo, za katere niso odgovorni.

(19) Ob upoštevanju pomena, ki ga imajo za kibernetsko varnost številni izdelki z digitalnimi elementi, ki štejejo za prosto in odprtokodno programsko opremo in ki se izdajo, vendar niso dostopni na trgu v smislu te uredbe, bi morala za pravne osebe, ki trajno zagotavljajo podporo za razvoj takih izdelkov, ki so namenjeni komercialnim dejavnostim, in ki imajo glavno vlogo pri zagotavljanju smotrnosti teh izdelkov (v nadaljnjem besedilu: upravljavci odprtokodne programske opreme), veljati enostavnejša in prilagojena regulativna ureditev. Upravljavci odprtokodne programske opreme vključujejo nekatere fundacije in subjekte, ki razvijajo in izdajajo prosto in odprtokodno programsko opremo v poslovnem okviru, vključno z neprofitnimi subjekti. Regulativna ureditev bi morala upoštevati njihovo posebno naravo in združljivost z vrsto naloženih obveznosti. Zajemati bi morala le izdelke z digitalnimi elementi, ki štejejo za prosto in odprtokodno programsko opremo in ki so na koncu namenjeni komercialnim dejavnostim, kot je vključevanje v komercialne storitve ali v monetizirane izdelke z digitalnimi elementi. Za namene navedene regulativne ureditve namera za vključitev v monetizirane izdelke z digitalnimi elementi vključuje primere, kadar proizvajalci, ki sestavni del vgradijo v svoje izdelke z digitalnimi elementi, bodisi redno prispevajo k razvoju tega sestavnega dela bodisi zagotavljajo redno finančno pomoč, da se zagotovi neprekinjeno delovanje programske opreme. Zagotavljanje trajne podpore razvoju izdelka z digitalnimi elementi med drugim vključuje gostovanje in upravljanje platform za sodelovanje pri razvoju programske opreme, gostovanje izvorne kode ali programske opreme, urejanje ali upravljanje izdelkov z digitalnimi elementi, ki štejejo za prosto in odprtokodno programsko opremo, ter usmerjanje razvoja takih izdelkov. Glede na to, da enostavnejša in prilagojena regulativna ureditev za tiste, ki delujejo kot upravljavci odprtokodne programske opreme, ne določa enakih obveznosti kot za tiste, ki delujejo kot proizvajalci na podlagi te uredbe, jim ne bi smelo biti dovoljeno, da na izdelke z digitalnimi elementi, katerih razvoj podpirajo, namestijo oznako CE.

(20) Gostovanje izdelkov z digitalnimi elementi v odprtih repozitorijih, tudi preko upravljavcev paketov ali na platformah za sodelovanje, samo po sebi ne pomeni omogočanja dostopnosti izdelka z digitalnimi elementi na trgu. Ponudniki takih storitev bi se morali šteti za distributerje le, če omogočajo dostopnost take programske opreme na trgu in jo zato dobavljajo za distribucijo ali uporabo na trgu Unije v okviru gospodarske dejavnosti.

(21) Da bi podprli in olajšali potrebno skrbnost proizvajalcev, ki v svoje izdelke z digitalnimi elementi vključujejo sestavne dele proste in odprtokodne programske opreme, za katere ne veljajo bistvene zahteve glede kibernetske varnosti iz te uredbe, bi morala imeti Komisija možnost vzpostavitve prostovoljnih programov varnostnih potrdil, bodisi z delegiranim aktom, ki dopolnjuje to uredbo, bodisi z zahtevo za evropsko certifikacijsko shemo za kibernetsko varnost na podlagi člena 48 Uredbe (EU) 2019/881, ki upošteva posebnosti modelov razvoja proste in odprtokodne programske opreme. Programi varnostnih potrdil bi morali biti zasnovani tako, da lahko proces za varnostno potrdilo sprožijo ali financirajo ne le fizične ali pravne osebe, ki razvijajo izdelek z digitalnimi elementi, ki se šteje za prosto in odprtokodno programsko opremo, ali prispevajo k njemu, temveč tudi tretje osebe, kot so proizvajalci, ki take izdelke vključujejo v svoje izdelke z digitalnimi elementi, uporabniki ali javna uprava Unije oziroma nacionalne javne uprave.

(22) Glede na cilje javne kibernetske varnosti iz te uredbe in za izboljšanje situacijskega zavedanja držav članic glede odvisnosti Unije od sestavnih delov programske opreme ter zlasti sestavnih delov potencialno proste in odprtokodne programske opreme bi morala imeti posebna skupina za upravno sodelovanje (v nadaljnjem besedilu: skupina ADCO), ustanovljena s to uredbo, možnost, da se odloči, da bo skupaj izvedla oceno odvisnosti Unije. Organi za nadzor trga bi morali imeti možnost, da od proizvajalcev kategorij izdelkov z digitalnimi elementi, ki jih določi skupina ADCO, zahtevajo predložitev kosovnic za programsko opremo, ki so jo razvili na podlagi te uredbe. Za zaščito zaupnosti kosovnic za programsko opremo bi morali organi za nadzor trga skupini ADCO anonimizirano in v združeni obliki predložiti ustrezne informacije o odvisnostih.

(23) Učinkovitost izvajanja te uredbe bo odvisna tudi od razpoložljivosti ustreznih znanj in spretnosti na področju kibernetske varnosti. Na ravni Unije so različni programski in politični dokumenti, vključno s sporočilom Komisije z dne 18. aprila 2023 o zapolnitvi vrzeli na področju strokovnjakov za kibernetsko varnost za povečanje konkurenčnosti, rasti in odpornosti EU ter sklepi Sveta z dne 22. maja 2023 o politiki EU za kibernetsko obrambo, potrdili vrzel v znanjih in spretnostih na področju kibernetske varnosti v Uniji in potrebo po prednostnem obravnavanju takih izzivov v javnem in zasebnem sektorju. Za učinkovito izvajanje te uredbe bi morale države članice poskrbeti, da bo na voljo dovolj sredstev za ustrezno kadrovanje organov za nadzor trga in organov za ugotavljanje skladnosti, tako da bodo lahko opravljali svoje naloge iz te uredbe. Ti ukrepi bi morali povečati mobilnost delovne sile na področju kibernetske varnosti in z njimi povezanih poklicnih poti. Prispevati bi morali tudi k temu, da bi delovna sila na področju kibernetske varnosti postala odpornejša in bolj vključujoča, tudi v smislu spolov. Države članice bi zato morale sprejeti ukrepe, ki bodo omogočali, da te naloge izvajajo ustrezno usposobljeni strokovnjaki s potrebnimi znanji in spretnostmi na področju kibernetske varnosti. Podobno bi morali proizvajalci zagotoviti, da ima njihovo osebje potrebna znanja in spretnosti za izpolnjevanje obveznosti iz te uredbe. Države članice in Komisija bi morale v skladu s svojimi pooblastili in pristojnostmi ter posebnimi nalogami, ki so jim dodeljene s to uredbo, sprejeti ukrepe za podporo proizvajalcev, zlasti mikropodjetij ter malih in srednjih podjetij, vključno z zagonskimi podjetji, tudi na področjih, kot je razvoj znanj in spretnosti, da bi izpolnile svoje obveznosti iz te uredbe. Glede na to, da Direktiva (EU) 2022/2555 od držav članic poleg tega zahteva, da v okviru svojih nacionalnih strategij za kibernetsko varnost sprejmejo politike za spodbujanje in razvoj usposabljanja o kibernetski varnosti ter znanje in spretnosti na področju kibernetske varnosti, lahko države članice pri sprejemanju takih strategij upoštevajo tudi potrebe po znanjih in spretnostih na področju kibernetske varnosti, ki izhajajo iz te uredbe, vključno s tistimi, ki so povezane s prekvalifikacijo in izpopolnjevanjem.

(24) Varen internet je nepogrešljiv za delovanje kritične infrastrukture in družbe kot celote. Direktiva (EU) 2022/2555 je namenjena zagotovitvi visoke ravni kibernetske varnosti storitev, ki jih opravljajo bistveni in pomembni subjekti iz člena 3 navedene direktive, vključno s ponudniki digitalne infrastrukture, ki podpirajo osnovne funkcije odprtega interneta ter zagotavljajo dostop do interneta in opravljajo internetne storitve. Zato je pomembno, da se izdelki z digitalnimi elementi, ki jih ponudniki digitalne infrastrukture potrebujejo za zagotavljanje delovanja interneta, razvijajo varno in spoštujejo uveljavljene standarde internetne varnosti. Ta uredba, ki se uporablja za vse izdelke strojne in programske opreme z možnostjo povezave, je namenjena tudi olajšanju skladnosti ponudnikov digitalne infrastrukture z zahtevami glede dobavne verige na podlagi Direktive (EU) 2022/2555 z zagotavljanjem varnega razvoja izdelkov z digitalnimi elementi, ki jih ti ponudniki uporabljajo za zagotavljanje svojih storitev, in njihovega dostopa do pravočasnih varnostnih posodobitev za take izdelke.

(25) Uredba (EU) 2017/745 Evropskega parlamenta in Sveta ([9]) določa pravila o medicinskih pripomočkih, Uredba (EU) 2017/746 Evropskega parlamenta in Sveta ([10]) pa pravila o in vitro diagnostičnih medicinskih pripomočkih. S tema uredbama se obravnavajo tveganja za kibernetsko varnost in upoštevajo posebni pristopi, ki so obravnavani tudi v tej uredbi. Natančneje, uredbi (EU) 2017/745 in (EU) 2017/746 določata bistvene zahteve za medicinske pripomočke, ki delujejo prek elektronskega sistema ali so sami programska oprema. Zajemata tudi nekatere vrste nevgrajene programske opreme in pristop na podlagi celotnega življenjskega cikla. V skladu s temi zahtevami morajo proizvajalci pri razvoju in izdelavi svojih izdelkov uporabljati načela obvladovanja tveganja in določiti zahteve za varnostne ukrepe v zvezi z IT ter ustrezne postopke ugotavljanja skladnosti. Poleg tega so od decembra 2019 na voljo posebne smernice o kibernetski varnosti medicinskih pripomočkov, ki proizvajalcem medicinskih pripomočkov, vključno z in vitro diagnostičnimi pripomočki, zagotavljajo usmeritve za izpolnjevanje vseh ustreznih bistvenih zahtev, določenih v Prilogi I k navedenima uredbama v zvezi s kibernetsko varnostjo. Zato se ta uredba ne bi smela uporabljati za izdelke z digitalnimi elementi, za katere se uporablja katera koli od navedenih uredb.

(26) Izdelki z digitalnimi elementi, ki se razvijajo ali spremenijo izključno za namene nacionalne varnosti ali obrambne namene, ali izdelki, ki so izrecno namenjeni obdelavi tajnih podatkov, ne spadajo na področje uporabe te uredbe. Države članice se spodbuja, naj za te izdelke zagotovijo enako ali višjo raven varstva kot za tiste izdelke, ki spadajo na področje uporabe te uredbe.

([9]) Uredba (EU) 2017/745 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o medicinskih pripomočkih, spremembi Direktive 2001/83/ES, Uredbe (ES) št. 178/2002 in Uredbe (ES) št. 1223/2009 ter razveljavitvi direktiv Sveta 90/385/EGS in 93/42/EGS (UL L 117, 5.5.2017, str. 1).

([10]) Uredba (EU) 2017/746 Evropskega parlamenta in Sveta z dne 5. aprila 2017 o in vitro diagnostičnih medicinskih pripomočkih ter razveljavitvi Direktive 98/79/ES in Sklepa Komisije 2010/227/EU (UL L 117, 5.5.2017, str. 176).

(27) Uredba (EU) 2019/2144 Evropskega parlamenta in Sveta ([11]) določa zahteve za homologacijo vozil ter njihovih sistemov in sestavnih delov, pri čemer uvaja nekatere zahteve glede kibernetske varnosti, vključno glede delovanja certificiranega sistema za upravljanje kibernetske varnosti in posodobitev programske opreme, zajema politike in postopke organizacij za tveganja za kibernetsko varnost, povezana s celotnim življenjskim ciklom vozil, opreme in storitev, v skladu z veljavnimi pravilniki Združenih narodov o tehničnih specifikacijah in kibernetski varnosti, zlasti s Pravilnikom OZN št. 155 – Enotne določbe o homologaciji vozil glede na kibernetsko varnost in sistem za upravljanje kibernetske varnosti ([12]), ter določa posebne postopke ugotavljanja skladnosti. Na področju letalstva je glavni cilj Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta ([13]) vzpostaviti in ohranjati visoko enotno raven varnosti v civilnem letalstvu v Uniji. Z njo je vzpostavljen okvir za bistvene zahteve glede plovnosti za aeronavtične izdelke, dele in opremo, vključno s programsko opremo, ki zajema obveznosti zaščite pred tveganji za varnost informacij. S postopkom certificiranja na podlagi Uredbe (EU) 2018/1139 se zagotovi raven zanesljivosti, ki je cilj te uredbe. Zato se bistvene zahteve glede kibernetske varnosti in postopki ugotavljanja skladnosti iz te uredbe ne bi smeli uporabljati za izdelke z digitalnimi elementi, za katere se uporablja Uredba (EU) 2019/2144, in izdelke, certificirane v skladu z Uredbo (EU) 2018/1139.

(28) Ta uredba določa horizontalna pravila glede kibernetske varnosti, ki niso specifična za posamezne sektorje ali izdelke z digitalnimi elementi. Ne glede na to se lahko uvedejo sektorska pravila Unije ali pravila Unije za posamezne izdelke, s katerimi se določijo zahteve, ki se nanašajo na vsa ali nekatera tveganja, zajeta z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe. V takih primerih se lahko uporaba te uredbe za izdelke z digitalnimi elementi, zajete z drugimi pravili Unije, s katerimi so določene zahteve, ki se nanašajo na vsa ali nekatera tveganja, zajeta z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I k tej uredbi, omeji ali izključi, kadar je taka omejitev ali izključitev v skladu s splošnim regulativnim okvirom, ki se uporablja za navedene izdelke, in kadar se s sektorskimi pravili doseže vsaj enaka raven varstva, kot je določena s to uredbo. Na Komisijo bi bilo treba prenesti pooblastilo za sprejemanje delegiranih aktov za dopolnitev te uredbe z opredelitvijo takih izdelkov in pravil. Ta uredba za obstoječe pravo Unije, v zvezi s katero bi se morale uporabljati take omejitve ali izključitve, vsebuje posebne določbe za pojasnitev njene povezave z navedenim pravom Unije.

(29) Da bi zagotovili učinkovito popravilo izdelkov z digitalnimi elementi, ki so dostopni na trgu, in podaljšanje njihove trajnosti, bi bilo treba določiti izjemo za rezervne dele. Ta izjema bi morala veljati za rezervne dele, katerih namen je popravilo obstoječih izdelkov, ki so bili dani na voljo pred datumom začetka uporabe te uredbe, kot tudi za nadomestne dele, za katere je bil že opravljen postopek ugotavljanja skladnosti na podlagi te uredbe.

(30) Delegirana uredba Komisije (EU) 2022/30 ([14]) določa, da se številne bistvene zahteve iz člena 3(3), točke (d), (e) in (f) Direktive 2014/53/EU Evropskega parlamenta in Sveta ([15]), ki se nanašajo na škodo na omrežju in zlorabo omrežnih virov, osebne podatke in zasebnost ter goljufe, uporabljajo za določeno radijsko opremo. Izvedbeni sklep Komisije C(2022) 5637 dne 5. avgusta 2022 o zahtevi za standardizacijo Evropskemu odboru za standardizacijo in Evropskemu odboru za elektrotehnično standardizacijo določa zahteve za razvoj posebnih standardov, s katerimi je podrobneje določeno, kako bi bilo treba obravnavati te tri bistvene zahteve. Bistvene zahteve glede kibernetske varnosti iz te uredbe vključujejo vse elemente bistvenih zahtev iz člena 3(3), točke (d), (e) in (f), Direktive

([11]) Uredba (EU) 2019/2144 Evropskega parlamenta in Sveta z dne 27. novembra 2019 o zahtevah za homologacijo motornih vozil in njihovih priklopnikov ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila, v zvezi z njihovo splošno varnostjo in zaščito potnikov v vozilu ter izpostavljenih udeležencev v cestnem prometu in o spremembi Uredbe (EU) 2018/858 Evropskega parlamenta in Sveta ter razveljavitvi uredb (ES) št. 78/2009, (ES) št. 79/2009 in (ES) št. 661/2009 Evropskega parlamenta in Sveta in uredb Komisije (ES) št. 631/2009, (EU) št. 406/2010, (EU) št. 672/2010, (EU) št. 1003/2010, (EU) št. 1005/2010, (EU) št. 1008/2010, (EU) št. 1009/2010, (EU) št. 19/2011, (EU) št. 109/2011, (EU) št. 458/2011, (EU) št. 65/2012, (EU) št. 130/2012, (EU) št. 347/2012, (EU) št. 351/2012, (EU) št. 1230/2012 in (EU) 2015/166 (UL L 325, 16.12.2019, str. 1).

([12]) UL L 82, 9.3.2021, str. 30.

([13]) Uredba (EU) 2018/1139 Evropskega parlamenta in Sveta z dne 4. julija 2018 o skupnih pravilih na področju civilnega letalstva in ustanovitvi Agencije Evropske unije za varnost v letalstvu ter spremembi uredb (ES) št. 2111/2005, (ES) št. 1008/2008, (EU) št. 996/2010, (EU) št. 376/2014 ter direktiv 2014/30/EU in 2014/53/EU Evropskega parlamenta in Sveta ter razveljavitvi uredb (ES) št. 552/2004 in (ES) št. 216/2008 Evropskega parlamenta in Sveta ter Uredbe Sveta (EGS) št. 3922/91 (UL L 212, 22.8.2018, str. 1).

([14]) Delegirana uredba Komisije (EU) 2022/30 z dne 29. oktobra 2021 o dopolnitvi Direktive 2014/53/EU Evropskega parlamenta in Sveta v zvezi z uporabo bistvenih zahtev iz člena 3(3), točke (d), (e) in (f), navedene direktive (UL L 7, 12.1.2022, str. 6).

([15]) Direktiva 2014/53/EU Evropskega parlamenta in Sveta z dne 16. aprila 2014 o harmonizaciji zakonodaj držav članic v zvezi z dostopnostjo radijske opreme na trgu in razveljavitvi Direktive 1999/5/ES (UL L 153, 22.5.2014, str. 62).

2014/53/EU. Poleg tega so bistvene zahteve glede kibernetske varnosti iz te uredbe usklajene s cilji zahtev za posebne standarde, vključene v navedeno zahtevo za standardizacijo. Ko torej Komisija razveljavi ali spremeni Delegirano uredbo Komisije (EU) 2022/30 in se navedena delegirana uredba zato preneha uporabljati za nekatere izdelke, za katere se uporablja ta uredba, bi morale Komisija in evropske organizacije za standardizacijo pri pripravi in razvoju harmoniziranih standardov za olajšanje izvajanja te uredbe upoštevati delo za standardizacijo, opravljeno v okviru Izvedbenega sklepa C(2022) 5637. Komisija bi morala v prehodnem obdobju za uporabo te uredbe proizvajalcem, za katere velja ta uredba in Delegirana uredba (EU) 2022/30, zagotoviti usmeritve, s pomočjo katerih bi jim olajšala dokazovanje skladnosti z obema uredbama.

(31) Direktiva (EU) 2024/2853 Evropskega parlamenta in Sveta ([16]) dopolnjuje to uredbo. Navedena direktiva določa pravila o odgovornosti za izdelke z napako, da lahko oškodovanci zahtevajo odškodnino za škodo, ki jo povzročijo izdelki z napako. Določa načelo, da je proizvajalec izdelka odgovoren za škodo, nastalo zaradi pomanjkanja varnosti njegovega izdelka, ne glede na krivdo (objektivna odgovornost). Kadar tako pomanjkanje varnosti vključuje neobstoj varnostnih posodobitev po dajanju izdelka na trg in zaradi tega nastane škoda, se lahko uveljavlja odgovornost proizvajalca. V tej uredbi bi bilo treba določiti obveznosti proizvajalcev, ki se nanašajo na zagotavljanje takih varnostnih posodobitev.

(32) Ta uredba ne bi smela posegati v Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta ([17]), vključno z določbami za uvedbo mehanizmov certificiranja za varstvo podatkov ter pečatov in označb za varstvo podatkov, namenjenih dokazovanju, da so dejanja obdelave s strani upravljavcev in obdelovalcev v skladu z navedeno uredbo. Taka dejanja so lahko vključena v izdelek z digitalnimi elementi. Vgrajeno in privzeto varstvo podatkov ter kibernetska varnost na splošno so ključni elementi Uredbe (EU) 2016/679. Bistvene zahteve glede kibernetske varnosti iz te uredbe naj bi z zaščito potrošnikov in organizacij pred tveganji za kibernetsko varnost prispevale tudi k izboljšanju varstva osebnih podatkov in zasebnosti posameznikov. V okviru sodelovanja med Komisijo, evropskimi organizacijami za standardizacijo, Agencijo Evropske unije za kibernetsko varnost (v nadaljnjem besedilu: agencija ENISA), Evropskim odborom za varstvo podatkov, ustanovljenim z Uredbo (EU) 2016/679, in nacionalnimi nadzornimi organi za varstvo podatkov bi bilo treba obravnavati sinergije glede standardizacije in certificiranja v zvezi z vidiki kibernetske varnosti. Poleg tega bi bilo treba ustvariti sinergije med to uredbo in pravom Unije o varstvu podatkov na področju nadzora trga in izvrševanja. V ta namen bi morali nacionalni organi za nadzor trga, imenovani na podlagi te uredbe, sodelovati z organi, pristojnimi za nadzor uporabe prava Unije o varstvu podatkov. Slednji bi morali imeti tudi dostop do informacij, pomembnih za opravljanje njihovih nalog.

(33) Ponudniki evropske denarnice za digitalno identiteto iz člena 5a(2) Uredbe (EU) št. 910/2014 Evropskega parlamenta in Sveta ([18]), bi morali izpolnjevati horizontalne bistvene zahteve glede kibernetske varnosti iz te uredbe in posebne varnostne zahteve iz člena 5a Uredbe (EU) št. 910/2014, če njihovi izdelki spadajo na področje uporabe te uredbe. Za olajšanje zagotavljanja skladnosti bi morali imeti ponudniki denarnice možnost, da dokažejo skladnost evropskih denarnic za digitalno identiteto z zahtevami iz te uredbe in Uredbe (EU) št. 910/2014 s certificiranjem svojih izdelkov v okviru evropske certifikacijske sheme kibernetske varnosti, vzpostavljene na podlagi Uredbe (EU) 2019/881, za katero je Komisija z delegiranimi akti oblikovala domnevo o skladnosti s to uredbo, kolikor certifikat ali njegovi deli zajemajo te zahteve.

(34) Pri vključevanju sestavnih delov, pridobljenih od tretjih oseb, v izdelke z digitalnimi elementi v fazi zasnove in razvoja bi morali proizvajalci za zagotovitev, da so izdelki zasnovani, razviti in proizvedeni v skladu z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe, ravnati s potrebno skrbnostjo v zvezi s temi sestavnimi deli, vključno s sestavnimi deli proste in odprtokodne programske opreme, ki niso bili dani na trg. Ustrezna raven

([16]) Direktiva (EU) 2024/2853 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o odgovornosti za proizvode z napako in razveljavitvi Direktive Sveta 85/374/EGS (UL L, 2024/2853, 18.11.2024, ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

([17]) 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).

([18]) 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).

potrebne skrbnosti je odvisna od narave in stopnje kibernetskega tveganja za posamezni sestavni del, in bi morala v ta namen upoštevati enega ali več naslednjih ukrepov: preverjanje, kot je ustrezno, ali je proizvajalec sestavnega dela dokazal skladnost s to uredbo, vključno s preverjanjem, ali ima sestavni del že oznako CE; preverjanje, ali je sestavni del deležen rednih varnostnih posodobitev, na primer tako, da se preveri zgodovina njegovih varnostnih posodobitev; preverjanje, da sestavni del ne vsebuje ranljivosti, evidentiranih v evropski podatkovni zbirki ranljivosti, vzpostavljeni na podlagi člena 12(2) Direktive (EU) 2022/2555, ali drugih javno dostopnih podatkovnih zbirkah ranljivosti; ali izvedba dodatnih varnostnih preskusov. Obveznosti glede obravnavanja ranljivosti iz te uredbe, ki jih morajo proizvajalci izpolnjevati pri dajanju izdelka z digitalnimi elementi na trg in v obdobju podpore, veljajo za izdelke z digitalnimi elementi v celoti, vključno z vsemi vgrajenimi sestavnimi deli. Kadar proizvajalec izdelka z digitalnimi elementi pri izvajanju potrebne skrbnosti ugotovi ranljivost v sestavnem delu, vključno s prostim in odprtokodnim sestavnim delom, bi moral obvestiti osebo ali subjekt, ki proizvaja ali vzdržuje sestavni del, obravnavati in odpraviti ranljivost ter, kadar je ustrezno, tej osebi ali subjektu zagotoviti uporabljeno varnostno rešitev.

(35) Takoj po prehodnem obdobju za uporabo te uredbe proizvajalec izdelka z digitalnimi elementi, ki vključuje enega ali več sestavnih delov, pridobljenih od tretjih oseb, za katere prav tako velja ta uredba, v okviru svoje obveznosti potrebne skrbnosti morda ne bo mogel preveriti, ali so proizvajalci teh sestavnih delov dokazali skladnost s to uredbo, tako da na primer preveri, ali imajo sestavni deli že oznako CE. To se lahko zgodi, če so bili sestavni deli vgrajeni, preden se ta uredba začne uporabljati za proizvajalce teh sestavnih delov. V takem primeru bi moral proizvajalec, ki vgrajuje take sestavne dele, ravnati s potrebno skrbnostjo na druge načine.

(36) Izdelki z digitalnimi elementi bi morali imeti oznako CE, ki vidno, čitljivo in neizbrisno označuje njihovo skladnost s to uredbo, da se omogoči njihov prosti pretok na notranjem trgu. Države članice ne bi smele neupravičeno ovirati dajanja na trg izdelkov z digitalnimi elementi, ki izpolnjujejo zahteve iz te uredbe in imajo oznako CE. Poleg tega države članice na sejmih, razstavah in predstavitvah ali podobnih dogodkih ne bi smele preprečiti predstavitve ali uporabe izdelka z digitalnimi elementi, ki ni skladen s to uredbo, vključno z njegovimi prototipi, če je izdelek opremljen z vidno oznako, ki jasno označuje, da ni skladen s to uredbo in da ne bo dan na trg, dokler ne bo skladen z njo.

(37) Da bi lahko proizvajalci pred ugotavljanjem skladnosti njihovih izdelkov z digitalnimi elementi izdali programsko opremo za namene preskušanja, države članice ne bi smele preprečiti dostopnosti nedokončane programske opreme, kakor so alfa ali beta različice ali predizdaje, če je nedokončana programska oprema dostopna samo za obdobje, potrebno za njeno preskušanje in zbiranje povratnih informacij. Proizvajalci bi morali zagotoviti, da se programska oprema, do katere zagotovijo dostop pod temi pogoji, izda šele po oceni tveganja in da v čim večjem obsegu izpolnjuje varnostne zahteve v zvezi z lastnostmi izdelkov z digitalnimi elementi, določene s to uredbo. Poleg tega bi morali proizvajalci v čim večjem obsegu izpolnjevati zahteve glede obravnavanja ranljivosti. Proizvajalci uporabnikov ne bi smeli prisiliti, da svoje izdelke nadgradijo na različice, izdane samo za namene preskušanja.

(38) Za zagotovitev, da izdelki z digitalnimi elementi, ko so dani na trg, ne pomenijo tveganja za kibernetsko varnost za osebe in organizacije, bi bilo treba za take izdelke določiti bistvene zahteve glede kibernetske varnosti. Te bistvene zahteve glede kibernetske varnosti, vključno z zahtevami za ravnanje z ranljivostmi, se uporabljajo za vsak posamezen izdelek z digitalnimi elementi, ko je dan na trg, ne glede na to, ali se izdelek z digitalnimi elementi proizvaja kot posamezna enota ali serija. Za posamezne vrste izdelkov bi moral tako na primer vsak posamezni izdelek z digitalnimi elementi, v času, ko je dan na trg, že prejeti vse varnostne popravke ali posodobitve, ki so na voljo za obravnavo ustreznih varnostnih vprašanj. Kadar se izdelki z digitalnimi elementi pozneje fizično ali digitalno spremenijo na način, ki ga izdelovalec v prvotni oceni tveganja ni predvidel in ki bi lahko pomenil, da ne izpolnjujejo več ustreznih bistvenih zahtev glede kibernetske varnosti, bi bilo treba spremembo šteti za bistveno. Na primer, popravila programske opreme se lahko štejejo za enakovredne vzdrževalnim postopkom, če izdelka z digitalnimi elementi, ki je že na trgu, ne spremenijo tako, da bi to vplivalo na skladnost z veljavnimi zahtevami ali da bi se lahko spremenil predviden namen, za katerega je bil izdelek ocenjen.

(39) Podobno kot pri fizičnih popravilih ali spremembah bi bilo treba šteti, da je izdelek z digitalnimi elementi bistveno spremenjen s spremembo programske opreme, kadar se s posodobitvijo programske opreme spremeni predviden namen tega izdelka in teh sprememb proizvajalec ni predvideval v začetni oceni tveganja ali kadar se zaradi

posodobitve programske opreme spremeni narava nevarnosti ali poviša raven tveganja, posodobljena različica izdelka pa je na voljo na trgu. Kadar varnostna posodobitev, namenjena zmanjšanju stopnje tveganja za kibernetsko varnost izdelka z digitalnimi elementi, ne spreminja predvidenega namena izdelka z digitalnimi elementi, se ne šteje za bistveno spremembo. To običajno vključuje primere, kadar varnostna posodobitev vključuje le manjše prilagoditve izvorne kode. To bi se na primer lahko zgodilo, kadar se varnostna posodobitev nanaša na znano ranljivost, vključno s primeri, kadar se funkcije ali zmogljivosti izdelka z digitalnimi elementi spremenijo samo zato, da bi zmanjšali stopnjo tveganja za kibernetsko varnost. Podobno se manjša posodobitev funkcij, kot je vizualna izboljšava, dodajanje novih piktogramov ali jezikov v uporabniški vmesnik, na splošno ne bi smela šteti za bistveno spremembo. Nasprotno pa bi morali posodobitev funkcij, ki spremeni prvotne predvidene funkcije ali vrsto ali zmogljivost izdelka z digitalnimi elementi in izpolnjuje zgornja merila, šteti za bistveno spremembo, saj dodajanje novih funkcij običajno povzroči širšo napadno površino, s čimer se poveča tveganje za kibernetsko varnost. To se lahko na primer zgodi, kadar se vlogi doda nov vhodni element, ki od proizvajalca zahteva, da zagotovi ustrezno validacijo vhodnih podatkov. Pri ocenjevanju, ali se posodobitev funkcije šteje za bistveno spremembo, ni pomembno, ali je zagotovljena kot ločena posodobitev ali v kombinaciji z varnostno posodobitvijo. Komisija bi morala izdati usmeritve o tem, kako določiti, kaj je bistvena sprememba.

(40) Ob upoštevanju ponavljajoče se narave razvoja programske opreme bi morali proizvajalci, ki so dali na trg poznejše različice izdelka programske opreme, zaradi naknadne bistvene spremembe tega izdelka imeti možnost zagotoviti varnostne posodobitve za obdobje podpore samo za različico programske opreme, ki so jo nazadnje dali na trg. To bi jim moralo biti omogočeno le, če imajo uporabniki zadevnih prejšnjih različic izdelka dostop do različice izdelka, ki je bila nazadnje dana na trg brezplačno, in nimajo dodatnih stroškov zaradi prilagoditve okolja strojne ali programske opreme, v katerem upravljajo izdelek. To bi lahko na primer veljalo, kadar za nadgradnjo operacijskega sistema namiznih računalnikov ni potrebna nova strojna oprema, na primer hitrejša osrednja procesna enota ali več pomnilnika. Kljub temu bi moral proizvajalec v obdobju podpore še naprej izpolnjevati druge zahteve glede obravnavanja ranljivosti, kot so politika o usklajenem razkrivanju ranljivosti ali ukrepi za lažjo izmenjavo informacij o morebitnih ranljivostih za vse nadaljnje bistveno spremenjene različice programske opreme, dane na trg. Proizvajalci bi morali imeti možnost zagotoviti manjše posodobitve varnosti ali funkcij, ki ne pomenijo bistvene spremembe, le za najnovejšo različico ali podrazličico programske opreme, ki ni bila bistveno spremenjena. Hkrati bi moral proizvajalec, kadar strojna oprema, kot je pametni telefon, ni združljiv z najnovejšo različico operacijskega sistema, s katerim je bil prvotno dobavljen, še naprej zagotavljati varnostne posodobitve vsaj za najnovejšo združljivo različico operacijskega sistema za obdobje podpore.

(41) V skladu s splošno uveljavljenim pojmom bistvene spremembe za izdelke, ki jih ureja harmonizacijska zakonodaja Unije, je primerno, da se za izdelek z digitalnimi elementi ob bistveni spremembi, ki bi lahko vplivala na skladnost izdelka z digitalnimi elementi s to uredbo, ali ob spremembi predvidenega namena tega izdelka preveri skladnost izdelka z digitalnimi elementi in po potrebi izvede novo ugotavljanje skladnosti. Kadar je ustrezno, če proizvajalec opravi ugotavljanje skladnosti, pri katerem sodeluje tretja oseba, bi bilo treba tretjo osebo obvestiti o spremembi, ki lahko pomeni bistveno spremembo.

(42) Kadar za izdelek z digitalnimi elementi veljajo „prenovitev“, „vzdrževanje“ in „popravilo“ kakor so opredeljeni v členu 2, točke 18, 19 in 20 Uredbe (EU) 2024/1781 Evropskega parlamenta in Sveta ([19]), to ne povzroči nujno bistvene spremembe izdelka, če se na primer predviden namen in funkcije ter raven tveganja ne spremenijo. Nadgradnja izdelka z digitalnimi elementi, ki jo izvede proizvajalec, pa lahko povzroči spremembe zasnove in razvoja izdelka ter tako vpliva na njegov predviden namen in skladnost z zahtevami iz te uredbe.

(43) Izdelke z digitalnimi elementi bi bilo treba šteti za pomembne, če je lahko negativni vpliv izrabljanja morebitnih ranljivosti izdelka v zvezi s kibernetsko varnostjo resen, med drugim zaradi funkcij, povezanih s kibernetsko varnostjo, ali funkcije z znatnim tveganjem škodljivih učinkov v smislu njene intenzivnosti in zmožnosti motenj, nadzora ali povzročanja škode velikemu številu drugih izdelkov z digitalnimi elementi ali zdravju, zaščiti ali varnosti njegovih uporabnikov z neposredno manipulacijo, kot je funkcija centralnega sistema, vključno z upravljanjem omrežja, nadzorom konfiguracije, virtualizacijo ali obdelavo osebnih podatkov. Zlasti lahko ranljivosti izdelkov z digitalnimi elementi, ki vključujejo funkcije, povezane s kibernetsko varnostjo, kakor so upravitelji zagona, povzročijo širjenje varnostnih težav po vsej dobavni verigi. Poleg tega se lahko resnost vpliva kibernetskega incidenta

([19]) Uredba (EU) 2024/1781 Evropskega parlamenta in Sveta z dne 13. junija 2024 o vzpostavitvi okvira za določitev zahtev za okoljsko primerno zasnovo za trajnostne izdelke, spremembi Direktive (EU) 2020/1828 in Uredbe (EU) 2023/1542 ter razveljavitvi Direktive 2009/125/ES (UL L, 2024/1781, 28.6.2024, ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

poveča, kadar izdelek opravlja predvsem funkcijo osrednjega sistema, vključno z upravljanjem omrežja, nadzorom konfiguracije, virtualizacijo ali obdelavo osebnih podatkov.

(44) Za določene kategorije izdelkov z digitalnimi elementi bi se morali uporabljati strožji postopki ugotavljanja skladnosti, pri čemer bi bilo treba ohraniti sorazmeren pristop. V ta namen bi bilo treba pomembne izdelke z digitalnimi elementi razdeliti v dva razreda, da se izrazi raven tveganja za kibernetsko varnost, povezana s temi kategorijami izdelkov. Incident v zvezi s pomembnimi izdelki z digitalnimi elementi iz razreda II bi lahko imel večje negativne učinke kot incident v zvezi s pomembnimi izdelki z digitalnimi elementi iz razreda I, na primer zaradi narave njihove funkcije, povezane s kibernetsko varnostjo, ali opravljanja druge funkcije, pri kateri obstaja znatno tveganje škodljivih učinkov. Kot znak takih večjih negativnih vplivov bi lahko izdelki z digitalnimi elementi iz razreda II opravljali funkcijo, povezano s kibernetsko varnostjo, ali drugo funkcijo, ki pomeni znatno tveganje škodljivih učinkov, ki je večje kot pri tistih iz razreda I, ali izpolnjevali obe zgoraj navedeni merili. Za pomembne izdelke z digitalnimi elementi iz razreda II bi zato moral veljati strožji postopek ugotavljanja skladnosti.

(45) Pomembne izdelke z digitalnimi elementi iz te uredbe bi bilo treba razumeti kot izdelke z osnovnimi funkcijami, ki spadajo med osnovne funkcije kategorije pomembnih izdelkov z digitalnimi elementi, ki je določena v tej uredbi. Na primer v tej uredbi so v razredu II določene kategorije pomembnih izdelkov z digitalnimi elementi, ki so na podlagi svoje osnovne funkcije opredeljeni kot požarni zidovi ali sistemi za odkrivanje ali preprečevanje vdorov. Zato se v zvezi s požarnimi zidovi ali sistemi za odkrivanje ali preprečevanje vdorov izvaja obvezno ugotavljanje skladnosti, ki ga opravi tretja oseba. To ne velja za druge izdelke z digitalnimi elementi, ki niso opredeljeni kot pomembni izdelki z digitalnimi elementi, in v katere se lahko vgradijo požarni zidovi ali sistemi za odkrivanje ali preprečevanje vdorov. Komisija bi morala sprejeti izvedbeni akt za opredelitev tehničnega opisa kategorij pomembnih izdelkov z digitalnimi elementi, ki spadajo v razreda I in II, kot je določeno v tej uredbi.

(46) Kategorije kritičnih izdelkov z digitalnimi elementi iz te uredbe imajo funkcijo, povezano s kibernetsko varnostjo, in opravljajo funkcijo, ki pomeni znatno tveganje škodljivih učinkov v smislu intenzivnosti in zmožnosti motenj, nadzora ali povzročanja škode velikemu številu drugih izdelkov z digitalnimi elementi z neposredno manipulacijo. Poleg tega se navedene kategorije izdelkov z digitalnimi elementi štejejo za kritične odvisnosti za bistvene subjekte iz člena 3(1) Direktive (EU) 2022/2555. Kategorije kritičnih izdelkov z digitalnimi elementi, navedene v prilogi k tej uredbi, zaradi svoje kritičnosti pogosto že uporabljajo različne oblike certificiranja, zanje pa velja tudi evropska certifikacijska shema za kibernetsko varnost s skupnimi merili, določena v Izvedbeni uredbi Komisije (EU) 2024/482 ([20]). Zato bi bilo lahko za zagotovitev ustrezne skupne kibernetske zaščite kritičnih izdelkov z digitalnimi elementi v Uniji ustrezno in sorazmerno, da se za take kategorije izdelkov z delegiranim aktom uvede obvezno evropsko certificiranje za kibernetsko varnost, kadar je že vzpostavljena ustrezna evropska certifikacijska shema za kibernetsko varnost, ki zajema te izdelke, Komisija pa je izvedla oceno morebitnega učinka predvidenega obveznega certificiranja na trg. Pri tej oceni bi bilo treba upoštevati tako ponudbo kot povpraševanje, vključno s tem, ali obstaja zadostno povpraševanje po zadevnih izdelkih z digitalnimi elementi iz držav članic in uporabnikov, ki upravičuje evropsko certificiranje za kibernetsko varnost, ter namene, za katere naj bi se izdelki z digitalnimi elementi uporabljali, vključno s kritično odvisnostjo od njih s strani bistvenih subjektov iz člena 3(1) Direktive (EU) 2022/2555. V oceni bi bilo treba analizirati tudi morebitne učinke obveznega certificiranja na razpoložljivost teh izdelkov na notranjem trgu ter zmogljivosti in pripravljenost držav članic za izvajanje ustreznih evropskih certifikacijskih shem za kibernetsko varnost.

(47) Delegirani akti, ki zahtevajo obvezno evropsko certificiranje za kibernetsko varnost, bi morali določati izdelke z digitalnimi elementi, ki imajo osnovno funkcijo kategorije kritičnih izdelkov z digitalnimi elementi iz te uredbe, za katere velja obvezno certificiranje, in zahtevano raven zanesljivosti, ki bi morala biti vsaj „znatna“. Zahtevana raven zanesljivosti bi morala biti sorazmerna s stopnjo tveganja za kibernetsko varnost, povezanega z izdelkom z digitalnimi elementi. Kadar ima na primer izdelek z digitalnimi elementi osnovno funkcijo kategorije kritičnih

([20]) Izvedbena uredba Komisije (EU) 2024/482 z dne 31. januarja 2024 o določitvi pravil za uporabo Uredbe (EU) 2019/881 Evropskega parlamenta in Sveta v zvezi s sprejetjem evropske certifikacijske sheme za kibernetsko varnost, ki temelji na skupnih merilih (UL L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

izdelkov z digitalnimi elementi iz te uredbe in je namenjen uporabi v občutljivem ali kritičnem okolju, kot so izdelki, namenjeni uporabi bistvenih subjektov iz člena 3(1) Direktive (EU) 2022/2555, bo morda potrebna najvišja raven zanesljivosti.

(48) Za zagotovitev ustrezne skupne kibernetske zaščite v Uniji izdelkov z digitalnimi elementi, ki imajo osnovno funkcijo kategorije kritičnih izdelkov z digitalnimi elementi iz te uredbe, bi bilo treba na Komisijo prenesti tudi pooblastilo za sprejemanje delegiranih aktov za spremembo te uredbe z dodajanjem ali umikom kategorij kritičnih izdelkov z digitalnimi elementi, za katere bi se od proizvajalcev lahko zahtevalo, da pridobijo evropski certifikat kibernetske varnosti v okviru evropske certifikacijske sheme za kibernetsko varnost na podlagi Uredbe (EU) 2019/881, in tako dokažejo skladnost s to uredbo. Tem kategorijam se lahko doda nova kategorija kritičnih izdelkov z digitalnimi elementi, če so bistveni subjekti iz člena 3(1) Direktive (EU) 2022/2555 od njih kritično odvisni, ali, če bi v primeru, da bi jih prizadeli incidenti ali če bi vsebovali izkoriščane ranljivosti, to lahko povzročilo motnje v kritičnih dobavnih verigah. Komisija bi morala imeti možnost, da pri ocenjevanju potrebe po dodajanju ali umiku kategorij kritičnih izdelkov z digitalnimi elementi z delegiranim aktom upošteva, ali so države članice na nacionalni ravni opredelile izdelke z digitalnimi elementi, ki imajo ključno vlogo za odpornost bistvenih subjektov iz člena 3(1) Direktive (EU) 2022/2555 in ki se vse pogosteje soočajo s kibernetskimi napadi v dobavni verigi z morebitnimi resnimi motečimi učinki. Poleg tega bi morala imeti Komisija možnost, da upošteva rezultate usklajene ocene tveganja za varnost kritičnih dobavnih verig na ravni Unije, izvedene v skladu s členom 22 Direktive (EU) 2022/2555.

(49) Komisija bi morala pri pripravi ukrepov za izvajanje te uredbe zagotoviti strukturirano in redno posvetovanje s številnimi ustreznimi deležniki. To bi moralo veljati zlasti, kadar Komisija oceni potrebo po morebitnih posodobitvah seznamov kategorij pomembnih ali kritičnih izdelkov z digitalnimi elementi, kadar bi se bilo treba posvetovati z zadevnimi proizvajalci in upoštevati njihova stališča, da bi analizirali tveganja za kibernetsko varnost ter ravnovesje med stroški in koristmi določitve takih kategorij izdelkov kot pomembnih ali kritičnih.

(50) Ta uredba obravnava tveganja za kibernetsko varnost na ciljno usmerjen način. Izdelki z digitalnimi elementi pa lahko povzročajo tudi druga varnostna tveganja, ki niso vedno povezana s kibernetsko varnostjo, so pa lahko posledica kršitve varnosti. Ta tveganja bi se morala še naprej urejati z drugo ustrezno harmonizacijsko zakonodajo Unije, ki ni ta uredba. Če se druga harmonizacijska zakonodaja Unije, ki ni ta uredba, ne uporablja, bi se morala v zvezi z njimi uporabljati Uredba (EU) 2023/988 Evropskega parlamenta in Sveta ([21]). Zaradi ciljno usmerjene narave te uredbe bi se morala z odstopanjem od člena 2(1), tretji pododstavek, točka (b), Uredbe (EU) 2023/988, poglavje III, oddelek 1, poglavji V in VII ter poglavja IX do XI Uredbe (EU) 2023/988 uporabljati za izdelke z digitalnimi elementi v zvezi z varnostnimi tveganji, ki niso zajeta s to uredbo, če za navedene izdelke ne veljajo posebne zahteve, ki jih nalaga druga harmonizacijska zakonodaja Unije, ki ni ta uredba, v smislu člena 3, točka 27, Uredbe (EU) 2023/988.

(51) Izdelki z digitalnimi elementi, ki so razvrščeni kot visokotvegani sistemi UI na podlagi člena 6 Uredbe (EU) 2024/1689 Evropskega parlamenta in Sveta ([22]) in spadajo na področje uporabe te uredbe, bi morali izpolnjevati bistvene zahteve glede kibernetske varnosti iz te uredbe. Kadar ti visokotvegani sistemi UI izpolnjujejo bistvene zahteve glede kibernetske varnosti, določene v tej uredbi, bi bilo treba šteti, da izpolnjujejo zahteve glede kibernetske varnosti iz člena 15 Uredbe (EU) 2024/1689, kolikor so te zahteve zajete z EU izjavo o skladnosti, izdano na podlagi te uredbe, ali njenimi deli. V ta namen bi morali pri oceni tveganja za kibernetsko varnost, povezanega z izdelkom z digitalnimi elementi, ki je razvrščen kot visokotvegani sistem UI na podlagi Uredbe (EU) 2024/1689, ki ga je treba upoštevati v fazah načrtovanja, zasnove, razvoja, proizvodnje, dobave in vzdrževanja takega izdelka, kot to zahteva ta uredba, zajeti tudi tveganja za kibernetsko odpornost sistemov UI zaradi poskusov nepooblaščenih tretjih oseb, da

([21]) Uredba (EU) 2023/988 Evropskega parlamenta in Sveta z dne 10. maja 2023 o splošni varnosti proizvodov, spremembi Uredbe (EU) št. 1025/2012 Evropskega parlamenta in Sveta in Direktive (EU) 2020/1828 Evropskega parlamenta in Sveta ter razveljavitvi Direktive 2001/95/ES Evropskega parlamenta in Sveta in Direktive Sveta 87/357/EGS (UL L 135, 23.5.2023, str. 1).

([22]) Uredba (EU) 2024/1689 Evropskega parlamenta in Sveta z dne 13. junija 2024 o določitvi harmoniziranih pravil o umetni inteligenci in spremembi uredb (ES) št. 300/2008, (EU) št. 167/2013, (EU) št. 168/2013, (EU) 2018/858, (EU) 2018/1139 in (EU) 2019/2144 ter direktiv 2014/90/EU, (EU) 2016/797 in (EU) 2020/1828 (Akt o umetni inteligenci) (UL L, 2024/1689, 12.7.2024, ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

bi spremenili njegovo uporabo, vedenje ali uspešnost, vključno z ranljivostmi, specifičnimi za umetno inteligenco, kot so zastrupljanje podatkov ali nasprotovalni napadi, ter tveganja za temeljne pravice, v skladu z Uredbo (EU) 2024/1689. Kar zadeva postopke ugotavljanja skladnosti v zvezi z bistvenimi zahtevami glede kibernetske varnosti za izdelek z digitalnimi elementi, ki spada na področje te uredbe in ki je razvrščen kot visokotvegani sistem UI, bi se praviloma moral namesto zadevnih določb te uredbe uporabljati člen 43 Uredbe (EU) 2024/1689. Vendar se zaradi tega pravila ne bi smela znižati potrebna raven zanesljivosti za pomembne ali kritične izdelke z digitalnimi elementi, zajete s to uredbo. Zato bi se moral z odstopanjem od tega pravila za visokotvegane sisteme UI, ki spadajo na področje uporabe Uredbe (EU) 2024/1689 in so tudi pomembni ali kritični izdelki z digitalnimi elementi v skladu s to uredbo ter za katere se uporablja postopek ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge VI k Uredbi (EU) 2024/1689, v zvezi z bistvenimi zahtevami glede kibernetske varnosti, določenimi v tej uredbi, uporabljati postopek ugotavljanja skladnosti iz te uredbe. V takem primeru bi se morale za vse druge vidike, zajete z Uredbo (EU) 2024/1689, uporabljati zadevne določbe o ugotavljanju skladnosti na podlagi notranje kontrole, določene v Prilogi VI te uredbe.

(52) Za izboljšanje varnosti izdelkov z digitalnimi elementi, ki se dajo na notranji trg, je treba določiti bistvene zahteve glede kibernetske varnosti, ki veljajo za take izdelke. Te bistvene zahteve glede kibernetske varnosti ne bi smele vplivati na usklajene ocene varnostnega tveganja v Uniji za kritične dobavne verige iz člena 22 Direktive (EU) 2022/2555, pri katerih se upoštevajo tehnični in, kadar je ustrezno, netehnični dejavniki tveganja, kot je neupravičen vpliv tretje države na dobavitelje. Poleg tega ne bi smele vplivati na pravico držav članic, da določijo dodatne zahteve za zagotovitev visoke ravni odpornosti, pri katerih se upoštevajo netehnični dejavniki, vključno z dejavniki, opredeljenimi v Priporočilu Komisije (EU) 2019/534 ([23]), iz usklajene ocene tveganj za kibernetsko varnost omrežij 5G na ravni EU in zbirke orodij za kibernetsko varnost 5G, o kateri se je dogovorila skupina za sodelovanje, ustanovljena na podlagi člena 14 Direktive (EU) 2022/2555.

(53) Proizvajalci izdelkov, ki spadajo na področje uporabe uredbe (EU) 2023/1230 Evropskega parlamenta in Sveta ([24]), ki so tudi izdelki z digitalnimi elementi, kakor so opredeljeni v tej uredbi, bi morali izpolnjevati bistvene zahteve glede kibernetske varnosti iz te uredbe in bistvene zdravstvene in varnostne zahteve iz Uredbe (EU) 2023/1230. Bistvene zahteve glede kibernetske varnosti iz te uredbe in nekatere bistvene zahteve, določene v Uredbi (EU) 2023/1230, bi lahko obravnavale podobna tveganja za kibernetsko varnost. Zato bi skladnost z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe lahko olajšala skladnost z bistvenimi zahtevami, ki zajemajo tudi nekatera tveganja za kibernetsko varnost iz Uredbe (EU) 2023/1230, zlasti tistimi v zvezi z zaščito pred korupcijo ter varnostjo in zanesljivostjo krmilnih sistemov iz oddelkov 1.1.9 in 1.2.1 Priloge III k navedeni uredbi. Take sinergije mora dokazati proizvajalec, na primer z uporabo harmoniziranih standardov ali drugih tehničnih specifikacij, kadar so na voljo, ki zajemajo ustrezne bistvene zahteve glede kibernetske varnosti, na podlagi ocene tveganja, ki zajema ta tveganja za kibernetsko varnost. Proizvajalec bi moral upoštevati tudi veljavne postopke ugotavljanja skladnosti iz te uredbe in Uredbe (EU) 2023/1230. Komisija in evropske organizacije za standardizacijo bi morale pri pripravljalnem delu, ki podpira izvajanje te uredbe in Uredbe (EU) 2023/1230 ter povezanih postopkov standardizacije, spodbujati doslednost pri tem, kako se ocenjujejo tveganja za kibernetsko varnost in kako naj bodo ta tveganja zajeta v harmoniziranih standardih v zvezi z ustreznimi bistvenimi zahtevami. Komisija in evropske organizacije za standardizacijo bi morale to uredbo upoštevati zlasti pri pripravi in razvoju harmoniziranih standardov za lažje izvajanje Uredbe (EU) 2023/1230, zlasti v zvezi z vidiki kibernetske varnosti, povezanimi z zaščito pred korupcijo, ter varnostjo in zanesljivostjo krmilnih sistemov iz oddelkov 1.1.9 in 1.2.1 Priloge III k navedeni uredbi. Komisija bi morala zagotoviti usmeritve za podporo proizvajalcem, za katere velja ta uredba in za katere velja tudi Uredba (EU) 2023/1230, zlasti za lažje dokazovanje skladnosti z ustreznimi bistvenimi zahtevami iz te uredbe in Uredbe (EU) 2023/1230.

(54) Za zagotovitev, da so izdelki z digitalnimi elementi varni, ko se dajo na trg in v času predvidene uporabe izdelka z digitalnimi elementi je treba določiti bistvene zahteve glede kibernetske varnosti za obravnavanje ranljivosti in bistvene zahteve glede kibernetske varnosti, ki se nanašajo na lastnosti izdelkov z digitalnimi elementi. Proizvajalci bi morali izpolnjevati vse bistvene zahteve glede kibernetske varnosti v zvezi z obravnavanjem ranljivosti v celotnem

([23]) Priporočilo Komisije (EU) 2019/534 z dne 26. marca 2019 – Kibernetska varnost omrežij 5G (UL L 88, 29.3.2019, str. 42).
([24]) Uredba (EU) 2023/1230 Evropskega parlamenta in Sveta z dne 14. junija 2023 o strojih in razveljavitvi Direktive 2006/42/ES Evropskega parlamenta in Sveta ter Direktive Sveta 73/361/EGS (UL L 165, 29.6.2023, str. 1).

predvidenem obdobju podpore, poleg tega pa bi morali ugotoviti, katere druge bistvene zahteve glede kibernetske varnosti v zvezi z lastnostmi izdelkov so pomembne za zadevno vrsto izdelka z ustreznimi digitalnimi elementi. V ta namen bi morali oceniti tveganja za kibernetsko varnost, povezana z izdelkom z digitalnimi elementi, da ugotovijo zadevna tveganja in zadevne bistvene zahteve glede kibernetske varnosti, da svoje izdelke z digitalnimi elementi dajo na voljo brez znanih ranljivosti, ki jih je mogoče izkoristiti, in ki bi lahko vplivale na varnost teh izdelkov, ter ustrezno uporabijo primerne harmonizirane standarde, skupne specifikacije ali evropske ali mednarodne standarde.

(55) Kadar se določene bistvene zahteve glede kibernetske varnosti ne uporabljajo za izdelek z digitalnimi elementi, bi moral proizvajalec v oceno tveganja za kibernetsko varnost, ki je del tehnične dokumentacije, vključiti jasno utemeljitev. To bi se lahko zgodilo, kadar bistvena zahteva glede kibernetske varnosti ni združljiva z naravo izdelka z digitalnimi elementi. Za predvideni namen izdelka z digitalnimi elementi se lahko na primer zahteva, da proizvajalec upošteva splošno priznane standarde interoperabilnosti, tudi če se njegove varnostne značilnosti ne štejejo več za najsodobnejše. Podobno tudi drugo pravo Unije od proizvajalcev zahteva, da uporabljajo posebne zahteve glede interoperabilnosti. Kadar se bistvena zahteva glede kibernetske varnosti ne uporablja za izdelek z digitalnimi elementi, vendar je proizvajalec opredelil tveganja za kibernetsko varnost v zvezi s to bistveno zahtevo glede kibernetske varnosti, bi moral sprejeti ukrepe za obravnavanje teh tveganj na druge načine, na primer z omejitvijo predvidenega namena izdelka na zaupanja vredna okolja ali z obveščanjem uporabnikov o teh tveganjih.

(56) Eden najpomembnejših ukrepov, ki jih morajo uporabniki sprejeti za zaščito svojih izdelkov z digitalnimi elementi pred kibernetskimi napadi, je čimprejšnja namestitev najnovejših razpoložljivih varnostnih posodobitev. Proizvajalci bi zato morali oblikovati svoje izdelke in vzpostaviti postopke za zagotovitev, da izdelki z digitalnimi elementi vključujejo funkcije, ki omogočajo samodejno obveščanje, distribucijo, prenos in namestitev varnostnih posodobitev, zlasti v primeru potrošniških izdelkov. Poleg tega bi morali omogočiti, da se kot zadnji korak odobri prenos in namestitev varnostnih posodobitev. Uporabniki bi morali ohraniti možnost deaktiviranja samodejnih posodobitev z jasnim in enostavnim mehanizmom za uporabo, podprtim z jasnimi navodili o tem, kako lahko uporabniki to funkcijo izključijo. Zahteve v zvezi s samodejnimi posodobitvami, kot je določeno v prilogi k tej uredbi, se ne uporabljajo za izdelke z digitalnimi elementi, ki so namenjeni predvsem vgradnji v druge izdelke kot sestavni deli. Prav tako se ne uporabljajo za izdelke z digitalnimi elementi, za katere uporabniki ne bi razumno pričakovali samodejnih posodobitev, vključno z izdelki z digitalnimi elementi, ki naj bi se uporabljali v profesionalnih omrežjih IKT, ter zlasti v kritičnih in industrijskih okoljih, kjer bi lahko samodejna posodobitev povzročila motnje v delovanju. Ne glede na to, ali je izdelek z digitalnimi elementi zasnovan tako, da prejema samodejne posodobitve ali ne, bi moral njegov proizvajalec uporabnike obvestiti o ranljivostih in nemudoma dati na voljo varnostne posodobitve. Kadar ima izdelek z digitalnimi elementi uporabniški vmesnik ali podobna tehnična sredstva, ki omogočajo neposredno interakcijo z njegovimi uporabniki, bi moral proizvajalec te funkcije uporabiti za obveščanje uporabnikov, da je njegov izdelek z digitalnimi elementi dosegel konec obdobja podpore. Obvestila bi morala biti omejena na to, kar je potrebno za zagotovitev učinkovitega prejema teh informacij in ne bi smela negativno vplivati na uporabniško izkušnjo izdelka z digitalnimi elementi.

(57) Da bi izboljšali preglednost postopkov obravnavanja ranljivosti in zagotovili, da uporabnikom ni treba namestiti novih posodobitev funkcij izključno za prejemanje najnovejših varnostnih posodobitev, bi morali proizvajalci, kadar je to tehnično izvedljivo, poskrbeti, da se nove varnostne posodobitve zagotavljajo ločeno od posodobitev funkcij.

(58) V skupnem sporočilu Komisije in visokega predstavnika Unije za zunanje zadeve in varnostno politiko z dne 20. junija 2023 z naslovom „Evropska gospodarska varnostna strategija“ je navedeno, da mora Unija s skupnim strateškim okvirom za gospodarsko varnost Unije čim bolj povečati koristi svoje gospodarske odprtosti, hkrati pa čim bolj zmanjšati tveganja zaradi gospodarske odvisnosti od ponudnikov z visokim tveganjem. Odvisnosti od zelo tveganih dobaviteljev izdelkov z digitalnimi elementi lahko predstavljajo strateško tveganje, ki ga je treba obravnavati na ravni Unije, zlasti kadar so izdelki z digitalnimi elementi namenjeni za uporabo s strani bistvenih subjektov iz člena 3(1) Direktive (EU) 2022/2555. Taka tveganja so lahko med drugim povezana z jurisdikcijo, pod katero spada proizvajalec, značilnostmi lastništva njegovega podjetja in povezavami z nadzorom vlade tretje države, v kateri ima sedež, zlasti kadar tretja država izvaja gospodarsko vohunjenje ali če njeno neodgovorno ravnanje v kibernetskem prostoru in njena zakonodaja omogočata samovoljen dostop do vseh vrst dejavnosti podjetja ali podatkov, vključno s poslovno občutljivimi podatki, ter lahko naloži obveznosti za obveščevalne namene brez uporabe demokratičnega sistema zavor in ravnovesij, nadzornih mehanizmov, dolžnega postopanja ali pravice do pritožbe pri neodvisnem sodišču. Komisija in organi za nadzor trga bi morali pri določanju pomembnosti tveganja za kibernetsko varnost v smislu te uredbe v skladu s svojimi odgovornostmi iz te uredbe upoštevati tudi netehnične dejavnike tveganja,

zlasti tiste, ki so bili ugotovljeni na podlagi usklajenih ocen tveganja za varnost kritičnih dobavnih verig na ravni Unije, izvedenih v skladu s členom 22 Direktive (EU) 2022/2555.

(59) Za zagotovitev varnosti izdelkov z digitalnimi elementi po tem, ko so bili dani na trg, bi morali proizvajalci določiti obdobja podpore, ki bi morala odražati predvideni čas uporabe izdelka z digitalnimi elementi. Proizvajalec bi moral pri določanju obdobja podpore upoštevati zlasti razumna pričakovanja uporabnikov, naravo izdelka in ustrezno pravo Unije, ki določa življenjsko dobo izdelkov z digitalnimi elementi. Proizvajalci bi morali imeti tudi možnost, da upoštevajo druge ustrezne dejavnike. Merila bi bilo treba uporabljati tako, da bi se zagotovila sorazmernost pri določanju obdobja podpore. Proizvajalec bi moral organom za nadzor trga na zahtevo zagotoviti informacije, ki jih je upošteval pri določitvi obdobja podpore za izdelek z digitalnimi elementi.

(60) Obdobje podpore, v katerem proizvajalec zagotovi učinkovito obravnavanje ranljivosti, ne bi smelo biti krajše od petih let, razen če je življenjska doba izdelka z digitalnimi elementi krajša od petih let, v tem primeru bi moral proizvajalec zagotoviti obravnavanje ranljivosti za to življenjsko dobo. Kadar se upravičeno pričakuje, da se bo izdelek z digitalnimi elementi uporabljal dlje kot pet let, kot pogosto velja za sestavne dele strojne opreme, kot so matične plošče ali mikroprocesorji, omrežne naprave, kot so usmerjevalniki, modemi ali stikala, ter programsko opremo, kot so operacijski sistemi ali orodja za urejanje video posnetkov, bi morali proizvajalci temu ustrezno zagotoviti daljša obdobja podpore. Zlasti izdelki z digitalnimi elementi, namenjeni za uporabo v industrijskem okolju, kot so industrijski nadzorni sistemi, se pogosto uporabljajo bistveno dlje. Proizvajalec bi moral imeti možnost, da določi obdobje podpore, krajše od petih let, samo kadar to upravičuje narava izdelka z zadevnimi digitalnimi elementi in kadar se pričakuje, da se bo ta izdelek uporabljal manj kot pet let; v tem primeru bi moralo obdobje podpore trajati toliko, kot pričakovani čas uporabe. Na primer, življenjska doba aplikacije za sledenje stikom, namenjene uporabi med pandemijo, bi lahko bila omejena na trajanje pandemije. Poleg tega se lahko nekatere programske aplikacije po naravi dajo na voljo le na podlagi naročnine, zlasti kadar aplikacija po izteku naročnine uporabniku ni več na voljo in se zato ne uporablja več.

(61) Ko se obdobje podpore za izdelek z digitalnimi elementi zaključi, bi moral proizvajalec za zagotovitev, da se ranljivosti lahko obravnavajo tudi po koncu obdobja podpore, razmisliti o tem, da bi izvorno kodo takih izdelkov z digitalnimi elementi dal na voljo drugim podjetjem, ki se zavežejo, da bodo storitve obravnavanja ranljivosti zagotavljala za daljše obdobje, ali javnosti. Kadar proizvajalci izvorno kodo dajo na voljo drugim podjetjem, bi morali imeti možnost, da zaščitijo lastništvo izdelka z digitalnimi elementi in preprečijo razširjanje izvorne kode v javnosti, na primer s pogodbo.

(62) Za zagotovitev, da bi proizvajalci po vsej Uniji določili podobna obdobja podpore za primerljive izdelke z digitalnimi elementi, bi morala skupina ADCO objaviti statistične podatke o povprečnih obdobjih podpore, ki jih določijo proizvajalci za kategorije izdelkov z digitalnimi elementi, in pripraviti usmeritve, v katerih bi navedla ustrezna obdobja podpore za take kategorije. Za zagotovitev harmoniziranega pristopa na notranjem trgu bi morala imeti Komisija tudi možnost, da sprejme delegirane akte za določitev minimalnih obdobij podpore za določene kategorije izdelkov, kadar podatki, ki jih zagotovijo organi za nadzor trga, kažejo, da obdobja podpore, ki jih določijo proizvajalci, bodisi sistematično niso v skladu z merili za določanje obdobij podpore iz te uredbe bodisi da proizvajalci v različnih državah članicah neupravičeno določijo različna obdobja podpore.

(63) Proizvajalci bi morali vzpostaviti enotno kontaktno točko, ki bi uporabnikom omogočala enostavno komunikacijo z njimi, tudi za namene poročanja in prejemanja informacij o ranljivostih izdelka z digitalnim elementom. Uporabnikom bi bilo treba zagotoviti enostaven dostop do enotne kontaktne točke in jasno navesti njeno razpoložljivost ter te informacije posodabljati. Kadar se proizvajalci odločijo ponuditi avtomatizirana orodja, npr. klepetalnice, bi morali ponuditi tudi telefonsko številko ali druga digitalna sredstva komunikacije, kot je elektronski naslov ali kontaktni obrazec. Enotna kontaktna točka ne bi smela delovati izključno z avtomatiziranimi orodji.

(64) Proizvajalci bi morali zagotoviti, da so njihovi izdelki z digitalnimi elementi dostopni na trgu s privzeto varno konfiguracijo, ter uporabnikom zagotoviti brezplačne varnostne posodobitve. Proizvajalci bi morali imeti možnost odstopanja od teh bistvenih zahtev glede kibernetske varnosti le v zvezi s po meri narejenimi izdelki, ki so za določen namen prilagojeni potrebam določenega poslovnega uporabnika, in kadar sta se proizvajalec in uporabnik o tem izrecno dogovorila s posebnimi pogodbenimi pogoji.

(65) Proizvajalci bi morali prek enotne platforme za poročanje hkrati obvestiti skupino za odzivanje na incidente na področju računalniške varnosti (CSIRT), ki je imenovana za koordinatorja, in agencijo ENISA o aktivno izrabljenih ranljivostih izdelkov z digitalnimi elementi ter o resnih incidentih, ki vplivajo na varnost teh izdelkov. Obvestilo bi bilo treba predložiti prek končne točke za elektronsko obveščanje skupine CSIRT, ki je imenovana za koordinatorja, in bi moralo biti hkrati dostopno agenciji ENISA.

(66) Proizvajalci bi morali sporočati aktivno izrabljene ranljivosti, da bi zagotovili, da imajo skupine CSIRT, ki so imenovane za koordinatorje, in agencija ENISA ustrezen pregled nad takimi ranljivostmi in da prejmeta informacije, potrebne za opravljanje njunih nalog iz Direktive (EU) 2022/2555, in povišanje splošne ravni kibernetske varnosti bistvenih in pomembnih subjektov iz člena 3 navedene direktive, ter za zagotovitev učinkovitega delovanja organov za nadzor trga. Ker se večina izdelkov z digitalnimi elementi prodaja na celotnem notranjem trgu, bi bilo treba vse izrabljene ranljivosti izdelka z digitalnimi elementi šteti za grožnjo delovanju notranjega trga. Agencija ENISA bi morala v dogovoru s proizvajalcem razkriti odpravljene ranljivosti v evropski podatkovni zbirki ranljivosti, vzpostavljeni na podlagi člena 12(2) Direktive (EU) 2022/2555. Evropska podatkovna zbirka ranljivosti bo proizvajalcem pomagala pri odkrivanju znanih ranljivosti, ki jih je mogoče izrabiti, odkritih v njihovih izdelkih, da se zagotovi, da se dajo na trg varni izdelki.

(67) Proizvajalci bi morali skupini CSIRT, ki je imenovana za koordinatorja in agenciji ENISA sporočiti tudi vsak resen incident, ki vpliva na varnost izdelka z digitalnimi elementi. Da bi se lahko uporabniki hitro odzvali na resne incidente, ki vplivajo na varnost njihovih izdelkov z digitalnimi elementi, bi morali proizvajalci tudi obvestiti njihove uporabnike o vseh takih incidentih in, kadar je ustrezno, o morebitnih popravnih ukrepih, ki jih lahko uporabniki sprejmejo za zmanjšanje vpliva incidenta, na primer z objavo ustreznih informacij na svojih spletnih mestih ali prek neposrednega stika z uporabniki, kadar ga lahko proizvajalec vzpostavi in tveganja za kibernetsko varnost to upravičujejo.

(68) Aktivno izrabljene ranljivosti se nanašajo na primere, kadar proizvajalec ugotovi, da je kršitev varnosti, ki vpliva na njegove uporabnike ali katero koli drugo fizično ali pravno osebo, posledica zlonamernega akterja, ki je uporabil napako v enem od izdelkov z digitalnimi elementi, ki jih je proizvajalec dal na voljo na trgu. Primeri takih ranljivosti so lahko slabosti v funkcijah za identifikacijo in avtentikacijo v izdelku. Sporočanje ranljivosti, ki se odkrijejo brez zlonamernosti za namene testiranja, preiskovanja, popravljanja ali razkritja v dobri veri, da bi izboljšali zaščito ali varnost lastnika sistema in njegovih uporabnikov, ne bi smelo biti obvezno. Po drugi strani pa se resni incidenti, ki vplivajo na varnost izdelka z digitalnimi elementi, nanašajo na primere, kadar kibernetski incident vpliva na proizvajalčeve postopke razvoja, proizvodnje ali vzdrževanja tako, da bi lahko povzročil povečano tveganje kibernetske varnosti za uporabnike ali druge osebe. Tak resen incident lahko vključuje situacijo, kadar napadalec uspešno vnese zlonamerno kodo v kanal, prek katerega proizvajalec uporabnikom posreduje varnostne posodobitve.

(69) Da se obvestila lahko hitro posredujejo vsem ustreznim skupinam CSIRT, ki so imenovane za koordinatorje, in da se proizvajalcem omogoči, da v vsaki fazi postopka obveščanja vložijo eno samo obvestilo, bi morala agencija ENISA vzpostaviti enotno platformo za poročanje z nacionalnimi končnimi točkami za elektronsko obveščanje. Vsakodnevno delovanje enotne platforme za poročanje bi morala upravljati in vzdrževati agencija ENISA. Skupine CSIRT, ki so imenovane za koordinatorje, bi morale svoje organe za nadzor trga obvestiti o sporočenih ranljivostih ali incidentih. Enotna platforma za poročanje bi morala biti zasnovana tako, da bo zagotavljala zaupnost obvestil, zlasti v zvezi z ranljivostmi, za katere varnostna posodobitev še ni na voljo. Poleg tega bi morala agencija ENISA vzpostaviti postopke za varno in zaupno ravnanje z informacijami. Agencija ENISA bi morala na podlagi informacij, ki jih zbere, pripraviti dvoletno tehnično poročilo o novih trendih glede tveganj za kibernetsko varnost pri izdelkih z digitalnimi elementi in ga predložiti skupini za sodelovanje, vzpostavljeni na podlagi člena 14 Direktive (EU) 2022/2555.

(70) V izjemnih okoliščinah in zlasti na zahtevo proizvajalca bi morala imeti skupina CSIRT, ki je imenovana za koordinatorja, ki je prvotno prejela obvestilo, možnost, da odloži posredovanje obvestila drugim relevantnim skupinam CSIRT, ki so imenovane za koordinatorje, prek enotne platforme za poročanje, kadar je to mogoče utemeljiti z razlogi, povezanimi s kibernetsko varnostjo, in za obdobje, ki je nujno potrebno. Skupina CSIRT, ki je imenovana za koordinatorja, bi morala agencijo ENISA nemudoma obvestiti o odložitvi in razlogih zanjo ter o tem, kdaj namerava posredovati obvestilo. Komisija bi morala z delegiranim aktom podrobneje opredeliti pogoje za uporabo razlogov, povezanih s kibernetsko varnostjo, ter pri pripravi osnutka delegiranega akta sodelovati z mrežo skupin CSIRT, vzpostavljeno na podlagi člena 15 Direktive (EU) 2022/2555, in agencijo ENISA. Primeri razlogov, povezanih s kibernetsko varnostjo, vključujejo postopek usklajenega razkrivanja ranljivosti, ki je v teku, ali situacije, v katerih se pričakuje, da bo proizvajalec kmalu zagotovil blažitveni ukrep, tveganja za kibernetsko varnost, ki bi jih prineslo takojšnje posredovanje obvestila prek enotne platforme za poročanje, pa odtehtajo koristi takojšnjega posredovanja. Agencija ENISA bi morala imeti možnost, da na zahtevo skupine CSIRT, ki je imenovana za

koordinatorja, to skupino podpre pri uporabi razlogov, povezanih s kibernetsko varnostjo, v zvezi z odložitvijo posredovanja obvestila na podlagi informacij, ki jih je agencija ENISA prejela od te skupine CSIRT v zvezi z odločitvijo o odložitvi posredovanja obvestila iz teh razlogov, povezanih s kibernetsko varnostjo. Poleg tega agencija ENISA v izjemnih okoliščinah ne bi smela sočasno prejeti vseh podrobnosti obvestila o aktivno izrabljeni ranljivosti. To bi veljalo v primeru, če bi proizvajalec v svojem obvestilu navedel, da je zlonamerni akter aktivno izrabil sporočeno ranljivost in da je bila glede na razpoložljive informacije izrabljena samo v državi članici skupine CSIRT, ki je imenovana za koordinatorja, ki ji je proizvajalec sporočil ranljivost, in kadar bi se s takojšnjim posredovanjem obvestila o ranljivosti verjetno posredovale informacije, katerih razkritje bi bilo v nasprotju z bistvenimi interesi zadevne države članice, ali kadar bi posredovanje obvestila pomenilo neposredno visoko tveganje za kibernetsko varnost. V takih primerih bo agencija ENISA imela samo hkraten dostop do informacije, da je proizvajalec predložil obvestilo, splošnih informacij o izdelku z digitalnimi elementi, na katerega se obvestilo nanaša, informacij o splošni naravi izrabljene ranljivosti in informacije, da se proizvajalec sklicuje na varnostne razloge in da zato celotna vsebina obvestila ni na voljo. Celotno obvestilo bi moralo biti nato na voljo agenciji ENISA in drugim ustreznim skupinam CSIRT, ki so imenovane za koordinatorje, kadar skupina CSIRT, ki je imenovana za koordinatorja, ki je prvotno prejela obvestilo, ugotovi, da ti varnostni razlogi, ki so nastali zaradi izjemnih okoliščin, kot so določene v tej uredbi, prenehajo obstajati. Kadar agencija ENISA na podlagi razpoložljivih informacij meni, da obstaja sistemsko tveganje, ki vpliva na varnost notranjega trga, bi morala skupini CSIRT, ki je obvestilo prejela, priporočiti, naj celotno obvestilo posreduje drugim skupinam CSIRT, ki so imenovane za koordinatorje, in agenciji ENISA.

(71) Kadar proizvajalci sporočijo aktivno izrabljeno ranljivost ali resen incident, ki vpliva na varnost izdelka z digitalnimi elementi, bi morali navesti, kako občutljive so po njihovem mnenju sporočene informacije. Skupina CSIRT, ki je imenovana za koordinatorja, ki je prvotno prejela obvestilo, bi morala to informacijo upoštevati pri oceni, ali je zaradi obvestila prišlo do izjemnih okoliščin, zaradi katerih je kasnejše posredovanje obvestila drugim zadevnim skupinam CSIRT, ki so imenovane za koordinatorje, upravičeno zaradi utemeljenih razlogov, povezanih s kibernetsko varnostjo. To informacijo bi morala upoštevati tudi pri oceni, ali je zaradi obvestila o aktivno izrabljeni ranljivosti prišlo do izjemnih okoliščin, ki upravičujejo, zakaj celotno obvestilo ni hkrati na voljo agenciji ENISA. Skupine CSIRT, ki so imenovane za koordinatorje, bi morale imeti možnost, da to informacijo upoštevajo pri določanju ustreznih ukrepov za zmanjšanje tveganj, ki izhajajo iz takih ranljivosti in incidentov.

(72) Da bi poenostavili sporočanje informacij, ki se zahtevajo na podlagi te uredbe, ob upoštevanju drugih dodatnih zahtev glede poročanja iz prava Unije, kot so Uredba (EU) 2016/679, Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta ([25]), Direktiva 2002/58/ES Evropskega parlamenta in Sveta ([26]) in Direktiva (EU) 2022/2555, ter zmanjšali upravno breme za subjekte, se države članice spodbuja, naj razmislijo o tem, da bi na nacionalni ravni zagotovile enotne vstopne točke za take zahteve glede poročanja. Uporaba take enotne vstopne točke za poročanje o varnostnih incidentih na podlagi Uredbe (EU) 2016/679 in Direktive 2002/58/ES ne bi smela vplivati na uporabo določb Uredbe (EU) 2016/679 in Direktive 2002/58/ES, zlasti tistih, ki se nanašajo na neodvisnost organov iz navedenih aktov. Agencija ENISA bi morala pri vzpostavitvi enotne platforme za poročanje iz te uredbe upoštevati možnost, da se nacionalne končne točke za elektronsko obveščanje iz te uredbe vključijo v nacionalne enotne vstopne točke, kamor se lahko vnašajo tudi druga obvestila, zahtevana na podlagi prava Unije.

(73) Agencija ENISA bi se morala pri vzpostavitvi enotne platforme za poročanje iz te uredbe in da bi izkoristila pretekle izkušnje, posvetovati z drugimi institucijami ali agencijami Unije, ki upravljajo platforme ali zbirke podatkov, za katere veljajo stroge varnostne zahteve, kot je Agencija Evropske unije za operativno upravljanje obsežnih informacijskih sistemov s področja svobode, varnosti in pravice (eu-LISA). Agencija ENISA bi morala analizirati tudi morebitno dopolnjevanje z evropsko podatkovno zbirko ranljivosti, vzpostavljeno na podlagi člena 12(2) Direktive (EU) 2022/2555.

(74) Proizvajalci ter druge fizične in pravne osebe bi morali imeti možnost, da skupini CSIRT, ki je imenovana za koordinatorja, ali agenciji ENISA prostovoljno sporočijo vsako ranljivost izdelka z digitalnimi elementi, kibernetske

([25]) Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011 (UL L 333, 27.12.2022, str. 1).

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

grožnje, ki bi lahko vplivale na profil tveganja izdelka z digitalnimi elementi, vsak incident, ki vpliva na varnost izdelka z digitalnimi elementi, pa tudi skorajšnje incidente, ki bi lahko povzročili tak incident.

(75) Države članice bi si morale prizadevati, da v skladu z nacionalnim pravom čim bolje obravnavajo izzive, s katerimi se soočajo raziskovalci ranljivosti, vključno z njihovo morebitno izpostavljenostjo kazenski odgovornosti. Glede na to, da bi bile lahko fizične in pravne osebe, ki raziskujejo ranljivosti, v nekaterih državah članicah izpostavljene kazenski in civilnopravni odgovornosti, se države članice spodbuja, naj sprejmejo smernice v zvezi s tem, da se raziskovalcev informacijske varnosti kazensko ne preganja in da so njihove dejavnosti izvzete iz civilnopravne odgovornosti.

(76) Proizvajalci izdelkov z digitalnimi elementi bi morali vzpostaviti politike usklajenega razkrivanja ranljivosti, da bi posameznikom ali subjektom neposredno ali posredno, na zahtevo pa anonimno, olajšali poročanje o ranljivostih prek skupin CSIRT, ki so imenovane za koordinatorje za namene usklajenega razkrivanja ranljivosti v skladu s členom 12(1) Direktive (EU) 2022/2555. Proizvajalčeva politika usklajenega razkrivanja ranljivosti bi morala določati strukturiran postopek, s katerim se ranljivosti sporočijo proizvajalcu tako, da lahko proizvajalec diagnosticira in odpravi take ranljivosti, preden se podrobne informacije o ranljivostih razkrijejo tretjim osebam ali javnosti. Poleg tega bi morali proizvajalci razmisliti tudi o objavi svojih varnostnih politik v strojno berljivi obliki. Ker se lahko informacije o ranljivostih, ki jih je mogoče izrabljati, v splošno razširjenih izdelkih z digitalnimi elementi prodajo na črnem trgu za visoke zneske, bi morali imeti proizvajalci takih izdelkov v okviru svojih politik usklajenega razkrivanja ranljivosti možnost, da uporabijo programe za spodbujanje poročanja o ranljivostih, pri katerih posamezniki ali subjekti prejmejo priznanje in nadomestilo za svoja prizadevanja. To velja za tako imenovane „programe za prijavljanje hroščev“.

(77) Za lajšanje analize ranljivosti bi morali proizvajalci opredeliti in dokumentirati sestavne dele izdelkov z digitalnimi elementi, med drugim s pripravo kosovnice za programsko opremo. S kosovnico za programsko opremo lahko tisti, ki izdelujejo, kupijo in upravljajo programsko opremo, pridobijo informacije za izboljšanje njihovega razumevanja dobavne verige, kar ima številne koristi, zlasti pa proizvajalcem in uporabnikom pomaga spremljati znane nove ranljivosti in tveganja kibernetske varnosti. Za proizvajalce je pomembno zlasti, da zagotovijo, da njihovi izdelki z digitalnimi elementi ne vsebujejo ranljivih sestavnih delov, ki jih razvijajo tretje osebe. Objava kosovnice za programsko opremo za proizvajalce ne bi smela biti obvezna.

(78) V kompleksnih novih poslovnih modelih, povezanih s spletno prodajo, lahko podjetje, ki deluje prek spleta, ponuja različne storitve. Odvisno od narave storitev, zagotovljenih v zvezi z določenim izdelkom z digitalnimi elementi, lahko isti subjekt spada v različne kategorije poslovnih modelov ali gospodarskih subjektov. Kadar subjekt zagotavlja samo spletne posredniške storitve za določeni izdelek z digitalnimi elementi in je samo ponudnik spletne tržnice, kakor je opredeljen v členu 3, točka 14, Uredbe (EU) 2023/988, ne izpolnjuje pogojev za opredelitev kot ena od vrst gospodarskih subjektov, opredeljenih v tej uredbi. Kadar je isti subjekt ponudnik spletne tržnice in deluje tudi kot gospodarski subjekt, kakor je opredeljen v tej uredbi, za prodajo posameznih izdelkov z digitalnimi elementi, bi morale zanj veljati obveznosti za to vrsto gospodarskih subjektov iz te uredbe. Če na primer ponudnik spletne tržnice izdelek z digitalnimi elementi tudi distribuira, potem bi se v zvezi s prodajo tega izdelka štel za distributerja. Podobno bi se ta subjekt, če bi prodajal svoje izdelke z digitalnimi elementi z lastno znamko, štel za proizvajalca in bi zato moral izpolnjevati veljavne zahteve za proizvajalce. Poleg tega se lahko nekateri subjekti štejejo za ponudnike storitev odpremnih skladišč, kakor so opredeljeni v členu 3, točka 11, Uredbe (EU) 2019/1020 Evropskega parlamenta in Sveta ([27]), če ponujajo take storitve. Take primere bi bilo treba ocenjevati posamično. Ker imajo spletne tržnice pomembno vlogo pri omogočanju elektronskega poslovanja, bi si morale prizadevati za sodelovanje z organi za nadzor trga držav članic, da bi zagotovile, da izdelki z digitalnimi elementi, kupljeni prek spletnih tržnic, izpolnjujejo zahteve glede kibernetske varnosti iz te uredbe.

(79) Za lajšanje ugotavljanja skladnosti z zahtevami iz te uredbe bi bilo treba oblikovati domnevo o skladnosti za izdelke z digitalnimi elementi, ki so skladni s harmoniziranimi standardi, s katerimi se bistvene zahteve glede kibernetske varnosti, določene v tej uredbi, prenesejo na podrobne tehnične specifikacije in ki se sprejmejo v skladu z Uredbo

([27]) Uredba (EU) 2019/1020 Evropskega parlamenta in Sveta z dne 20. junija 2019 o nadzoru trga in skladnosti proizvodov ter spremembi Direktive 2004/42/ES in uredb (ES) št. 765/2008 in (EU) št. 305/2011 (UL L 169, 25.6.2019, str. 1).

(EU) št. 1025/2012 Evropskega parlamenta in Sveta ([28]). Navedena uredba določa postopek za nasprotovanje harmoniziranim standardom, kadar ti standardi ne izpolnjujejo v celoti zahtev, določenih v tej uredbi. Postopek standardizacije bi moral zagotoviti uravnoteženo zastopanost interesov ter učinkovito sodelovanje deležnikov civilne družbe, vključno s potrošniškimi organizacijami. Upoštevati bi bilo treba tudi mednarodne standarde, ki so v skladu z ravnjo kibernetske varnosti, za katero si prizadevajo bistvene zahteve glede kibernetske varnosti iz te uredbe, da bi olajšali razvoj harmoniziranih standardov in izvajanje te uredbe ter podjetjem, zlasti mikropodjetjem, malim in srednjim podjetjem ter podjetjem, ki delujejo na svetovni ravni, olajšali skladnost.

(80) Za učinkovito izvajanje uredbe bosta zlasti pomembna pravočasen razvoj harmoniziranih standardov v prehodnem obdobju za uporabo te uredbe in njihova razpoložljivost pred datumom začetka njene uporabe. Zlasti to velja za pomembne izdelke z digitalnimi elementi, ki spadajo v razred I. Razpoložljivost harmoniziranih standardov bo proizvajalcem takih izdelkov omogočila, da izvajajo ugotavljanje skladnosti prek postopka notranje kontrole, s tem pa preprečijo ozka grla in zamude pri dejavnostih organov za ugotavljanje skladnosti.

(81) Z Uredbo (EU) 2019/881 je vzpostavljen prostovoljen evropski certifikacijski okvir za kibernetsko varnost za izdelke, postopke in storitve IKT. Evropske certifikacijske sheme za kibernetsko varnost zagotavljajo skupni okvir zaupanja za uporabnike pri uporabi izdelkov z digitalnimi elementi, ki spadajo na področje uporabe te uredbe. Ta uredba bi morala zato ustvariti sinergije z Uredbo (EU) 2019/881. Za lajšanje ugotavljanja skladnosti z zahtevami iz te uredbe se za izdelke z digitalnimi elementi, ki so certificirani ali za katere je bila izdana izjava o skladnosti v okviru evropske sheme za kibernetsko varnost na podlagi Uredbe (EU) 2019/881, ki jo je Komisija opredelila v izvedbenem aktu, domneva, da izpolnjujejo bistvene zahteve glede kibernetske varnosti iz te uredbe, kolikor evropski certifikat kibernetske varnosti ali izjava o skladnosti ali njuni deli zajemajo navedene zahteve. Potrebo po novih evropskih certifikacijskih shemah za kibernetsko varnost za izdelke z digitalnimi elementi bi bilo treba oceniti ob upoštevanju te uredbe, tudi pri pripravi tekočega delovnega programa Unije v skladu z Uredbo (EU) 2019/881. Kadar je potrebna nova shema, ki bi zajemala izdelke z digitalnimi elementi, tudi da bi olajšali skladnost s to uredbo, lahko Komisija od agencije ENISA zahteva, da pripravi predloge za sheme v skladu s členom 48 Uredbe (EU) 2019/881. Pri takih prihodnjih evropskih certifikacijskih shemah za kibernetsko varnost, ki vključujejo izdelke z digitalnimi elementi, bi se morale upoštevati bistvene zahteve glede kibernetske varnosti in postopki za ugotavljanje skladnosti iz te uredbe, te sheme pa bi morale olajšati skladnost s to uredbo. Za evropske certifikacijske sheme za kibernetsko varnost, ki začnejo veljati pred začetkom veljavnosti te uredbe, bodo morda potrebne dodatne specifikacije, s katerimi bodo podrobno določeni vidiki uporabe domneve o skladnosti. Na Komisijo bi bilo treba prenesti pooblastilo, da z delegiranimi akti določi, pod katerimi pogoji se lahko evropske certifikacijske sheme kibernetske varnosti uporabljajo za dokazovanje skladnosti z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe. Da bi se izognili nepotrebnemu upravnemu bremenu, proizvajalci prav tako ne bi smeli biti obvezani, da zagotovijo ugotavljanje skladnosti z ustreznimi zahtevami, ki ga opravi tretja oseba, kot je določeno v tej uredbi, kadar je bil evropski certifikat kibernetske varnosti izdan v okviru takih evropskih certifikacijskih shem za kibernetsko varnost na vsaj „znatni“ ravni.

(82) Po začetku veljavnosti Izvedbene uredbe (EU) 2024/482, ki se nanaša na izdelke, ki spadajo na področje uporabe te uredbe, kakor so varnostni moduli strojne opreme in mikroprocesorji, bi morala imeti Komisija možnost, da z delegiranim aktom določi, kako evropska certifikacijska shema za kibernetsko varnost s skupnimi merili zagotavlja domnevo o skladnosti z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe ali njihovimi deli. Poleg tega se lahko s takim delegiranim aktom določi, kako se s certifikatom, izdanim v okviru evropske certifikacijske sheme za kibernetsko varnost s skupnimi merili, odpravi obveznost proizvajalcev, da za ustrezne zahteve zagotovijo ugotavljanje skladnosti, ki ga opravi tretja oseba, kot se zahteva na podlagi te uredbe.

(83) Sedanji evropski okvir za standardizacijo, ki temelji na načelih novega pristopa iz Resolucije Sveta z dne 7. maja 1985 o novem pristopu k tehnični uskladitvi in standardom in na Uredbi (EU) št. 1025/2012, predstavlja vnaprej določen okvir za pripravo standardov, s katerimi se zagotavlja domneva o skladnosti z ustreznimi bistvenimi zahtevami glede kibernetske varnosti iz te uredbe. Evropski standardi bi morali biti tržno usmerjeni in upoštevati javni interes ter cilje politike, ki so jasno navedeni v zahtevi Komisije eni ali več evropskim organizacijam za standardizacijo, naj v določenem roku pripravijo harmonizirane standarde, ki temeljijo na soglasju. Vendar bi morala imeti Komisija možnost, da – kadar ni ustreznih sklicev na harmonizirane standarde in če pri tem ustrezno upošteva

([28]) 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).

vlogo in funkcije evropskih organizacij za standardizacijo,– kot izjemno nadomestno rešitev sprejme izvedbene akte za določitev skupnih specifikacij za bistvene zahteve glede kibernetske varnosti iz te uredbe, da bi olajšala obveznosti proizvajalca, da izpolnjuje te bistvene zahteve glede kibernetske varnosti, kadar je postopek standardizacije ustavljen ali kadar pride do zamud pri določanju ustreznih harmoniziranih standardov. Če je razlog za tako zamudo tehnična zapletenost zadevnega standarda, bi morala Komisija to upoštevati pred razmislekom o določitvi skupnih specifikacij.

(84) Komisija bi morala v postopek vključiti ustrezne deležnike, da bi se skupne specifikacije, ki zajemajo bistvene zahteve glede kibernetske varnosti iz te uredbe, določile na najučinkovitejši način.

(85) V zvezi z objavo sklica na harmonizirane standarde v *Uradnem listu Evropske unije* v skladu z Uredbo (EU) št. 1025/2012 bi moralo razumno obdobje pomeniti obdobje, v katerem se pričakuje objava sklica na standard, njegovega popravka ali spremembe v *Uradnem listu Evropske unije*, ki ne bi smelo biti daljše od enega leta po roku za pripravo evropskega standarda, določenega v skladu z Uredbo (EU) št. 1025/2012.

(86) Za olajšanje ugotavljanja skladnosti z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe bi bilo treba oblikovati domnevo o skladnosti za izdelke z digitalnimi elementi, ki so skladni s skupnimi specifikacijami, ki jih je Komisija sprejela na podlagi te uredbe za namen določitve podrobnih tehničnih specifikacij teh zahtev.

(87) Uporaba harmoniziranih standardov, skupnih specifikacij ali evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi Uredbe (EU) 2019/881, ki določajo domnevo o skladnosti v zvezi z bistvenimi zahtevami glede kibernetske varnosti, ki se uporabljajo za izdelke z digitalnimi elementi, bo proizvajalcem olajšala ugotavljanje skladnosti. Če se proizvajalec odloči, da takih sredstev ne bo uporabil za nekatere zahteve, mora v svoji tehnični dokumentaciji navesti, kako bo skladnost dosežena drugače. Poleg tega bi uporaba harmoniziranih standardov, skupnih specifikacij ali evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi Uredbe (EU) 2019/881, ki določajo domnevo o skladnosti s strani proizvajalcev, organom za nadzor trga olajšala preverjanje skladnosti izdelkov z digitalnimi elementi. Zato se proizvajalce izdelkov z digitalnimi elementi spodbuja k uporabi takih harmoniziranih standardov, skupnih specifikacij ali evropskih certifikacijskih shem za kibernetsko varnost.

(88) Proizvajalci bi morali pripraviti EU izjavo o skladnosti, da se zagotovijo informacije, ki se zahtevajo s to uredbo, o skladnosti izdelkov z digitalnimi elementi z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe in, kadar je ustrezno, druge ustrezne harmonizacijske zakonodaje Unije, ki zajema izdelek z digitalnimi elementi. Priprava EU izjave o skladnosti se lahko od proizvajalcev zahteva tudi z drugimi pravnimi akti Unije. Da bi se zagotovil učinkovit dostop do informacij za namene nadzora trga, bi bilo treba pripraviti enotno EU izjavo o skladnosti za vse ustrezne pravne akte Unije. Omogočiti bi bilo treba, da je enotna EU izjava o skladnosti tudi dosje z zadevnimi posameznimi izjavami o skladnosti, da se zmanjša upravno breme gospodarskih subjektov.

(89) Oznaka CE, ki označuje skladnost izdelka, je vidna posledica celotnega postopka, ki obsega ugotavljanje skladnosti v širšem pomenu. Splošna načela, ki urejajo oznako CE, so določena v Uredbi (ES) št. 765/2008 Evropskega parlamenta in Sveta ([29]). V tej uredbi bi bilo treba določiti pravila o namestitvi oznake CE na izdelke z digitalnimi elementi. Oznaka CE bi morala biti edina oznaka, ki jamči skladnost izdelkov z digitalnimi elementi z zahtevami iz te uredbe.

(90) Da bi lahko gospodarski subjekti dokazali skladnost z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe, organi za nadzor trga pa zagotovili, da izdelki z digitalnimi elementi, dostopni na trgu, izpolnjujejo te zahteve, je treba določiti postopke ugotavljanja skladnosti. Sklep št. 768/2008/ES Evropskega parlamenta in Sveta ([30]) določa

([29]) 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).

([30]) Sklep št. 768/2008/ES Evropskega parlamenta in Sveta z dne 9. julija 2008 o skupnem okviru za trženje proizvodov in razveljavitvi Sklepa Sveta 93/465/EGS (UL L 218, 13.8.2008, str. 82).

module za postopke ugotavljanja skladnosti, ki so sorazmerni z ravnjo tveganja in zahtevano ravnjo varnosti. Za zagotovitev medsektorske skladnosti in preprečitev *ad hoc* različic bi morali postopki ugotavljanja skladnosti, primerni za preverjanje skladnosti izdelkov z digitalnimi elementi z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe, temeljiti na teh modulih. Pri postopkih ugotavljanja skladnosti bi bilo treba proučiti in preveriti zahteve, povezane z izdelki in postopki, ki zajemajo celotni življenjski cikel izdelkov z digitalnimi elementi, vključno z načrtovanjem, zasnovo, razvojem ali proizvodnjo, preskušanjem in vzdrževanjem izdelka z digitalnimi elementi.

(91) Proizvajalec se lahko odloči, da na lastno odgovornost po postopku notranjega nadzora na podlagi modula A iz Sklepa št. 768/2008/ES opravi ugotavljanje skladnosti izdelkov z digitalnimi elementi, ki niso navedeni v tej uredbi kot pomembni ali kritični izdelki z digitalnimi elementi, v skladu s to uredbo. Enako velja tudi za primere, kadar se proizvajalec odloči, da v celoti ali delno ne bo uporabljal veljavnega harmoniziranega standarda, skupne specifikacije ali evropske certifikacijske sheme za kibernetsko varnost. Proizvajalec ohrani prožnost, da izbere strožji postopek ugotavljanja skladnosti, pri katerem sodeluje tretja oseba. Proizvajalec v okviru postopka notranjega nadzora za ugotavljanje skladnosti zagotovi in na lastno odgovornost izjavi, da izdelek z digitalnimi elementi in postopki proizvajalca izpolnjujejo veljavne bistvene zahteve glede kibernetske varnosti iz te uredbe. Če pomemben izdelek z digitalnimi elementi sodi v razred I, je potrebno dodatno zagotovilo, da se dokaže skladnost z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe. Proizvajalec, ki želi na lastno odgovornost opraviti ugotavljanje skladnosti (modul A), bi moral uporabiti harmonizirane standarde, skupne specifikacije ali evropske certifikacijske sheme za kibernetsko varnost, sprejete na podlagi Uredbe (EU) 2019/881, ki jih je Komisija opredelila v izvedbenem aktu. Če proizvajalec ne uporabi takih harmoniziranih standardov, skupnih specifikacij ali evropskih certifikacijskih shem za kibernetsko varnost, bi moral izvesti ugotavljanje skladnosti, pri katerem sodeluje tretja oseba (na podlagi modulov B in C ali modula H). Ob upoštevanju upravnega bremena za proizvajalce ter dejstva, da ima kibernetska varnost pomembno vlogo v fazi zasnove in razvoja materialnih in nematerialnih izdelkov z digitalnimi elementi, so bili postopki ugotavljanja skladnosti, ki temeljijo na modulih B in C oziroma modulu H iz Sklepa št. 768/2008/ES, izbrani kot najustreznejši za sorazmerno in učinkovito ugotavljanje skladnosti pomembnih izdelkov z digitalnimi elementi. Proizvajalec, ki zagotovi ugotavljanje skladnosti, ki ga opravi tretja oseba, lahko izbere najustreznejši postopek za svoj postopek zasnove in proizvodnje. Zaradi še večjega tveganja za kibernetsko varnost, povezanega z uporabo pomembnih izdelkov z digitalnimi elementi, ki spadajo v razred II, bi morala pri ugotavljanju skladnosti vselej sodelovati tretja oseba, tudi kadar je izdelek v celoti ali delno skladen s harmoniziranimi standardi, skupnimi specifikacijami ali evropskimi certifikacijskimi shemami za kibernetsko varnost. Proizvajalcem pomembnih izdelkov z digitalnimi elementi, ki se štejejo za prosto in odprtokodno programsko opremo, je treba omogočiti, da sledijo postopku notranje kontrole na podlagi modula A, če tehnično dokumentacijo dajo na voljo javnosti.

(92) Medtem ko so pri ustvarjanju materialnih izdelkov z digitalnimi elementi običajno potrebna precejšnja prizadevanja proizvajalcev v fazah zasnove, razvoja in proizvodnje, je ustvarjanje izdelkov z digitalnimi elementi v obliki programske opreme skoraj povsem osredotočeno na zasnovo in razvoj, faza proizvodnje pa ima manjšo vlogo. Ne glede na to je v številnih primerih vseeno treba izdelke programske opreme pripraviti, izdelati, pakirati, dati na voljo za prenos ali prenesti na fizične nosilce, preden se dajo na trg. Te dejavnosti bi bilo treba šteti za dejavnosti, ki pomenijo proizvodnjo, kadar se ustrezni moduli za ugotavljanje skladnosti uporabijo za preverjanje skladnosti izdelka z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe v fazah zasnove, razvoja in proizvodnje.

(93) Da bi zagotovili sorazmernost za mikropodjetja in mala podjetja, je primerno zmanjšati upravne stroške, ne da bi pri tem vplivali na raven kibernetske zaščite izdelkov z digitalnimi elementi, ki spadajo na področje uporabe te uredbe, ali na enake konkurenčne pogoje med proizvajalci. Zato je primerno, da Komisija za potrebe mikropodjetij in malih podjetij vzpostavi poenostavljen obrazec za tehnično dokumentacijo. Poenostavljeni obrazec za tehnično dokumentacijo, ki ga sprejme Komisija, bi moral zajemati vse veljavne elemente v zvezi s tehnično dokumentacijo iz te uredbe in določati, kako lahko mikropodjetje ali malo podjetje v jedrnati obliki zagotovi zahtevane elemente, na primer z opisom zasnove, razvoja in proizvodnje izdelka z digitalnimi elementi. Z obrazcem bi prispevali k zmanjšanju upravnega bremena v zvezi s skladnostjo, saj bi zadevnim podjetjem zagotovil pravno varnost glede obsega in podrobnosti informacij, ki jih je treba zagotoviti. Mikropodjetjem in malim podjetjem bi bilo treba omogočiti, da se odločijo za obsežno zagotavljanje ustreznih elementov, povezanih s tehnično dokumentacijo, ter ne bi smela izkoristiti poenostavljene tehnične oblike, ki jim je na voljo.

(94) Da bi spodbudili in zaščitili inovacije je treba zlasti upoštevati interese proizvajalcev, ki so mikropodjetja ali mala ali srednja podjetja, predvsem pa mikropodjetij in malih podjetij, vključno z zagonskimi podjetji. Države članice bi lahko zato razvile pobude, namenjene proizvajalcem, ki so mikropodjetja ali mala podjetja, vključno z usposabljanjem, ozaveščanjem, obveščanjem, testiranjem ter dejavnostmi ugotavljanja skladnosti, ki jih izvajajo tretje osebe, ter vzpostavitvijo peskovnikov. Stroški prevajanja obvezne dokumentacije, kot so tehnična dokumentacija ter informacije in navodila za uporabnika, ki se zahtevajo na podlagi te uredbe, ter komunikacija z organi so lahko pomemben strošek za proizvajalce, zlasti manjše. Države članice bi morale zato morale imeti možnost, da štejejo enega od jezikov, ki jih določijo in sprejmejo za dokumentacijo zadevnih proizvajalcev in za komunikacijo s proizvajalci, za jezik, ki ga na splošno razume največje možno število uporabnikov.

(95) Da bi omogočili nemoteno izvajanje te uredbe, bi si morale države članice prizadevati, da pred datumom začetka uporabe te uredbe zagotovijo, da je v Uniji dovolj priglašenih organov za ugotavljanje skladnosti, ki ga opravi tretja oseba. Komisija bi si morala prizadevati, da pomaga državam članicam in drugim ustreznim strankam pri teh prizadevanjih, da bi preprečili nastajanje ozkih grl in ovir za proizvajalce pri vstopu na trg. S ciljno usmerjenimi dejavnostmi usposabljanja, ki jih vodijo države članice, kadar je primerno tudi s podporo Komisije, se lahko prispeva k razpoložljivosti usposobljenih strokovnjakov, tudi v podporo dejavnostim priglašenih organov na podlagi te uredbe. Glede na stroške, ki jih lahko povzroči ugotavljanje skladnosti, ki ga opravi tretja oseba, bi bilo treba razmisliti tudi o pobudah za financiranje na ravni Unije in nacionalni ravni, s katerimi bi zmanjšali take stroške za mikropodjetja in mala podjetja.

(96) Da bi poskrbeli za sorazmernost, bi morali organi za ugotavljanje skladnosti pri določanju pristojbin za postopke ugotavljanja skladnosti upoštevati posebne interese in potrebe mikropodjetij ter malih in srednjih podjetij, vključno z zagonskimi podjetji. Zlasti bi morali organi za ugotavljanje skladnosti uporabljati ustrezen postopek pregleda in preskuse iz te uredbe le, kadar je primerno in v skladu s pristopom, ki temelji na tveganju.

(97) Cilj regulativnih peskovnikov bi moral biti, da spodbujajo inovacije in konkurenčnost podjetij z vzpostavitvijo nadzorovanih preskusnih okolij za izdelke z digitalnimi elementi preden se dajo na trg. Regulativni peskovniki bi morali prispevati k izboljšanju pravne varnosti za vse akterje, ki spadajo na področje uporabe te uredbe, ter olajšati in pospešiti dostop do trga Unije za izdelke z digitalnimi elementi, zlasti kadar jih zagotavljajo mikro podjetja in mala podjetja, vključno z zagonskimi podjetji.

(98) Za izvajanje ugotavljanja skladnosti, ki ga opravi tretja oseba, za izdelke z digitalnimi elementi bi morali nacionalni priglasitveni organi Komisiji in drugim državam članicam priglasiti organe za ugotavljanje skladnosti, če izpolnjujejo vrsto zahtev, zlasti glede neodvisnosti, pristojnosti in neobstoja nasprotja interesov.

(99) Za zagotovitev dosledne ravni kakovosti pri ugotavljanju skladnosti izdelkov z digitalnimi elementi je treba določiti tudi zahteve za priglasitvene organe in druge organe, vključene v ocenjevanje, priglasitev in spremljanje priglašenih organov. Sistem iz te uredbe bi bilo treba dopolniti s sistemom akreditacije, določenim v Uredbi (ES) št. 765/2008. Ker je akreditacija ključno sredstvo za preverjanje usposobljenosti organov za ugotavljanje skladnosti, bi jo bilo treba uporabljati tudi za namene priglasitve.

(100) Organe za ugotavljanje skladnosti, ki so bili akreditirani in priglašeni na podlagi prava Unije, ki določa zahteve, podobne tistim iz te uredbe, kot je organ za ugotavljanje skladnosti, ki je bil priglašen za evropsko certifikacijsko shemo za kibernetsko varnost, sprejeto na podlagi Uredbe (EU) 2019/881, ali priglašen na podlagi Delegirane uredbe (EU) 2022/30, bi bilo treba na novo oceniti in priglasiti na podlagi te uredbe. Ustrezni organi pa lahko določijo sinergije med zahtevami, ki se morda prekrivajo, da bi preprečili nepotrebno finančno in upravno breme ter zagotovili nemoten in pravočasen postopek obveščanja.

(101) Nacionalni javni organi po vsej Uniji bi morali pregledno akreditacijo, kot je določena v Uredbi (ES) št. 765/2008 za zagotovitev potrebne ravni zaupanja v certifikate o skladnosti, šteti za prednostno sredstvo za dokazovanje strokovne usposobljenosti organov za ugotavljanje skladnosti. Vendar pa lahko nacionalni organi menijo, da razpolagajo z ustreznimi sredstvi, s katerimi lahko sami opravijo to ocenjevanje. V takih primerih bi morali za zagotovitev ustrezne ravni verodostojnosti ocenjevanja, ki ga opravijo drugi nacionalni organi, Komisiji in drugim državam članicam predložiti potrebne listinske dokaze, da ocenjeni organi za ugotavljanje skladnosti izpolnjujejo ustrezne regulativne zahteve.

(102) Organi za ugotavljanje skladnosti za dele svojih dejavnosti, povezanih z ugotavljanjem skladnosti, pogosto sklenejo pogodbo s podizvajalci ali jih prenesejo na odvisno podjetje. Za ohranitev ravni varstva, ki se zahteva za izdelke z digitalnimi elementi, ki bodo dani na trg, je bistveno, da podizvajalci in odvisna podjetja, ki ugotavljajo skladnost, izpolnjujejo iste zahteve kot priglašeni organi glede opravljanja nalog ugotavljanja skladnosti.

(103) Priglasitveni organ bi moral Komisiji in drugim državam članicam priglasiti organ za ugotavljanje skladnosti prek informacijskega sistema o priglašenih in določenih organih novega pristopa (v nadaljnjem besedilu: informacijski sistem NANDO). Informacijski sistem NANDO je elektronsko orodje za priglasitev, ki ga je razvila in ga upravlja Komisija ter vsebuje seznam vseh priglašenih organov.

(104) Ker lahko priglašeni organi ponujajo svoje storitve po vsej Uniji, je primerno državam članicam in Komisiji dati priložnost, da izrazijo svoje pripombe glede priglašenega organa. Zato je pomembno določiti obdobje, v katerem se lahko pojasnijo vsi dvomi ali pomisleki glede sposobnosti organov za ugotavljanje skladnosti, preden začnejo delovati kot priglašeni organi.

(105) Za konkurenčnost je ključno, da priglašeni organi uporabljajo postopke ugotavljanja skladnosti brez nepotrebne obremenitve gospodarskih subjektov. Iz istega razloga in za zagotovitev enake obravnave gospodarskih subjektov je treba zagotoviti dosledno tehnično uporabo postopkov ugotavljanja skladnosti. To bi bilo mogoče najbolje doseči z ustreznim usklajevanjem in sodelovanjem priglašenih organov.

(106) Nadzor trga je ključno sredstvo za zagotavljanje pravilne in enotne uporabe prava Unije. Zato je primerno vzpostaviti pravni okvir, v katerem se lahko ustrezno izvaja nadzor trga. Pravila o nadzoru trga Unije in nadzoru izdelkov, ki vstopajo na trg Unije, določena v Uredbi (EU) 2019/1020, se uporabljajo za izdelke z digitalnimi elementi, ki spadajo na področje uporabe te uredbe.

(107) V skladu z Uredbo (EU) 2019/1020 organ za nadzor trga izvaja nadzor trga na ozemlju države članice, ki ga imenuje. Ta uredba državam članicam ne bi smela preprečevati izbire pristojnih organov za izvedbo nalog nadzora trga. Vsaka država članica bi morala imenovati en ali več organov za nadzor trga na svojem ozemlju. Države članice bi morale imeti možnost, da za opravljanje nalog organa za nadzor trga imenujejo kateri koli obstoječ ali nov organ, vključno s pristojnimi organi, imenovanimi ali ustanovljenimi na podlagi člena 8 Direktive (EU) 2022/2555, nacionalnimi certifikacijskimi organi za kibernetsko varnost, imenovanimi na podlagi člena 58 Uredbe (EU) 2019/881, ali organi za nadzor trga, imenovanimi za namene Direktive 2014/53/EU. Gospodarski subjekti bi morali v celoti sodelovati z organi za nadzor trga in drugimi pristojnimi organi. Vsaka država članica bi morala Komisijo in druge države članice obvestiti o svojih organih za nadzor trga in področjih, za katera je vsak od teh organov pristojen, ter zagotoviti potrebne vire ter znanja in spretnosti za izvajanje nalog nadzora trga v zvezi s to uredbo. Na podlagi člena 10(2) in (3) Uredbe (EU) 2019/1020 bi morala vsaka država članica imenovati enotni povezovalni organ, ki bi moral biti med drugim odgovoren za zastopanje usklajenega stališča organov za nadzor trga in pomoč pri sodelovanju med organi za nadzor trga v različnih državah članicah.

(108) Na podlagi člena 30(2) Uredbe (EU) 2019/1020 bi bilo treba za enotno uporabo te uredbe ustanoviti posebno skupino ADCO za kibernetsko odpornost izdelkov z digitalnimi elementi. Skupino ADCO bi morali sestavljati predstavniki imenovanih organov za nadzor trga in po potrebi predstavniki enotnih povezovalnih organov. Komisija bi morala podpirati in spodbujati sodelovanje med organi za nadzor trga v okviru mreže Unije za skladnost proizvodov, ustanovljene na podlagi člena 29 Uredbe (EU) 2019/1020, ki jo sestavljajo predstavniki vsake države članice, vključno s predstavnikom vsakega enotnega povezovalnega organa iz člena 10 navedene uredbe, ter neobvezen nacionalni strokovnjak, predsedniki skupin ADCO in predstavniki Komisije. Komisija bi morala sodelovati pri sestankih mreže Unije za skladnost proizvodov, njenih podskupin in zadevne skupine ADCO. Poleg tega bi morala pomagati skupini ADCO z izvršnim sekretariatom, ki zagotavlja tehnično in logistično podporo. Skupina ADCO lahko k sodelovanju povabi tudi neodvisne strokovnjake in se poveže z drugimi skupinami ADCO, kot je tista iz Direktive 2014/53/EU.

(109) Organi za nadzor trga bi morali prek skupine ADCO, ustanovljene na podlagi te uredbe, tesno sodelovati in imeti možnost, da pripravijo usmeritve za olajšanje dejavnosti nadzora trga na nacionalni ravni, na primer z razvojem najboljših praks in kazalnikov za učinkovito preverjanje skladnosti izdelkov z digitalnimi elementi s to uredbo.

(110) Za zagotovitev pravočasnih, sorazmernih in učinkovitih ukrepov v zvezi z izdelki z digitalnimi elementi, ki predstavljajo povečano tveganje za kibernetsko varnost, bi bilo treba zagotoviti zaščitni postopek Unije, v okviru katerega so zainteresirane strani obveščene o ukrepih, ki se bodo predvidoma izvajali v zvezi s takimi izdelki. To bi moralo tudi organom za nadzor trga omogočiti, da po potrebi v sodelovanju z zadevnimi gospodarskimi subjekti ukrepajo v zgodnejši fazi. Kadar se države članice in Komisija strinjajo glede upravičenosti ukrepa, ki ga sprejme država članica, nadaljnja udeležba Komisije ne bi smela biti potrebna, razen kadar je neskladnost posledica pomanjkljivosti harmoniziranega standarda.

(111) V nekaterih primerih lahko izdelek z digitalnimi elementi, ki je skladen s to uredbo, vseeno predstavlja povečano tveganje za kibernetsko varnost ali tveganje za zdravje ali varnost oseb, tveganje za skladnost z obveznostmi na podlagi prava Unije ali nacionalnega prava, namenjene varstvu temeljnih pravic, tveganje za razpoložljivost, avtentičnost, celovitost ali zaupnost storitev, ki jih z uporabo elektronskega informacijskega sistema zagotavljajo bistveni subjekti iz člena 3(1) Direktive (EU) 2022/2555, ali tveganje za druge vidike zaščite javnega interesa. Treba je torej določiti pravila, s katerimi se zmanjšajo ta tveganja. Zato bi morali organi za nadzor trga sprejeti ukrepe in od gospodarskega subjekta zahtevati, da zagotovi, da izdelek ne predstavlja več tveganja ali ga odpokliče ali umakne, odvisno od tveganja. Ko organ za nadzor trga tako omeji ali prepove prosti pretok izdelka z digitalnimi elementi, bi morala država članica Komisijo in druge države članice nemudoma uradno obvestiti o začasnih ukrepih ter pri tem navesti razloge in utemeljitev svoje odločitve. Kadar organ za nadzor trga sprejme take ukrepe za izdelke z digitalnimi elementi, ki predstavljajo tveganje, bi se morala Komisija brez odlašanja posvetovati z državami članicami in zadevnim gospodarskim subjektom ali subjekti ter oceniti nacionalni ukrep. Na podlagi rezultatov te ocene bi se morala Komisija odločiti, ali je nacionalni ukrep upravičen ali ne. Komisija bi morala svojo odločitev nasloviti na vse države članice ter jo nemudoma sporočiti njim in zadevnemu gospodarskemu subjektu ali subjektom. Če se šteje, da je ukrep upravičen, bi morala Komisija razmisliti tudi o sprejetju predlogov za revizijo ustreznega prava Unije.

(112) Komisija bi morala imeti možnost, da za izdelke z digitalnimi elementi, ki predstavljajo povečano tveganje za kibernetsko varnost in v zvezi s katerimi obstaja razlog za domnevo, da niso skladni s to uredbo, ali za izdelke, ki so skladni s to uredbo, vendar predstavljajo druga pomembna tveganja, kot so tveganja za zdravje ali varnost oseb, skladnost z obveznostmi na podlagi prava Unije ali nacionalnega prava, namenjenih varstvu temeljnih pravic ali razpoložljivosti, avtentičnosti, celovitosti ali zaupnosti storitev bistvenih subjektov, ki jih zagotavlja uporaba elektronskega informacijskega sistema iz člena 3(1) Direktive (EU) 2022/2555, od agencije ENISA zahteva, naj opravi oceno. Na podlagi te ocene bi morala imeti Komisija možnost, da z izvedbenimi akti sprejme popravne ali omejevalne ukrepe na ravni Unije, vključno z zahtevo za umik zadevnih izdelkov z digitalnimi elementi s trga ali njihovega odpoklica v razumnem roku, ki je sorazmeren z naravo tveganja. Komisija bi morala imeti možnost, da uporabi take ukrepe samo v izjemnih okoliščinah, ki upravičujejo takojšnje ukrepanje za ohranitev pravilnega delovanja notranjega trga, in samo, kadar organi za nadzor trga niso sprejeli učinkovitih ukrepov za odpravo težave. Take izjemne okoliščine so lahko izredne razmere, v katerih na primer proizvajalec zagotovi splošno dostopnost neskladnega izdelka z digitalnimi elementi v več državah članicah in ta izdelek v ključnih sektorjih uporabljajo tudi subjekti, ki spadajo na področje uporabe Direktive (EU) 2022/2555, pri čemer pa vključuje znane ranljivosti, ki jih izrabljajo zlonamerni akterji in za katere proizvajalec ne zagotovi razpoložljivih popravkov. Komisija bi morala imeti možnost, da posreduje v takih izrednih razmerah, samo med trajanjem izjemnih okoliščin in če se neskladnost s to uredbo ali pomembna tveganja ne odpravijo.

(113) Kadar obstajajo znaki neskladnosti s to uredbo v več državah članicah, bi morali imeti organi za nadzor trga možnost, da izvajajo skupne dejavnosti z drugimi organi, da preverijo skladnost in ugotovijo tveganja za kibernetsko varnost, ki jih povzročajo izdelki z digitalnimi elementi.

(114) Sočasni usklajeni kontrolni ukrepi (v nadaljnjem besedilu: usklajene preiskave) so posebni izvršilni ukrepi organov za nadzor trga, s katerimi je mogoče dodatno izboljšati varnost izdelkov. Usklajene preiskave bi bilo treba izvesti zlasti, kadar tržni trendi, pritožbe potrošnikov ali drugi znaki kažejo, da nekatere kategorije izdelkov z digitalnimi elementi pogosto predstavljajo tveganja za kibernetsko varnost. Poleg tega bi morali organi za nadzor trga pri določanju kategorij izdelkov, ki bodo predmet usklajenih preiskav, upoštevati tudi razmere v zvezi z netehničnimi dejavniki tveganja. Organi za nadzor trga bi zato morali imeti možnost, da upoštevajo rezultate usklajenih ocen tveganja za varnost kritičnih dobavnih verig na ravni Unije, izvedenih v skladu s členom 22 Direktive (EU) 2022/2555, vključno z razmerami v zvezi z netehničnimi dejavniki tveganja. Agencija ENISA bi morala organom za nadzor trga predložiti predloge za kategorije izdelkov z digitalnimi elementi, za katere bi se lahko organizirale usklajene preiskave, med drugim na podlagi obvestil o ranljivostih izdelkov in incidentih, ki jih prejme.

(115) Glede na svoje strokovno znanje in mandat bi morala agencija ENISA biti sposobna podpirati postopek za izvajanje te uredbe. Zlasti bi morala biti agencija ENISA zmožna predlagati skupne dejavnosti organov za nadzor trga na podlagi znakov ali informacij v zvezi z morebitno neskladnostjo izdelkov z digitalnimi elementi s to uredbo v več državah članicah ali določiti kategorije izdelkov, za katere bi bilo treba organizirati usklajene preiskave. Agencija ENISA bi morala biti na zahtevo Komisije sposobna v izjemnih okoliščinah opraviti ocene v zvezi s posameznimi izdelki z digitalnimi elementi, ki pomenijo povečano tveganje za kibernetsko varnost, kadar je potrebno takojšnje ukrepanje, da se ohrani dobro delovanje notranjega trga.

(116) S to uredbo se na agencijo ENISA prenesejo nekatere naloge, za katere so potrebni ustrezni viri v smislu strokovnega znanja in človeških virov, da bi jih lahko agencija ENISA učinkovito izvajala. Komisija bo pri pripravi predloga splošnega proračuna Unije predlagala potrebna proračunska sredstva za kadrovski načrt agencije ENISA v skladu s postopkom iz člena 29 Uredbe (EU) 2019/881. Med tem postopkom bo Komisija preučila skupna sredstva agencije ENISA, da bi ji omogočila izpolnjevanje njenih nalog, vključno s tistimi, ki se na agencijo ENISA prenesejo na podlagi te uredbe.

(117) Za zagotovitev, da se lahko regulativni okvir po potrebi prilagodi, bi bilo treba na Komisijo prenesti pooblastilo, da v skladu s členom 290 Pogodbe o delovanju Evropske unije (PDEU) sprejeme akte, da se posodobi priloga k tej uredbi s seznamom pomembnih izdelkov z digitalnimi elementi. V skladu z navedenim členom bi bilo treba na Komisijo prenesti pooblastilo za sprejemanje aktov za opredelitev izdelkov z digitalnimi elementi, zajetih z drugimi pravili Unije, s katerimi se doseže enaka raven varstva kot s to uredbo, v katerih se določi, ali bi bila potrebna omejitev ali izključitev s področja uporabe te uredbe, in po potrebi obseg te omejitve. Poleg tega bi bilo treba v skladu z navedenim členom na Komisijo prenesti tudi pooblastilo za sprejemanje aktov v zvezi z morebitno zahtevo po certificiranju kritičnih izdelkov z digitalnimi elementi v okviru evropske certifikacijske sheme za kibernetsko varnost iz priloge k tej uredbi, pa tudi za posodobitev seznama kritičnih izdelkov z digitalnimi elementi na podlagi meril kritičnosti iz te uredbe ter za določitev evropskih certifikacijskih shem za kibernetsko varnost, sprejetih na podlagi Uredbe (EU) 2019/881, ki se lahko uporabijo za dokazovanje skladnosti z bistvenimi zahtevami glede kibernetske varnosti ali njihovimi deli, iz priloge k tej uredbi. Na Komisijo bi bilo treba prenesti tudi pooblastilo za sprejemanje aktov za določitev minimalnih obdobij podpore za določene kategorije izdelkov, kadar podatki o nadzoru trga kažejo, da so obdobja podpore neustrezna, ter za določitev pogojev za uporabo razlogov, povezanih s kibernetsko varnostjo, v zvezi z odložitvijo razširjanja obvestil o aktivno izrabljenih ranljivostih. Poleg tega bi bilo treba na Komisijo prenesti pooblastilo za sprejemanje aktov za vzpostavitev prostovoljnih programov izdajanja varnostnih potrdil za ocenjevanje skladnosti izdelkov z digitalnimi elementi, ki se štejejo za prosto in odprtokodno programsko opremo, z vsemi ali nekaterimi bistvenimi zahtevami glede kibernetske varnosti ali drugimi obveznostmi iz te uredbe, ter za določitev minimalne vsebine EU izjave o skladnosti in dopolnitev elementov, ki jih je treba vključiti v tehnično dokumentacijo. Zlasti je pomembno, da se Komisija pri svojem pripravljalnem delu ustrezno posvetuje, vključno na ravni strokovnjakov, in da se ta posvetovanja izvedejo v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje ([31]). Za zagotovitev enakopravnega sodelovanja pri pripravi delegiranih aktov Evropski parlament in Svet zlasti prejmeta vse dokumente sočasno s strokovnjaki iz držav članic, njuni strokovnjaki pa se sistematično lahko udeležujejo sestankov strokovnih skupin Komisije, ki zadevajo pripravo delegiranih aktov. Pooblastilo za sprejetje delegiranih aktov na podlagi te uredbe bi se moralo prenesti na Komisijo za obdobje petih let od 10. decembra 2024. Komisija bi morala pripraviti poročilo o prenosu pooblastila najpozneje devet mesecev pred koncem petletnega obdobja. Prenos pooblastila bi se moral samodejno podaljševati za enako dolga obdobja, razen če Evropski parlament ali Svet nasprotuje temu podaljšanju najpozneje tri mesece pred koncem vsakega obdobja.

(118) Za zagotovitev enotnih pogojev za izvajanje te uredbe bi bilo treba na Komisijo prenesti izvedbena pooblastila za določitev tehničnega opisa kategorij pomembnih izdelkov z digitalnimi elementi iz priloge k tej uredbi, določitev oblike in elementov kosovnice za programsko opremo, podrobnejšo določitev oblike in postopka za obvestila o aktivno izrabljenih ranljivostih in resnih incidentih, ki vplivajo na varnost izdelkov z digitalnimi elementi, ki jih predložijo proizvajalci, določitev skupnih specifikacij, ki zajemajo tehnične zahteve, ki zagotavljajo način za izpolnjevanje bistvenih zahtev glede kibernetske varnosti iz priloge k tej uredbi, določitev tehničnih specifikacij za označbe, piktograme ali druge oznake v zvezi z varnostjo izdelkov z digitalnimi elementi, obdobja njihove podpore in mehanizmov za spodbujanje njihove uporabe ter za povečanje ozaveščenosti javnosti o varnosti izdelkov z digitalnimi elementi, določitev poenostavljenega dokumentacijskega obrazca, namenjenega potrebam mikropodjetij in malih podjetij, ter sprejetje odločitve o popravnih ali omejevalnih ukrepih na ravni Unije v izjemnih

([31]) UL L 123, 12.5.2016, str. 1.

okoliščinah, ki upravičujejo takojšnje ukrepanje za ohranitev pravilnega delovanja notranjega trga. Ta pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta ([32]).

(119) Za zagotovitev zaupanja vrednega in konstruktivnega sodelovanja organov za nadzor trga na ravni Unije in nacionalni ravni bi morale vse strani, vključene v uporabo te uredbe, spoštovati zaupnost informacij in podatkov, pridobljenih pri opravljanju svojih nalog.

(120) Za zagotovitev učinkovitega izvrševanja obveznosti iz te uredbe bi moral biti vsak organ za nadzor trga pooblaščen, da naloži ali zahteva naložitev upravnih glob. Zato bi bilo treba določiti najvišje zneske upravnih glob za neizpolnjevanje obveznosti iz te uredbe, ki se predpišejo v nacionalnem pravu. Pri odločanju o znesku upravne globe v vsakem posameznem primeru bi bilo treba upoštevati vse zadevne okoliščine obravnavanega primera in vsaj tiste, ki so izrecno navedene v tej uredbi, vključno s tem, ali je proizvajalec mikropodjetje, malo ali srednje podjetje ali zagonsko podjetje, in ali so upravne globe istemu gospodarskemu subjektu za podobne kršitve že naložili isti ali drugi organi za nadzor trga. Take okoliščine bi lahko bile obteževalne, kadar se kršitev istega gospodarskega subjekta ne odpravi na ozemlju držav članic, ki niso država članica, v kateri je bila že naložena upravna globa, ali olajševalne, pri čemer bi se morala pri morebitni drugi upravni globi, ki jo za isti gospodarski subjekt ali isto vrsto kršitve obravnava drug organ za nadzor trga, poleg drugih ustreznih posebnih okoliščin že upoštevati kazen, naložena v drugih državah članicah, in njen znesek. V vseh takih primerih bi bilo treba pri skupni upravni globi, ki jo lahko istemu gospodarskemu subjektu za isto vrsto kršitve naložijo organi za nadzor trga v več državah članicah, zagotoviti upoštevanje načela sorazmernosti. Glede na to, da se upravne globe ne uporabljajo za mikropodjetja ali mala podjetja, ker niso izpolnila 24-urnega roka za zgodnje opozarjanje o aktivno izrabljenih ranljivostih ali resnih incidentih, ki vplivajo na varnost izdelka z digitalnimi elementi, niti za upravljavce odprtokodne programske opreme, za vsako kršitev te uredbe, in glede na načelo, da bi morale biti kazni učinkovite, sorazmerne in odvračilne, države članice tem subjektom ne bi smele naložiti drugih vrst denarnih kazni.

(121) Kadar se upravne globe naložijo osebi, ki ni podjetje, bi moral pristojni organ pri določanju ustreznega zneska globe upoštevati splošno raven dohodka v državi članici in ekonomski položaj osebe. Države članice bi morale določiti, ali bi se morale upravne globe uporabljati tudi za javne organe in v kakšnem obsegu.

(122) Države članice bi morale ob upoštevanju nacionalnih okoliščin preučiti možnost uporabe prihodkov od kazni iz te uredbe ali enakovrednih finančnih sredstev, da podprejo politike na področju kibernetske varnosti in povečajo raven kibernetske varnosti v Uniji, med drugim s povečanjem števila usposobljenih strokovnjakov za kibernetsko varnost, krepitvijo zmogljivosti mikropodjetij ter malih in srednjih podjetij ter ozaveščanjem javnosti o kibernetskih grožnjah.

(123) Unija si v odnosih s tretjimi državami prizadeva za spodbujanje mednarodne trgovine z reguliranimi izdelki. Za spodbujanje trgovine se lahko uporabijo najrazličnejši ukrepi, vključno z več pravnimi instrumenti, kakor so dvostranski (medvladni) sporazumi o vzajemnem priznavanju za ugotavljanje skladnosti in označevanje reguliranih izdelkov. Sporazumi o vzajemnem priznavanju se sklenejo med Unijo in tretjimi državami s primerljivo ravnjo tehničnega razvoja in združljivim pristopom k ugotavljanju skladnosti. Ti sporazumi temeljijo na vzajemnem sprejemanju certifikatov, oznak skladnosti in poročil o preskusih, ki jih izdajo organi za ugotavljanje skladnosti katere koli pogodbenice v skladu z zakonodajo druge pogodbenice. Trenutno so sklenjeni sporazumi o vzajemnem priznavanju z več tretjimi državami. Ti sporazumi o vzajemnem priznavanju so sklenjeni za več specifičnih sektorjev, ki se lahko od ene tretje države do druge razlikujejo. Za dodatno spodbujanje trgovine in ob upoštevanju, da so dobavne verige izdelkov z digitalnimi elementi globalne, lahko Unija v skladu s členom 218 PDEU sklene sporazume o vzajemnem priznavanju v zvezi z ugotavljanjem skladnosti za izdelke, ki se urejajo na podlagi te uredbe. Sodelovanje s partnerskimi tretjimi državami je prav tako pomembno za krepitev kibernetske odpornosti na svetovni ravni, saj bo to dolgoročno prispevalo k okrepljenemu okviru kibernetske varnosti v Uniji in zunaj nje.

([32]) 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, ELI: https://eur-lex.europa.eu/eli/reg/2011/182/oj).

(124) Potrošniki bi morali imeti pravico uveljavljati svoje pravice v zvezi z obveznostmi, ki se na podlagi te uredbe naložijo gospodarskim subjektom z zastopniškimi tožbami na podlagi Direktive (EU) 2020/1828 Evropskega parlamenta in Sveta ([33]). V ta namen bi bilo treba v tej uredbi določiti, da se Direktiva (EU) 2020/1828 uporablja za zastopniške tožbe v zvezi s kršitvami te uredbe, ki škodujejo ali bi lahko škodile kolektivnim interesom potrošnikov. Prilogo I k navedeni direktivi bi bilo zato treba ustrezno spremeniti. Države članice morajo zagotoviti, da se te spremembe odražajo v ukrepih za prenos, sprejetih na podlagi navedene direktive, četudi sprejetje nacionalnih ukrepov za prenos v zvezi s tem ni pogoj za uporabo navedene direktive za te zastopniške tožbe. Uporaba navedene direktive za zastopniške tožbe zaradi kršitev določb te uredbe s strani gospodarskih subjektov, ki škodujejo ali bi lahko škodili kolektivnim interesom potrošnikov, bi se morala začeti 11. decembra 2027.

(125) Komisija bi morala v posvetovanju z ustreznimi deležniki redno ocenjevati in pregledovati to uredbo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim družbenim, političnim, tehnološkim ali tržnim razmeram. Ta uredba bo olajšala izpolnjevanje obveznosti glede varnosti dobavne verige za subjekte, ki spadajo na področje uporabe Uredbe (EU) 2022/2554 in Direktive (EU) 2022/2555 ter uporabljajo izdelke z digitalnimi elementi. Komisija bi morala v okviru tega rednega pregleda oceniti skupne učinke okvira Unije za kibernetsko varnost.

(126) Gospodarskim subjektom bi bilo treba zagotoviti dovolj časa za prilagoditev zahtevam, določenim v tej uredbi. Ta uredba bi se morala začeti uporabljati 11. decembra 2027, razen obveznosti poročanja v zvezi z aktivno izkoriščenimi ranljivostmi in resnimi incidenti, ki vplivajo na varnost izdelkov z digitalnimi elementi, ki bi se morale začeti uporabljati 11. septembra 2026 in določb o priglasitvi organov za ugotavljanje skladnosti, ki bi se morale začeti uporabljati 11. junija 2026.

(127) Pomembno je, da se mikropodjetjem ter malim in srednjim podjetjem, vključno z zagonskimi podjetji, zagotovi podpora pri izvajanju te uredbe in se čim bolj zmanjšajo tveganja za izvajanje, ki so posledica pomanjkanja znanja in strokovnega znanja na trgu, pa tudi da se proizvajalcem olajša izpolnjevanje njihovih obveznosti iz te uredbe. Program Digitalna Evropa in drugi ustrezni programi Unije zagotavljajo finančno in tehnično podporo, ki tem podjetjem omogoča, da prispevajo k rasti gospodarstva Unije in povečanju skupne ravni kibernetske varnosti v Uniji. Tudi Evropski strokovni center za kibernetsko varnost in nacionalni koordinacijski centri ter evropska vozlišča za digitalne inovacije, ki so jih vzpostavile Komisija in države članice na ravni Unije ali nacionalni ravni, bi tudi lahko podprli podjetja in organizacije javnega sektorja ter prispevali k izvajanju te uredbe. V okviru svojih nalog in področij pristojnosti bi lahko mikropodjetjem ter malim in srednjim podjetjem zagotavljali tehnično in znanstveno podporo, na primer pri dejavnostih preskušanja in ugotavljanjih skladnosti, ki jih opravijo tretje osebe. Prav tako bi lahko spodbujali uporabo orodij za lažje izvajanje te uredbe.

(128) Poleg tega bi morale države članice razmisliti o sprejetju dopolnilnih ukrepov, namenjenih zagotavljanju usmeritev in podpore mikropodjetjem ter malim in srednjim podjetjem, kot je vzpostavitev regulativnih peskovnikov in namenskih kanalov za komunikacijo. Države članice bi lahko raven kibernetske varnosti v Uniji povečale tudi z zagotavljanjem podpore za razvoj zmogljivosti ter znanj in spretnosti, povezanih s kibernetsko varnostjo izdelkov z digitalnimi elementi, izboljšanjem kibernetske odpornosti gospodarskih subjektov, zlasti mikropodjetij ter malih in srednjih podjetij, ter spodbujanjem ozaveščenosti javnosti o kibernetski varnosti izdelkov z digitalnimi elementi.

(129) Ker cilja te uredbe države članice ne morejo zadovoljivo doseči, temveč se zaradi učinkov ukrepa lažje doseže na ravni Unije, lahko Unija sprejme ukrepe v skladu z načelom subsidiarnosti iz člena 5 Pogodbe o Evropski uniji. V skladu z načelom sorazmernosti iz navedenega člena ta uredba ne presega tistega, kar je potrebno za doseganje navedenega cilja.

(130) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta ([34]) je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal 9. novembra 2022 ([35]) –

([33]) Direktiva (EU) 2020/1828 Evropskega parlamenta in Sveta z dne 25. novembra 2020 o zastopniških tožbah za varstvo kolektivnih interesov potrošnikov in razveljavitvi Direktive 2009/22/ES (UL L 409, 4.12.2020, str. 1.

([34]) 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).

([35]) UL C 452, 29.11.2022, str. 23.

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

Ta uredba določa:

(a) pravila za omogočanje dostopnosti izdelkov z digitalnimi elementi na trgu za zagotovitev njihove kibernetske varnosti;

(b) bistvene zahteve glede kibernetske varnosti za zasnovo, razvoj in proizvodnjo izdelkov z digitalnimi elementi ter obveznosti gospodarskih subjektov v zvezi s kibernetsko varnostjo teh izdelkov;

(c) bistvene zahteve glede kibernetske varnosti za postopke obravnavanja ranljivosti, ki jih vzpostavijo proizvajalci, za zagotovitev kibernetske varnosti izdelkov z digitalnimi elementi v času, ko naj bi se izdelki uporabljali, ter obveznosti gospodarskih subjektov v zvezi s temi postopki;

(d) pravila o nadzoru trga, vključno s spremljanjem, ter izvrševanje pravil in zahtev iz tega člena.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za izdelke z digitalnimi elementi, dostopne na trgu, katerih predvideni namen ali razumno predvidljiva uporaba vključuje neposredno ali posredno logično ali fizično podatkovno povezavo z napravo ali omrežjem.

2. Ta uredba se ne uporablja za izdelke z digitalnimi elementi, za katere se uporabljajo naslednji pravni akti Unije:

(a) Uredba (EU) 2017/745;

(b) Uredba (EU) 2017/746;

(c) Uredba (EU) 2019/2144.

3. Ta uredba se ne uporablja za izdelke z digitalnimi elementi, ki so bili certificirani v skladu z Uredbo (EU) 2018/1139.

4. Ta uredba se ne uporablja za opremo, ki spada na področje uporabe Direktive 2014/90/EU Evropskega parlamenta in Sveta ([36]).

5. Uporaba te uredbe za izdelke z digitalnimi elementi, zajete z drugimi pravili Unije, s katerimi so določene zahteve, ki se nanašajo na vsa ali nekatera tveganja, zajeta z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I, se lahko omeji ali izključi, kadar:

(a) je taka omejitev ali izključitev v skladu s splošnim regulativnim okvirom, ki se uporablja za te izdelke, ter

(b) se s sektorskimi pravili doseže enaka ali višja raven varstva, kakor je določena s to uredbo.

V skladu s členom 61 se na Komisijo prenese pooblastilo za sprejemanje delegiranih aktov za dopolnitev te uredbe, tako da se določi, ali je potrebna taka omejitev ali izključitev, ter navedejo zadevni izdelki in pravila ter obseg omejitve, če je ustrezno.

([36]) Direktiva 2014/90/EU Evropskega parlamenta in Sveta z dne 23. julija 2014 o pomorski opremi in razveljavitvi Direktive Sveta 96/98/ES (UL L 257, 28.8.2014, str. 146).

6. Ta uredba se ne uporablja za rezervne dele, ki so dostopni na trgu, da nadomestijo enake sestavne dele v izdelkih z digitalnimi elementi, in so proizvedeni v skladu z istimi specifikacijami kot sestavni deli, ki naj bi jih nadomestili.

7. Ta uredba se ne uporablja za izdelke z digitalnimi elementi, ki se razvijajo ali so spremenjeni izključno za namene nacionalne varnosti ali obrambe, ali za izdelke, ki so izrecno namenjeni obdelavi tajnih podatkov.

8. Obveznosti iz te uredbe ne vključujejo posredovanja informacij, katerih razkritje bi bilo v nasprotju z bistvenimi interesi držav članic na področju nacionalne varnosti, javne varnosti ali obrambe.

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

(1) „izdelek z digitalnimi elementi“ pomeni izdelek programske ali strojne opreme ter njegove rešitve za daljinsko obdelavo podatkov, vključno s sestavnimi deli programske ali strojne opreme, ki se dajejo na trg ločeno;

(2) „daljinska obdelava podatkov“ pomeni obdelavo podatkov na daljavo, za katero je programsko opremo zasnoval in razvil proizvajalec ali je bila zasnovana in razvita pod njegovo odgovornostjo ter brez katere izdelek z digitalnimi elementi ne bi mogel opravljati ene od svojih funkcij;

(3) „kibernetska varnost“ pomeni kibernetsko varnost, kakor je opredeljena v členu 2, točka 1, Uredbe (EU) 2019/881;

(4) „programska oprema“ pomeni del elektronskega informacijskega sistema, ki ga sestavlja računalniška koda;

(5) „strojna oprema“ pomeni fizičen elektronski informacijski sistem, s katerim je mogoče obdelovati, shranjevati ali pošiljati digitalne podatke, ali njegove dele;

(6) „sestavni del“ pomeni programsko ali strojno opremo, predvideno za vgradnjo v elektronski informacijski sistem;

(7) „elektronski informacijski sistem“ pomeni sistem, vključno z električno ali elektronsko opremo, s katerim je mogoče obdelovati, shranjevati ali pošiljati digitalne podatke;

(8) „logična povezava“ pomeni virtualno predstavitev podatkovne povezave, vzpostavljene prek vmesniške programske opreme;

(9) „fizična povezava“ pomeni povezavo med elektronskimi informacijskimi sistemi ali sestavnimi deli, vzpostavljeno s fizičnimi sredstvi, vključno z električnimi, optičnimi ali mehanskimi vmesniki, žicami ali radijskimi valovi;

(10) „posredna povezava“ pomeni povezavo z napravo ali omrežjem, ki ni neposredna, ampak je del večjega sistema, ki ga je mogoče povezati neposredno s tako napravo ali omrežjem;

(11) „končna točka“ pomeni vsako napravo, ki je povezana z omrežjem in se uporablja kot vstopna točka v to omrežje;

(12) „gospodarski subjekt“ pomeni proizvajalca, pooblaščenega zastopnika, uvoznika, distributerja ali drugo fizično ali pravno osebo, za katero veljajo obveznosti v zvezi s proizvodnjo izdelkov z digitalnimi elementi ali omogočanjem dostopnosti izdelkov z digitalnimi elementi na trgu v skladu s to uredbo;

(13) „proizvajalec“ pomeni fizično ali pravno osebo, ki razvija ali izdeluje izdelke z digitalnimi elementi ali za katero se taki izdelki oblikujejo, razvijajo ali izdelujejo ter ki jih trži pod svojim imenom ali znamko, bodisi za plačilo, monetizacijo ali brezplačno;

(14) „upravljavec odprtokodne programske opreme“ pomeni pravno osebo, ki ni proizvajalec in katere namen ali cilj je sistematično in trajno zagotavljati podporo za razvoj posebnih izdelkov z digitalnimi elementi, ki se štejejo za prosto in odprtokodno programsko opremo ter so namenjeni komercialnim dejavnostim, in ki zagotavlja sposobnost preživetja teh izdelkov;

(15) „pooblaščeni zastopnik“ pomeni fizično ali pravno osebo s sedežem v Uniji, ki jo je proizvajalec pisno pooblastil, da v njegovem imenu opravlja določene naloge;

(16) „uvoznik“ pomeni fizično ali pravno osebo s sedežem v Uniji, ki da na trg izdelek z digitalnimi elementi, ki nosi ime ali znamko fizične ali pravne osebe s sedežem zunaj Unije;

(17) „distributer“ pomeni fizično ali pravno osebo v dobavni verigi, razen proizvajalca ali uvoznika, ki da izdelek z digitalnimi elementi na trg Unije, ne da bi vplival na njegove lastnosti;

(18) „potrošnik“ pomeni fizično osebo, ki deluje zunaj okvira svoje trgovske, poslovne, obrtne ali poklicne dejavnosti;

(19) „mikropodjetja“, „mala podjetja“ in „srednja podjetja“ pomeni mikropodjetja, mala in srednja podjetja, kakor so opredeljena v Prilogi k Priporočilu 2003/361/ES;

(20) „obdobje podpore“ pomeni obdobje, v katerem mora proizvajalec zagotoviti, da se ranljivosti izdelka z digitalnimi elementi obravnavajo učinkovito in v skladu z bistvenimi zahtevami glede kibernetske varnosti iz dela II Priloge I;

(21) „dajanje na trg“ pomeni prvo omogočanje dostopnosti izdelka z digitalnimi elementi na trgu Unije;

(22) „omogočanje dostopnosti na trgu“ pomeni dobavo izdelka z digitalnimi elementi za distribucijo ali uporabo na trgu Unije v okviru gospodarske dejavnosti, za plačilo ali brezplačno;

(23) „predvideni namen“ pomeni uporabo, za katero je proizvajalec namenil izdelek z digitalnimi elementi, vključno s posebnimi okoliščinami in pogoji uporabe, kot je navedeno v informacijah, ki jih je proizvajalec predložil v navodilih za uporabo, promocijskem ali prodajnem gradivu in izjavah ter v tehnični dokumentaciji;

(24) „razumno predvidljiva uporaba“ pomeni uporabo, ki ni nujno predvideni namen, ki ga je proizvajalec navedel v navodilih za uporabo, promocijskem ali prodajnem gradivu in izjavah ter v tehnični dokumentaciji, vendar je verjetna posledica razumno predvidljivega človeškega vedenja ali tehničnih operacij ali interakcij;

(25) „razumno predvidljiva napačna uporaba“ pomeni uporabo izdelka z digitalnimi elementi na način, ki ni v skladu s predvidenim namenom, vendar je lahko posledica razumno predvidljivega človeškega vedenja ali interakcije z drugimi sistemi;

(26) „priglasitveni organ“ pomeni nacionalni organ, odgovoren za vzpostavitev in izvajanje potrebnih postopkov za ocenjevanje, imenovanje in priglasitev organov za ugotavljanje skladnosti ter za njihovo spremljanje;

(27) „ugotavljanje skladnosti“ pomeni postopek preverjanja, ali so bistvene zahteve glede kibernetske varnosti iz Priloge I izpolnjene;

(28) „organ za ugotavljanje skladnosti“ pomeni organ za ugotavljanje skladnosti, kakor je opredeljen v členu 2, točka 13, Uredbe (ES) št. 765/2008;

(29) „priglašeni organ“ pomeni organ za ugotavljanje skladnosti, imenovan v skladu s členom 43 in drugo ustrezno harmonizacijsko zakonodajo Unije;

(30) „bistvena sprememba“ pomeni spremembo izdelka z digitalnimi elementi po tem, ko je bil dan na trg, ki vpliva na skladnost tega izdelka z bistvenimi zahtevami glede kibernetske varnosti iz dela I Priloge I ali povzroči spremembo predvidenega namena, za katerega je bil izdelek z digitalnimi elementi ocenjen;

(31) „oznaka CE“ pomeni oznako, s katero proizvajalec izjavlja, da so izdelek z digitalnimi elementi in postopki, ki jih je vzpostavil proizvajalec, skladni z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I in drugo harmonizacijsko zakonodajo Unije, ki se uporablja in določa namestitev oznake;

(32) „harmonizacijska zakonodaja Unije“ pomeni zakonodajo Unije iz Priloge I k Uredbi (EU) 2019/1020 in katero koli drugo zakonodajo Unije, ki harmonizira pogoje za trženje izdelkov, za katere se uporablja navedena uredba;

(33) „organ za nadzor trga“ pomeni organ za nadzor trga, kakor je opredeljen v členu 3, točka 4, Uredbe (EU) 2019/1020;

(34) „mednarodni standard“ pomeni mednarodni standard, kakor je opredeljen v členu 2, točka 1(a), Uredbe (EU) št. 1025/2012;

(35) „evropski standard“ pomeni evropski standard, kakor je opredeljen v členu 2, točka 1(b), Uredbe (EU) št. 1025/2012;

(36) „harmonizirani standard“ pomeni harmonizirani standard, kakor je opredeljen v členu 2, točka 1(c), Uredbe (EU) št. 1025/2012;

(37) „tveganje za kibernetsko varnost“ pomeni možnost izgube ali motnje zaradi incidenta ter se izrazi kot kombinacija razsežnosti take izgube ali motnje in verjetnosti, da bi do incidenta prišlo;

(38) „povečano tveganje za kibernetsko varnost“ pomeni tveganje za kibernetsko varnost, za katero se lahko na podlagi njegovih tehničnih značilnosti domneva, da vključuje veliko verjetnost incidenta, ki bi lahko imel resen negativen vpliv, vključno s povzročitvijo precejšnje materialne ali nematerialne izgube ali motnje;

(39) „kosovnica za programsko opremo“ pomeni uraden zapis, ki vsebuje podrobnosti o sestavnih delih elementov programske opreme izdelka z digitalnimi elementi in njihove odnose v dobavni verigi;

(40) „ranljivost“ pomeni pomanjkljivost, dovzetnost ali napako izdelka z digitalnimi elementi, ki jo kibernetska grožnja lahko izkoristi;

(41) „izrabljiva ranljivost“ pomeni ranljivost, ki jo lahko nasprotnik učinkovito uporabi v praktičnih pogojih delovanja;

(42) „aktivno izrabljena ranljivost“ pomeni ranljivost, za katero obstajajo zanesljivi dokazi, da jo je zlonamerni akter izrabil v sistemu brez dovoljenja lastnika sistema;

(43) „incident“ pomeni incident, kakor je opredeljen v členu 6, točka 6, Direktive (EU) 2022/2555;

(44) „incident, ki vpliva na varnost izdelka z digitalnimi elementi“ pomeni incident, ki negativno vpliva ali bi lahko negativno vplival na zmožnost izdelka z digitalnimi elementi, da zaščiti razpoložljivost, avtentičnost, celovitost ali zaupnost podatkov ali funkcij;

(45) „skorajšnji incident“ pomeni skorajšnji incident, kakor je opredeljen v členu 6, točka 5, Direktive (EU) 2022/2555;

(46) „kibernetska grožnja“ pomeni kibernetsko grožnjo, kakor je opredeljena v členu 2, točka 8, Uredbe (EU) 2019/881;

(47) „osebni podatki“ pomeni osebne podatke, kakor so opredeljeni členu 4, točka 1, Uredbe (EU) 2016/679;

(48) „prosta in odprtokodna programska oprema“ pomeni programsko opremo, katere izvorna koda se odprto deli in ki je na voljo na podlagi proste in odprtokodne licence, ki zagotavlja vse pravice, da postane prosto dostopna, uporabna, jo je mogoče spremeniti in prerazporediti;

(49) „odpoklic“ pomeni odpoklic, kakor je opredeljen v členu 3, točka 22, Uredbe (EU) 2019/1020;

(50) „umik“ pomeni umik, kakor je opredeljen v členu 3, točka 23, Uredbe (EU) 2019/1020;

(51) „skupina CSIRT, ki je imenovana za koordinatorja“ pomeni skupino CSIRT, ki je imenovana za koordinatorja na podlagi člena 12(1) Direktive (EU) 2022/2555.

Člen 4

Prosti pretok

1. Države članice za zadeve, zajete v tej uredbi, ne ovirajo omogočanja dostopnosti izdelkov z digitalnimi elementi, ki so skladni s to uredbo, na trgu.

2. Države članice na sejmih, razstavah in predstavitvah ali podobnih dogodkih ne preprečijo predstavitve ali uporabe izdelka z digitalnimi elementi, ki ni skladen s to uredbo, vključno s prototipi, če je izdelek opremljen z vidno oznako, ki jasno označuje, da ni skladen s to uredbo in da ne bo dan na trg, dokler ne bo skladen z njo.

3. Države članice ne preprečijo omogočanja dostopnosti nedokončane programske opreme, ki ni skladna s to uredbo, na trgu, če je programska oprema dostopna samo za omejeno obdobje, potrebno za preskušanje, ter ima viden znak, ki jasno kaže, da ni skladna s to uredbo in bo dostopna na trgu samo za namene preskušanja.

4. Odstavek 3 se ne uporablja za varnostne komponente iz harmonizacijske zakonodaje Unije, razen te uredbe.

Člen 5

Javno naročanje ali uporaba izdelkov z digitalnimi elementi

1. Ta uredba državam članicam ne preprečuje, da za izdelke z digitalnimi elementi določijo dodatne zahteve glede kibernetske varnosti za javno naročanje ali uporabo teh izdelkov za posebne namene, tudi kadar se ti izdelki naročijo ali uporabljajo za namene nacionalne varnosti ali obrambe, če so take zahteve skladne z obveznostmi držav članic, določenimi v pravu Unije, ter če so potrebne in sorazmerne za doseganje teh namenov.

2. Brez poseganja v direktivi 2014/24/EU in 2014/25/EU države članice pri naročanju izdelkov z digitalnimi elementi, ki spadajo na področje uporabe te uredbe, zagotovijo, da se v postopku javnega naročanja upošteva skladnost z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I k tej uredbi, vključno z zmožnostjo proizvajalcev za učinkovito obravnavanje ranljivosti.

Člen 6

Zahteve za izdelke z digitalnimi elementi

Izdelki z digitalnimi elementi so dostopni na trgu le, kadar:

(a) izpolnjujejo bistvene zahteve glede kibernetske varnosti iz dela I Priloge I, če se ustrezno namestijo, vzdržujejo, uporabljajo za predvideni namen ali pod razumno predvidljivimi pogoji in če so, kadar je ustrezno, nameščene potrebne varnostne posodobitve, ter

(b) so postopki, ki jih je vzpostavil proizvajalec, skladni z bistvenimi zahtevami glede kibernetske varnosti iz dela II Priloge I.

Člen 7

Pomembni izdelki z digitalnimi elementi

1. Izdelki z digitalnimi elementi, ki imajo osnovno funkcijo kategorije izdelkov iz Priloge III, se štejejo za pomembne izdelke z digitalnimi elementi in zanje veljajo postopki ugotavljanja skladnosti iz člena 32(2) in (3). Vgradnja izdelka z digitalnimi elementi, ki ima osnovno funkcijo kategorije izdelkov iz Priloge III, sama po sebi ne pomeni, da za izdelek, v katerega je vgrajen, veljajo postopki ugotavljanja skladnosti iz člena 32(2) in (3).

2. Kategorije izdelkov z digitalnimi elementi iz odstavka 1 tega člena, ki so razdeljene v razreda I in II, kot je določeno v Prilogi III, izpolnjujejo vsaj eno od naslednjih meril:

(a) izdelek z digitalnimi elementi opravlja predvsem funkcije, ki so ključne za kibernetsko varnost drugih izdelkov, omrežij ali storitev, vključno z zagotavljanjem avtentikacije in dostopa, preprečevanjem in odkrivanjem vdorov, varnostjo končnih točk ali zaščito omrežja;

(b) izdelek z digitalnimi elementi opravlja funkcijo z znatnim tveganjem škodljivih učinkov v smislu njene intenzivnosti in zmožnosti motenj, nadzora ali povzročanja škode velikemu številu drugih izdelkov ali zdravju, zaščiti ali varnosti njegovih uporabnikov z neposredno manipulacijo, kot je funkcija centralnega sistema, vključno z upravljanjem omrežja, nadzorom konfiguracije, virtualizacijo ali obdelavo osebnih podatkov.

3. V skladu s členom 61 se na Komisijo prenese pooblastilo za sprejemanje delegiranih aktov za spremembo Priloge III z vključitvijo nove kategorije izdelkov z digitalnimi elementi znotraj vsakega razreda na seznam kategorij izdelkov z digitalnimi elementi in določitvijo njene opredelitve, premikom kategorije izdelkov iz enega razreda v drugega ali umikom obstoječe kategorije s seznama. Komisija pri ocenjevanju potrebe po spremembi seznama iz Priloge III upošteva funkcije, povezane s kibernetsko varnostjo, ali funkcijo in raven tveganja za kibernetsko varnost, ki ga predstavljajo izdelki z digitalnimi elementi, kot je določeno v merilih iz odstavka 2 tega člena.

Delegirani akti iz prvega pododstavka tega odstavka, kadar je ustrezno, določajo minimalno prehodno obdobje 12 mesecev, zlasti kadar se nova kategorija pomembnih izdelkov z digitalnimi elementi doda v razred I ali II ali se premakne iz razreda I v II, kot je določeno v Prilogi III, preden se začnejo uporabljati ustrezni postopki ugotavljanja skladnosti iz člena 32(2) in (3), razen če je zaradi nujnih razlogov upravičeno krajše prehodno obdobje.

4. Komisija do 11. decembra 2025 sprejme izvedbeni akt, v katerem je določen tehnični opis kategorij izdelkov z digitalnimi elementi iz razredov I in II iz Priloge III in tehnični opis kategorij izdelkov z digitalnimi elementi iz Priloge IV. Navedeni izvedbeni akt se sprejme v skladu s postopkom pregleda iz člena 62(2).

Člen 8

Kritični izdelki z digitalnimi elementi

1. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 61 za dopolnitev te uredbe, da se določi, kateri izdelki z digitalnimi elementi, ki imajo osnovno funkcionalnost kategorije izdelkov iz Priloge IV k tej uredbi, morajo pridobiti evropski certifikat kibernetske varnosti na ravni zanesljivosti vsaj „znatno“ v okviru evropske certifikacijske sheme za kibernetsko varnost, sprejete na podlagi Uredbe (EU) 2019/881, da se dokaže skladnost z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I k tej uredbi ali njihovimi deli, če je bila evropska certifikacijska shema za kibernetsko varnost, ki zajema navedene kategorije izdelkov z digitalnimi elementi, sprejeta na podlagi Uredbe (EU) 2019/881 in je na voljo proizvajalcem. V teh delegiranih aktih se določi zahtevana raven zanesljivosti, ki je sorazmerna z ravnjo tveganja za kibernetsko varnost, povezanega z izdelki z digitalnimi elementi, in upošteva njihov predvideni namen, vključno s kritično odvisnostjo od njih s strani bistvenih subjektov iz člena 3(1) Direktive (EU) 2022/2555.

Komisija pred sprejetjem takih delegiranih aktov izvede oceno morebitnega učinka predvidenih ukrepov na trg in se posvetuje z ustreznimi deležniki, vključno z Evropsko certifikacijsko skupino za kibernetsko varnost, vzpostavljeno z Uredbo (EU) 2019/881. Pri oceni se upoštevata pripravljenost in raven zmogljivosti držav članic za izvajanje ustrezne evropske certifikacijske sheme za kibernetsko varnost. Kadar delegirani akti iz prvega pododstavka tega odstavka niso bili sprejeti, se za izdelke z digitalnimi elementi, ki imajo osnovno funkcionalnost kategorije izdelkov iz Priloge IV, uporabljajo postopki ugotavljanja skladnosti iz člena 32(3).

Delegirani akti iz prvega pododstavka določajo minimalno prehodno obdobje šestih mesecev, razen če je zaradi nujnih razlogov upravičeno krajše prehodno obdobje.

2. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 61 za spremembo Priloge IV z vključitvijo ali umikom kategorij kritičnih izdelkov z digitalnimi elementi. Komisija pri določanju takih kategorij kritičnih izdelkov z digitalnimi elementi in zahtevane ravni zanesljivosti v skladu z odstavkom 1 tega člena upošteva merila iz člena 7(2) in obseg in zagotovi, da kategorije izdelkov z digitalnimi elementi izpolnjujejo vsaj eno od naslednjih meril:

(a) obstaja kritična odvisnost bistvenih subjektov iz člena 3 Direktive (EU) 2022/2555 od kategorije izdelkov z digitalnimi elementi;

(b) incidenti in izkoriščane šibke točke v zvezi s kategorijo izdelkov z digitalnimi elementi bi lahko povzročili resne motnje v kritičnih dobavnih verigah na notranjem trgu.

Komisija pred sprejetjem takšnih delegiranih aktov izvede oceno vrste iz odstavka 1.

Delegirani akti iz prvega pododstavka določajo minimalno prehodno obdobje šestih mesecev, razen če je zaradi nujnih razlogov upravičeno krajše prehodno obdobje.

Člen 9

Posvetovanje z deležniki

1. Komisija se pri pripravi ukrepov za izvajanje te uredbe posvetuje z ustreznimi deležniki, kot so ustrezni organi držav članic, podjetja zasebnega sektorja, vključno z mikropodjetji ter malimi in srednjimi podjetji, skupnost odprtokodne programske opreme, združenja potrošnikov, akademski krogi ter ustrezne agencije in organi Unije ter strokovne skupine, ustanovljene na ravni Unije, in jih upošteva. Komisija se zlasti strukturirano, kadar je ustrezno, posvetuje s temi deležniki in jih zaprosi za mnenje, kadar:

(a) pripravlja usmeritve iz člena 26;

(b) pripravlja tehnične opise kategorij izdelkov iz Priloge III v skladu s členom 7(4), ocenjuje potrebe po morebitnih posodobitvah seznama kategorij izdelkov v skladu s členom 7(3) in členom 8(2) ali izvaja oceno morebitnega vpliva na trg iz člena 8(1), brez poseganja v člen 61;

(c) izvaja pripravljalno delo za oceno in pregled te uredbe.

2. Komisija organizira redna posvetovanja in informativne sestanke, vsaj enkrat letno, da bi zbrala mnenja deležnikov iz odstavka 1 o izvajanju te uredbe.

Člen 10

Izboljšanje veščin v kibernetsko odpornem digitalnem okolju

Za namene te uredbe in v odziv na potrebe strokovnjakov v podporo izvajanju te uredbe države članice, kadar je ustrezno s podporo Komisije, Evropskega kompetenčnega centra za kibernetsko varnost in agencije ENISA, pri čemer v celoti upoštevajo odgovornost držav članic na področju izobraževanja, spodbujajo ukrepe in strategije, katerih cilj je:

(a) razvijati veščine na področju kibernetske varnosti ter oblikovati organizacijska in tehnološka orodja za zagotovitev zadostne razpoložljivosti usposobljenih strokovnjakov za podporo dejavnostim organov za nadzor trga in organov za ugotavljanje skladnosti;

(b) okrepiti sodelovanje med zasebnim sektorjem in gospodarskimi subjekti, tudi s preusposabljanjem ali izpopolnjevanjem delavcev proizvajalcev, potrošnikov, ustanov za usposabljanje ter javnih uprav, da bi s tem mladim zagotovili dostop do delovnih mest v sektorju kibernetske varnosti.

Člen 11

Splošna varnost izdelkov

Kadar za izdelke z digitalnimi elementi ne veljajo posebne zahteve glede varnosti, ki jih nalaga druga harmonizacijska zakonodaja Unije, kakor je opredeljena v členu 3, točka 27, Uredbe (EU) 2023/988, se z odstopanjem od člena 2(1), tretji pododstavek, točka (b), Uredbe (EU) 2023/988 poglavje III, oddelek 1, poglavji V in VII ter poglavja IX do XI navedene uredbe uporabljajo za te izdelke v zvezi z vidiki in tveganji ali kategorijami tveganj, ki niso zajeta s to uredbo.

Člen 12

Visokotvegani sistemi UI

1. Brez poseganja v zahteve v zvezi s točnostjo in robustnostjo iz člena 15 Uredbe (EU) 2024/1689 se za izdelke z digitalnimi elementi, ki spadajo na področje uporabe te uredbe in so razvrščeni kot visokotvegani sistemi UI na podlagi člena 6 navedene uredbe šteje, da so skladni z zahtevami v zvezi s kibernetsko varnostjo iz člena 15 navedene uredbe, kadar:

(a) ti izdelki izpolnjujejo bistvene zahteve glede kibernetske varnosti iz dela I Priloge I;

(b) so procesi, ki jih je vzpostavil proizvajalec, skladni z bistvenimi zahtevami glede kibernetske varnosti iz dela II Priloge I ter

(c) se uresničitev ravni kibernetske zaščite, ki se zahteva na podlagi člena 15 Uredbe (EU) 2024/1689, izkaže v EU izjavi o skladnosti, izdani na podlagi te uredbe.

2. Za izdelke z digitalnimi elementi in zahteve glede kibernetske varnosti iz odstavka 1 tega člena se uporablja ustrezni postopek ugotavljanja skladnosti, kot je določen v členu 43 Uredbe (EU) 2024/1689. Za namene tega ugotavljanja so priglašeni organi, ki so pristojni za nadzorovanje skladnosti visokotveganih sistemov UI na podlagi Uredbe (EU) 2024/1689, tudi pristojni za nadzorovanje skladnosti visokotveganih sistemov UI, ki spadajo na področje uporabe te uredbe, z zahtevami iz Priloge I k tej uredbi, če je bila skladnost teh priglašenih organov z zahtevami iz člena 39 te uredbe ocenjena v okviru postopka priglasitve na podlagi Uredbe (EU) 2024/1689.

3. Z odstopanjem od odstavka 2 tega člena se za pomembne izdelke z digitalnimi elementi iz Priloge III k tej uredbi, za katere veljajo postopki ugotavljanja skladnosti iz člena 32(2), točki (a) in (b), ter člena 32(3) te uredbe, in kritične izdelke z digitalnimi elementi iz Priloge IV k tej uredbi, za katere je treba pridobiti evropski certifikat kibernetske varnosti na podlagi člena 8(1) te uredbe ali, v odsotnosti tega, za katere je treba uporabljati postopke ugotavljanja skladnosti iz člena 32(3) te uredbe ter ki so razvrščeni kot visoko tvegani sistemi UI na podlagi člena 6 Uredbe (EU) 2024/1689, za katere se uporablja postopek ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge VI k Uredbi (EU) 2024/1689, v zvezi z bistvenimi zahtevami glede kibernetske varnosti iz te uredbe uporabljajo postopki ugotavljanja skladnosti, določeni v tej uredbi.

4. Proizvajalci izdelkov z digitalnimi elementi iz odstavka 1 tega člena lahko sodelujejo v regulativnih peskovnikih za UI iz člena 57 Uredbe (EU) 2024/1689.

POGLAVJE II

OBVEZNOSTI GOSPODARSKIH SUBJEKTOV IN DOLOČBE V ZVEZI S PROSTO IN ODPRTOKODNO PROGRAMSKO OPREMO

Člen 13

Obveznosti proizvajalcev

1. Proizvajalci pri dajanju izdelka z digitalnimi elementi na trg zagotovijo, da je bil ta izdelek zasnovan, razvit in proizveden v skladu z bistvenimi zahtevami glede kibernetske varnosti iz dela I Priloge I.

2. Za namene izpolnjevanja obveznosti iz odstavka 1 proizvajalci opravijo oceno tveganj za kibernetsko varnost, povezanih z izdelkom z digitalnimi elementi, ter upoštevajo rezultat navedene ocene v fazah načrtovanja, zasnove, razvoja, proizvodnje, dobave in vzdrževanja izdelka z digitalnimi elementi, da čim bolj zmanjšajo tveganja za kibernetsko varnost, preprečijo incidente in čim bolj zmanjšajo njihove vplive, tudi v zvezi z zdravjem in varnostjo uporabnikov.

3. Ocena tveganja za kibernetsko varnost se dokumentira in po potrebi posodablja v obdobju podpore, ki se določi v skladu z odstavkom 8 tega člena. Ta ocena tveganja za kibernetsko varnost vključuje vsaj analizo tveganj za kibernetsko varnost na podlagi predvidenega namena in razumno predvidljive uporabe ter pogojev uporabe izdelka z digitalnimi elementi, kot so operativno okolje ali sredstva, ki jih je treba zaščititi, ob upoštevanju trajanja pričakovane uporabe izdelka. V oceni tveganja za kibernetsko varnost se navede, ali in na kakšen način se varnostne zahteve iz dela I, točka 2, Priloge I, uporabljajo za zadevni izdelek z digitalnimi elementi ter kako se te zahteve izvajajo na podlagi ocene tveganja za kibernetsko varnost. Navede se tudi, kako proizvajalec uporablja del I, točka 1, Priloge I, in zahteve glede obravnavanja ranljivosti iz dela II Priloge I.

4. Proizvajalec pri dajanju izdelka z digitalnimi elementi na trg vključi oceno tveganj za kibernetsko varnost iz odstavka 3 tega člena v tehnično dokumentacijo, ki se zahteva na podlagi člena 31 in Prilogo VII. Za izdelke z digitalnimi elementi iz člena 12, za katere se uporabljajo tudi drugi pravni akti Unije, je lahko ocena tveganj za kibernetsko varnost del ocene tveganj, ki se zahteva v skladu z navedenimi pravnimi akti Unije. Kadar se določene bistvene zahteve glede kibernetske varnosti ne uporabljajo za izdelek z digitalnimi elementi, proizvajalec v navedeno tehnično dokumentacijo vključi jasno utemeljitev v zvezi s tem.

5. Za namen izpolnjevanja obveznosti iz odstavka 1 so proizvajalci pri vgradnji sestavnih delov, pridobljenih od tretjih oseb, v izdelke z digitalnimi elementi primerno skrbni, zato da taki sestavni deli ne ogrozijo kibernetske varnosti izdelka z digitalnimi elementi, niti pri vgradnji sestavnih delov proste in odprtokodne programske opreme, ki niso bili dani na trg v okviru gospodarske dejavnosti.

6. Proizvajalci po ugotovitvi ranljivosti v sestavnem delu, vključno z odprtokodnim sestavnim delom, vgrajenim v izdelek z digitalnimi elementi, sporočijo ranljivost osebi ali subjektu, ki izdeluje ali vzdržuje sestavni del, ter obravnava in odpravi ranljivost v skladu z zahtevami glede obravnavanja ranljivosti, določenimi v delu II Priloge I. Kadar so proizvajalci razvili spremembo programske ali strojne opreme za odpravo ranljivosti tega sestavnega dela, zadevno kodo ali dokumentacijo delijo z osebo ali subjektom, ki izdeluje ali vzdržuje sestavni del, kadar je primerno, v strojno berljivem formatu.

7. Proizvajalci sistematično in na način, ki je sorazmeren z naravo in tveganji za kibernetsko varnost, dokumentirajo ustrezne vidike kibernetske varnosti v zvezi z izdelki z digitalnimi elementi, vključno z ranljivostmi, s katerimi se seznanijo, in morebitnimi ustreznimi informacijami, ki jih zagotovijo tretje osebe, ter po potrebi posodobijo oceno tveganj za kibernetsko varnost za izdelke.

8. Proizvajalci pri dajanju izdelka z digitalnimi elementi na trg in v obdobju podpore zagotovijo učinkovito obravnavanje ranljivosti tega izdelka, vključno z njegovimi sestavnimi deli, v skladu z bistvenimi zahtevami glede kibernetske varnosti iz dela II Priloge I.

Proizvajalci določijo obdobje podpore, tako da odraža obdobje, v katerem se pričakuje, da se bo izdelek uporabljal, ob upoštevanju zlasti razumnih pričakovanj uporabnikov, narave izdelka, vključno z njegovim predvidenim namenom, ter ustreznega prava Unije, ki določa življenjsko dobo izdelkov z digitalnimi elementi. Proizvajalci lahko pri določanju obdobja podpore upoštevajo tudi obdobja podpore za izdelke z digitalnimi elementi, ki ponujajo podobno funkcionalnost in jih dajo na trg drugi proizvajalci, razpoložljivost delovnega okolja, obdobja podpore za integrirane sestavne dele, ki zagotavljajo osnovne funkcije in so pridobljeni od tretjih oseb, ter ustrezne usmeritve, ki jih zagotovita namenska skupina za upravno sodelovanje (v nadaljnjem besedilu: skupina ADCO), ustanovljena na podlagi člena 52(15), in Komisija. Zadeve, ki jih je treba upoštevati pri določitvi obdobja podpore, se upoštevajo na način, ki zagotavlja sorazmernost.

Brez poseganja v drugi pododstavek obdobje podpore traja najmanj pet let. Kadar se pričakuje, da se bo izdelek z digitalnimi elementi uporabljal manj kot pet let, obdobje podpore ustreza pričakovanemu času uporabe.

Komisija lahko ob upoštevanju priporočil skupine ADCO iz člena 52(16) sprejme delegirane akte v skladu s členom 61 za dopolnitev te uredbe z določitvijo najkrajšega obdobja podpore za posebne kategorije izdelkov, kadar podatki o nadzoru trga kažejo na neustrezna obdobja podpore.

Proizvajalci v tehnično dokumentacijo iz Priloge VII vključijo informacije, ki so bile upoštevane pri določitvi obdobja podpore za izdelek z digitalnimi elementi.

Proizvajalci imajo vzpostavljene ustrezne politike in postopke, vključno s politikami usklajenega razkrivanja ranljivosti iz dela II, točka 5, Priloge I, za obravnavo in odpravo morebitnih ranljivosti izdelka z digitalnimi elementi, ki jih sporočijo notranji ali zunanji viri.

9. Proizvajalci zagotovijo, da vsaka varnostna posodobitev iz dela II, točka 8, Priloge I, ki je bila dana na voljo uporabnikom v obdobju podpore, ostane na voljo po izdaji vsaj 10 let ali za preostanek obdobja podpore, pri čemer se upošteva daljše obdobje.

10. Kadar je proizvajalec dal na trg naknadno bistveno spremenjene različice programske opreme, lahko ta proizvajalec zagotovi skladnost z bistveno zahtevo glede kibernetske varnosti iz dela II, točka 2, Priloge I samo za različico, ki jo je proizvajalec nazadnje dal na trg, pod pogojem, da imajo uporabniki različic, ki so bile predhodno dane na trg, brezplačen dostop do različice, ki je bila nazadnje dana na trg, in nimajo dodatnih stroškov zaradi prilagoditve okolja strojne in programske opreme, v katerem uporabljajo prvotno različico tega izdelka.

11. Proizvajalci lahko vzdržujejo javne arhive programske opreme, ki izboljšujejo dostop uporabnikov do zgodovinskih različic. V teh primerih so uporabniki na lahko dostopen način jasno obveščeni o tveganjih, povezanih z uporabo nepodprte programske opreme.

12. Proizvajalci pred dajanjem izdelka z digitalnimi elementi na trg pripravijo tehnično dokumentacijo iz člena 31.

Proizvajalci izvedejo izbrane postopke ugotavljanja skladnosti iz člena 32 ali zagotovijo, da se taki postopki izvedejo.

Kadar se pri postopku ugotavljanja skladnosti ugotovi, da je izdelek z digitalnimi elementi skladen z bistvenimi zahtevami glede kibernetske varnosti iz dela I Priloge I, postopki, ki jih je vzpostavil proizvajalec, pa so skladni z bistvenimi zahtevami glede kibernetske varnosti iz dela II Priloge I, proizvajalci pripravijo EU izjavo o skladnosti v skladu s členom 28 in namestijo oznako CE v skladu s členom 30.

13. Proizvajalci hranijo tehnično dokumentacijo in EU izjavo o skladnosti ter organom za nadzor trga omogočijo dostop do njiju še vsaj deset let po tem, ko so izdelek z digitalnimi elementi dali na trg, ali v obdobju podpore, pri čemer se upošteva daljše obdobje.

14. Proizvajalci zagotovijo, da so za izdelke z digitalnimi elementi v serijski proizvodnji vzpostavljeni postopki za ohranjanje njihove skladnosti s to uredbo. Proizvajalci ustrezno upoštevajo spremembe postopka razvoja in proizvodnje ali spremembe zasnove ali lastnosti izdelka z digitalnimi elementi ter spremembe harmoniziranih standardov, evropskih certifikacijskih shem kibernetske varnosti ali skupnih specifikacij iz člena 27, na podlagi katerih se potrdi ali preverja skladnost izdelka z digitalnimi elementi.

15. Proizvajalci zagotovijo, da je na njihovih izdelkih z digitalnimi elementi označena številka tipa, številka serije, serijska številka ali drug identifikacijski element ali, kadar to ni mogoče, da so te informacije navedene na embalaži ali v dokumentu, priloženem izdelku z digitalnimi elementi.

16. Proizvajalci navedejo ime, registrirano trgovsko ime ali registrirano znamko proizvajalca, poštni naslov, e-poštni naslov ali druge digitalne kontaktne podatke in po potrebi spletno mesto, na katerem je mogoče stopiti v stik s proizvajalcem, na izdelku z digitalnimi elementi, njegovi embalaži ali v dokumentu, priloženem izdelku z digitalnimi elementi. Te informacije se vključijo tudi v informacije in navodila za uporabnika iz Priloge II. Kontaktni podatki so v jeziku, ki ga uporabniki in organi za nadzor trga zlahka razumejo.

17. Za namene te uredbe proizvajalci imenujejo enotno kontaktno točko, ki uporabnikom omogoča neposredno in hitro komunikacijo z njimi, tudi za lažje poročanje o ranljivostih izdelka z digitalnimi elementi.

Proizvajalci zagotovijo, da uporabniki zlahka prepoznajo enotno kontaktno točko. V informacije in navodila za uporabnika iz Priloge II vključijo tudi enotno kontaktno točko.

Enotna kontaktna točka uporabnikom omogoča izbiro želenih komunikacijskih sredstev in takih sredstev ne omejuje na avtomatizirana orodja.

18. Proizvajalci zagotovijo, da se izdelkom z digitalnimi elementi priložijo informacije in navodila za uporabnika iz Priloge II v papirnati ali elektronski obliki. Take informacije in navodila so v jeziku, ki ga uporabniki in organi za nadzor trga zlahka razumejo. Take informacije in navodila so jasni, razumljivi in berljivi. Omogočajo varno namestitev, delovanje in uporabo izdelkov z digitalnimi elementi. Proizvajalci hranijo informacije in navodila za uporabnika iz Priloge II ter organom za nadzor trga omogočijo dostop do njih še vsaj deset let po tem, ko so izdelek z digitalnimi elementi dali na trg, ali v obdobju podpore, pri čemer se upošteva daljše obdobje. Kadar se take informacije in navodila objavijo na spletu, proizvajalci zagotovijo, da so dostopni, uporabnikom prijazni in na voljo na spletu še vsaj deset let po tem, ko so izdelek z digitalnimi elementi dali na trg, ali v obdobju podpore, pri čemer se upošteva daljše obdobje.

19. Proizvajalci zagotovijo, da je končni datum obdobja podpore iz odstavka 8, ki vključuje vsaj mesec in leto, jasno in razumljivo določen ob nakupu na lahko dostopen način in po potrebi na izdelku z digitalnimi elementi, njegovi embalaži ali z digitalnimi sredstvi.

Kadar je to tehnično izvedljivo glede na naravo izdelka z digitalnimi elementi, proizvajalci uporabnikom prikažejo obvestilo, v katerem jih obvestijo, da je njihov izdelek z digitalnimi elementi dosegel konec obdobja podpore.

20. Proizvajalci izvod EU izjave o skladnosti ali poenostavljeno EU izjavo o skladnosti priložijo izdelku z digitalnimi elementi. Kadar je priložena poenostavljena EU izjava o skladnosti, ta vsebuje točen spletni naslov, na katerem je dostopna celotna EU izjava o skladnosti.

21. Po dajanju izdelka z digitalnimi elementi na trg in v obdobju podpore proizvajalci, ki ugotovijo ali upravičeno domnevajo, da izdelek z digitalnimi elementi ali postopki, ki jih je vzpostavil proizvajalec, ni v skladu z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I, nemudoma sprejmejo potrebne popravne ukrepe, da zagotovijo skladnost tega izdelka z digitalnimi elementi ali postopki, ki jih je vzpostavil proizvajalec, ali po potrebi umaknejo izdelek s trga ali ga odpokličejo.

22. Proizvajalci organu za nadzor trga na njegovo utemeljeno zahtevo predložijo vse informacije in dokumentacijo v papirni ali elektronski obliki, ki so potrebne za dokazovanje skladnosti izdelka z digitalnimi elementi in postopki, ki jih je vzpostavil proizvajalec, z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I, in sicer v jeziku, ki ga navedeni organ zlahka razume. Proizvajalci na zahtevo tega organa z njim sodelujejo pri vseh ukrepih, sprejetih za odpravo tveganj za kibernetsko varnost, prisotnih pri izdelku z digitalnimi elementi, ki so ga dali na trg.

23. Proizvajalec, ki preneha opravljati dejavnosti in zato ni skladen s to uredbo, še pred prenehanjem dejavnosti obvesti ustrezne organe za nadzor trga, kolikor je mogoče in na kakršen koli možen način pa tudi uporabnike zadevnih izdelkov z digitalnimi elementi, danih na trg, o skorajšnjem prenehanju dejavnosti.

24. Komisija lahko z izvedbenimi akti in ob upoštevanju evropskih ali mednarodnih standardov in najboljših praks določi obliko in elemente kosovnice za programsko opremo iz dela II, točka 1, Priloge I. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 62(2).

25. Za oceno odvisnosti držav članic in Unije kot celote od sestavnih delov programske opreme in zlasti od sestavnih delov, ki se štejejo za prosto in odprtokodno programsko opremo, se lahko skupina ADCO odloči za izvedbo ocene odvisnosti po vsej Uniji za posebne kategorije izdelkov z digitalnimi elementi. V ta namen lahko organi za nadzor trga od proizvajalcev takih kategorij izdelkov z digitalnimi elementi zahtevajo, da predložijo ustrezne kosovnice za programsko opremo iz dela II, točka 1, Priloge I. Organi za nadzor trga lahko na podlagi takih informacij skupine ADCO zagotovijo anonimizirane in združene informacije o odvisnostih programske opreme. Skupina ADCO skupini za sodelovanje, ustanovljeni na podlagi člena 14 Direktive (EU) 2022/2555, predloži poročilo o rezultatih ocene odvisnosti.

Člen 14

Obveznosti poročanja za proizvajalce

1. Proizvajalec o vsaki aktivno izrabljeni ranljivosti v izdelku z digitalnimi elementi, ki jo sočasno ugotovi, obvesti skupino CSIRT, ki je imenovana za koordinatorja, v skladu z odstavkom 7 tega člena, in agencijo ENISA. Proizvajalec o tej aktivno izrabljeni ranljivosti obvesti prek enotne platforme za poročanje, vzpostavljene na podlagi člena 16.

2. Za namene obvestila iz odstavka 1 proizvajalec predloži:

(a) obvestilo za zgodnje opozarjanje o aktivno izrabljeni ranljivosti brez nepotrebnega odlašanja in v vsakem primeru 24 ur po tem, ko je bil proizvajalec s tem seznanjen, in po potrebi z navedbo držav članic, na ozemlju katerih je proizvajalec seznanjen, da je bil njihov izdelek z digitalnimi elementi dan na voljo;

(b) razen v primeru, da so bile ustrezne informacije že zagotovljene, obvestilo o ranljivosti, brez nepotrebnega odlašanja in v vsakem primeru v 72 urah po tem, ko je bil proizvajalec seznanjen z aktivno izrabljeno ranljivostjo; v obvestilu so navedene splošne informacije, če so na voljo, o zadevnem izdelku z digitalnimi elementi, splošni naravi izrabljene in zadevne ranljivosti ter vseh popravnih ali blažilnih ukrepih, ki so že bili sprejeti in ki jih lahko sprejmejo uporabniki in ki navajajo, kadar je ustrezno, za kako občutljive se štejejo sporočene informacije;

(c) razen v primeru, da so bile ustrezne informacije že zagotovljene, končno poročilo, najpozneje 14 dni po tem, ko so na voljo popravni ali blažilni ukrepi, ki vključujejo vsaj naslednje:

(i) opis ranljivosti, vključno z njeno resnostjo in vplivom;

(ii) kadar so na voljo, informacije o vsakem zlonamernem akterju, ki je izrabil ali izrablja ranljivost;

(iii) podrobnosti o varnostni posodobitvi ali drugih popravnih ukrepih, ki so bili dani na voljo za odpravo ranljivosti.

3. Proizvajalec o vsakem resnem incidentu, ki vpliva na varnost izdelka z digitalnimi elementi, ki jo sočasno ugotovi, obvesti skupino CSIRT, ki je imenovana za koordinatorja, v skladu z odstavkom 7 tega člena, in agencijo ENISA. Proizvajalec o tem incidentu obvesti prek enotne platforme za poročanje, vzpostavljene na podlagi člena 16.

4. Za namene obvestila iz odstavka 3 proizvajalec predloži:

(a) zgodnje opozorilo o resnem incidentu, ki vpliva na varnost izdelka z digitalnimi elementi, brez nepotrebnega odlašanja in v vsakem primeru v 24 urah po tem, ko je bil proizvajalec seznanjen s resnim incidentom, pri čemer je iz zgodnjega opozorila razvidno vsaj, ali je bil pomemben incident domnevno povzročen z nezakonitimi ali zlonamernimi dejanji, in po potrebi navedeno, na ozemlju katerih držav članic je proizvajalec seznanjen, da je bil njihov izdelek z digitalnimi elementi dan na voljo;

(b) razen v primeru, da so bile ustrezne informacije že zagotovljene, obvestilo o incidentu, brez nepotrebnega odlašanja in v vsakem primeru v 72 urah po tem, ko je bil proizvajalec seznanjen z incidentom, v katerem so navedene splošne informacije, kadar so na voljo, o naravi incidenta, prvotni oceni incidenta, ter vseh sprejetih popravnih ali blažilnih ukrepih, in takih ukrepih, ki jih lahko sprejmejo uporabniki, in ki tudi navajajo, kadar je ustrezno, za kako občutljive šteje uporabnik sporočene informacije;

(c) razen v primeru, da so bile ustrezne informacije že zagotovljene, končno poročilo, v enem mesecu po predložitvi obvestila o incidentu iz točke (b), ki vključuje vsaj naslednje:

(i) podroben opis incidenta, vključno z njegovo resnostjo in učinkom;

(ii) vrsto grožnje ali temeljnega vzroka, ki je verjetno sprožil incident;

(iii) izvedene blažilne ukrepe in take ukrepe, ki se še izvajajo;

5. Za namene odstavka 3 se incident, ki vpliva na varnost izdelka z digitalnimi elementi, šteje za resnega, če:

(a) negativno vpliva ali bi lahko negativno vplival na zmožnost izdelka z digitalnimi elementi, da zaščiti razpoložljivost, avtentičnost, celovitost ali zaupnost občutljivih oziroma pomembnih podatkov ali funkcij, ali

(b) je privedel ali je zmožen privesti do uvedbe ali izvedbe zlonamerne kode v izdelku z digitalnimi elementi ali v mreži in informacijskih sistemih uporabnika izdelka z digitalnimi elementi.

6. Skupina CSIRT, ki je imenovana za koordinatorja, ki je prvotno prejela obvestilo, lahko po potrebi od proizvajalcev zahteva, da predložijo vmesno poročilo o ustreznih posodobitvah stanja o aktivno izrabljeni ranljivosti ali resnem incidentu, ki vpliva na varnost izdelka z digitalnimi elementi.

7. Obvestila iz odstavkov 1 in 3 tega člena se predložijo prek enotne platforme za poročanje iz člena 16 z uporabo ene od končnih točk za elektronsko obveščanje iz člena 16(1). Obvestilo se predloži prek elektronske končne točke za obveščanje skupine CSIRT, imenovane za koordinatorja države članice, v kateri imajo proizvajalci glavni sedež v Uniji, in je hkrati dostopna agenciji ENISA.

Za namene te uredbe se šteje, da ima proizvajalec svoj glavni sedež v Uniji, v državi članici, v kateri se večinoma sprejemajo odločitve, povezane s kibernetsko varnostjo njenih izdelkov z digitalnimi elementi. Če take države članice ni mogoče določiti, se šteje, da je glavni sedež v državi članici, v kateri ima zadevni proizvajalec sedež z največjim številom zaposlenih v Uniji.

Kadar proizvajalec nima glavnega sedeža v Uniji, obvestila iz odstavkov 1 in 3 predloži z uporabo končne točke za elektronsko obveščanje skupine CSIRT, ki je imenovana za koordinatorja v državi članici, določene na podlagi naslednjega vrstnega reda in na podlagi informacij, ki so na voljo proizvajalcu:

(a) država članica, v kateri ima sedež pooblaščeni zastopnik, ki deluje v imenu proizvajalca za največje število izdelkov z digitalnimi elementi tega proizvajalca;

(b) država članica, v kateri ima sedež uvoznik, ki daje na trg največje število izdelkov z digitalnimi elementi tega proizvajalca;

(c) država članica, v kateri ima sedež distributer, ki daje na trg največje število izdelkov z digitalnimi elementi tega proizvajalca;

(d) država članica, v kateri ima sedež največje število uporabnikov izdelkov z digitalnimi elementi tega proizvajalca.

V zvezi s tretjim pododstavkom, točka (d), proizvajalec lahko predloži obvestila v zvezi s katero koli naslednjo izrabljeno ranljivostjo ali resnim incidentom, ki vpliva na varnost izdelka z digitalnimi elementi, isti skupini CSIRT, ki je imenovana za koordinatorja, ki ji je prvič poročal.

8. Po seznanitvi z aktivno izrabljeno ranljivostjo ali resnim incidentom, ki vpliva na varnost izdelka z digitalnimi elementi, proizvajalec obvesti prizadete uporabnike izdelka z digitalnimi elementi in, kadar je ustrezno, vse uporabnike o tej ranljivosti ali incidentu, ki vpliva na varnost izdelka z digitalnimi elementi, in po potrebi o zmanjšanju tveganja ter vseh popravnih ukrepih, ki jih lahko uporabnik sprejme za zmanjšanje vpliva te ranljivosti ali incidenta, kadar je ustrezno, v strukturiranem in strojno berljivem formatu, ki se zlahka avtomatsko obdeluje. Kadar proizvajalec uporabnikov izdelka z digitalnimi elementi ne obvesti pravočasno, lahko obveščene skupine CSIRT, ki so imenovane za koordinatorje, uporabnikom posredujejo take informacije, kadar menijo, da so sorazmerne in potrebne za preprečevanje ali ublažitev učinka te ranljivosti ali incidenta.

9. Komisija do 11. decembra 2025 sprejme delegirane akte v skladu s členom 61 te uredbe za dopolnitev te uredbe in določi pogoje za uporabo razlogov, povezanih s kibernetsko varnostjo, v zvezi z odložitvijo posredovanja obvestil, kakor je določeno v členu 16(2) te uredbe. Komisija pri pripravi osnutkov delegiranih aktov sodeluje z mrežo skupin CSIRT, kakor je vzpostavljena na podlagi člena 15 Direktive (EU) 2022/2555 in agencijo ENISA.

10. Komisija lahko z izvedbenimi akti podrobneje določi obliko in postopke za obvestila iz tega člena ter členov 15 in 16. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 62(2). Komisija pri pripravi osnutkov izvedbenih aktov sodeluje z mrežo skupin CSIRT in agencijo ENISA.

Člen 15

Prostovoljno poročanje

1. Proizvajalci ter druge fizične ali pravne osebe lahko prostovoljno sporočijo vsako ranljivost, vsebovano v izdelku z digitalnimi elementi, ter kibernetske grožnje, ki bi lahko vplivale na profil tveganja izdelka z digitalnimi elementi skupini CSIRT, ki je imenovana za koordinatorja, ali agenciji ENISA.

2. Proizvajalci ter druge fizične in pravne osebe bi morali imeti možnost, da skupini CSIRT, ki je imenovana za koordinatorja, ali agenciji ENISA prostovoljno sporočijo vsak incident, ki vpliva na varnost izdelka z digitalnimi elementi, pa tudi skorajšnje incidente, ki bi lahko povzročili tak incident.

3. Skupina CSIRT, ki je imenovana za koordinatorja, ali agencija ENISA obravnava obvestila iz odstavkov 1 in 2 tega člena v skladu s postopkom iz člena 16.

Skupina CSIRT, ki je imenovana za koordinatorja, da lahko prednost obravnavi obveznih obvestil pred prostovoljnimi.

4. Kadar fizična ali pravna oseba, ki ni proizvajalec, sporoči aktivno izrabljeno ranljivost ali resen incident, ki vpliva na varnost izdelka z digitalnimi elementi, v skladu z odstavkom 1 ali 2, skupina CSIRT, ki je imenovana za koordinatorja, o tem brez nepotrebnega odlašanja obvesti proizvajalca.

5. Skupine CSIRT, ki so imenovane za koordinatorje, ter agencija ENISA zagotovijo zaupnost in ustrezno zaščito informacij, ki jih predloži fizična ali pravna oseba. Za fizično ali pravno osebo, ki prostovoljno predloži obvestilo, ne veljajo nikakršne dodatne obveznosti, ki zanjo ne bi veljale, če obvestila ne bi predložila, pri čemer se ne posega v preprečevanje, preiskovanje, odkrivanje in pregon kaznivih dejanj.

Člen 16

Vzpostavitev enotne platforme za poročanje

1. Za namene obvestil iz člena 14(1) in (3) ter člena 15(1) in (2) in za poenostavitev obveznosti poročanja za proizvajalce agencija ENISA vzpostavi enotno platformo za poročanje. Vsakodnevno delovanje enotne platforme za poročanje upravlja in vzdržuje agencija ENISA. Struktura enotne platforme za poročanje omogoča državam članicam in agenciji ENISA, da vzpostavijo svoje lastne končne točke za elektronsko obveščanje.

2. Po prejemu obvestila skupina CSIRT, ki je imenovana za koordinatorja, ki je prvotno prejela obvestilo, to obvestilo prek enotne platforme za poročanje brez odlašanja posreduje skupinam CSIRT, ki so imenovane za koordinatorje na ozemlju, za katerega je proizvajalec navedel, da je izdelek z digitalnimi elementi bil dan na voljo.

V izjemnih okoliščinah in zlasti na zahtevo proizvajalca ter ob upoštevanju stopnje občutljivosti sporočenih informacij, kot jih je navedel proizvajalec na podlagi člena 14(2), točka (a), te uredbe, se posredovanje obvestila na podlagi utemeljenih razlogov v zvezi s kibernetsko varnostjo lahko odloži za obdobje, ki je nujno potrebno, tudi, kadar je ranljivost vključena v postopek usklajenega razkrivanja ranljivosti, kot je navedeno v členu 12(1) Direktive (EU) 2022/2555. Kadar se skupina CSIRT odloči zadržati obvestilo, o odločitvi nemudoma obvesti agencijo ENISA in predloži utemeljitev za zadržanje obvestila ter navede, kdaj bo posredovala obvestilo v skladu s postopkom posredovanja iz tega odstavka. Agencija ENISA lahko skupino CSIRT podpre v zvezi z razlogi glede kibernetske varnosti, ki jih ta uporabi za odložitev posredovanja obvestila.

V izjemnih okoliščinah, kadar proizvajalec v obvestilu iz člena 14(2), točka (b), navede:

(a) da je sporočeno ranljivost aktivno izrabljal zlonamerni akter in da je bila glede na razpoložljive informacije izrabljena samo v državi članici skupine CSIRT, ki je imenovana za koordinatorja, ki ji je proizvajalec sporočil ranljivost, in v nobeni drugi državi članici;

(b) da bi vsako takojšnje nadaljnje razširjanje sporočene ranljivosti verjetno imelo za posledico posredovanje informacij, katerih razkritje bi bilo v nasprotju z bistvenimi interesi te države članice, ali

(c) da sporočena ranljivost predstavlja neposredno visoko tveganje za kibernetsko varnost, ki izhaja iz nadaljnjega posredovanja;

samo informacije, da je proizvajalec predložil obvestilo, splošne informacije o izdelku, informacije o splošni naravi izrabljene ranljivosti in informacije, da se proizvajalec sklicuje na varnostne razloge, se sočasno predložijo agenciji ENISA, dokler se celotno obvestilo ne posreduje zadevnim skupinam CSIRT in agenciji ENISA. Kadar agencija ENISA na podlagi informacij meni, da obstaja sistemsko tveganje, ki vpliva na varnost notranjega trga, skupini CSIRT, ki je obvestilo prejela, priporoči, naj celotno obvestilo posreduje drugim skupinam CSIRT, ki so imenovane za koordinatorje, in agenciji ENISA.

3. Potem ko so prejele obvestilo o aktivno izrabljeni ranljivosti izdelka z digitalnimi elementi ali resnem incidentu, ki vpliva na varnost izdelka z digitalnimi elementi, skupine CSIRT, ki so imenovane za koordinatorje, posredujejo organom za nadzor trga svojih držav članic sporočene informacije, ki jih ti potrebujejo za izpolnjevanje svojih obveznosti na podlagi te uredbe.

4. Agencija ENISA sprejme ustrezne in sorazmerne tehnične, operativne in organizacijske ukrepe za obvladovanje tveganj za varnost enotne platforme za poročanje in informacij, ki se predložijo ali posredujejo prek enotne platforme za poročanje. O vsakem varnostnem incidentu, ki je prizadel enotno platformo za poročanje, brez nepotrebnega odlašanja obvesti mrežo skupin CSIRT ter Komisijo.

5. Agencija ENISA v sodelovanju z mrežo skupin CSIRT zagotovi in izvaja specifikacije o tehničnih, operativnih in organizacijskih ukrepih v zvezi z vzpostavitvijo, vzdrževanjem in varnim delovanjem enotne platforme za poročanje iz odstavka 1, ki vključujejo vsaj varnostne ureditve, povezane z vzpostavitvijo, delovanjem in vzdrževanjem enotne platforme za poročanje, ter končne točke za elektronsko obveščanje, ki so jih vzpostavile skupine CSIRT, imenovane za koordinatorje na nacionalni ravni, in agencija ENISA na ravni Unije, vključno s postopkovnimi vidiki, s katerimi se zagotovi, da sporočena ranljivost nima na voljo korektivnih ali blažilnih ukrepov, da se informacije o tej ranljivosti izmenjujejo v skladu s strogimi varnostnimi protokoli in na podlagi potrebe po seznanitvi.

6. Kadar je bila skupina CSIRT, ki je imenovana za koordinatorja, obveščena o aktivno izrabljeni ranljivosti kot del postopka usklajenega razkrivanja ranljivosti iz člena 12(1) Direktive (EU) 2022/2555, skupina CSIRT, ki je imenovana za koordinatorja, ki je prvotno prejela obvestilo, lahko odloži posredovanje zadevnega obvestila preko enotne platforme za poročanje na podlagi utemeljenih razlogov v zvezi s kibernetsko varnostjo za obdobje, ki ni daljše od nujno potrebnega, in dokler strani, vpletene v politiko usklajenega razkrivanja ranljivosti, ne podajo soglasja za razkritje. Ta zahteva proizvajalcem ne preprečuje, da prostovoljno sporočijo tako ranljivost v skladu s postopkom iz tega člena.

Člen 17

Druge določbe v zvezi s poročanjem

1. Agencija ENISA lahko informacije, sporočene na podlagi člena 14(1) in (3) ter člena 15(1) in (2) te uredbe, predloži evropski organizacijski mreži za povezovanje v kibernetski krizi (EU-CyCLONe), ustanovljeni s členom 16 Direktive (EU) 2022/2555, če so take informacije pomembne za usklajeno upravljanje velikih kibernetskih incidentov in kriz na operativni ravni. Za namene določitve take pomembnosti lahko agencija ENISA upošteva tehnične analize, ki jih izvede mreža skupin CSIRT, kadar so na voljo.

2. Kadar je ozaveščenost javnosti potrebna za preprečitev ali ublažitev resnega incidenta, ki bi lahko vplival na varnost izdelka z digitalnimi elementi, ali za obravnavo incidenta, ki je v teku, ali kadar je razkritje incidenta kako drugače v javnem interesu, lahko skupina CSIRT, ki je imenovana za koordinatorja zadevne države članice, po posvetovanju z zadevnim proizvajalcem in, kadar je primerno, v sodelovanju z agencijo ENISA obvesti javnost o incidentu ali zahteva, da to stori proizvajalec.

3. Agencija ENISA na podlagi obvestil, ki jih prejme na podlagi člena 14(1) in (3) ter člena 15(1) in (2) te uredbe, vsakih 24 mesecev pripravi tehnično poročilo o novih trendih glede tveganj za kibernetsko varnost pri izdelkih z digitalnimi elementi ter ga predloži skupini za sodelovanje, ustanovljeni na podlagi člena 14 Direktive (EU) 2022/2555. Prvo tako poročilo predloži v 24 mesecih po začetku uporabe obveznosti iz člena 14(1) in (3). Agencija ENISA vključi ustrezne informacije iz svojih tehničnih poročil v poročilo o stanju kibernetske varnosti v Uniji na podlagi člena 18 Direktive (EU) 2022/2555.

4. Samo dejanje obveščanja v skladu s členom 14(1) in (3) ali členom 15(1) in (2) priglasitveni fizični ali pravni osebi ne naloži dodatne odgovornosti.

5. Potem ko je na voljo varnostna posodobitev ali druga oblika popravnega ali blažilnega ukrepa, agencija ENISA v dogovoru s proizvajalcem zadevnega izdelka z digitalnimi elementi doda javno znano ranljivost, priglašeno na podlagi člena 14(1) ali člena 15(1) te uredbe, v evropsko podatkovno zbirko ranljivosti, vzpostavljeno na podlagi člena 12(2) Direktive (EU) 2022/2555.

6. Skupine CSIRT, ki so imenovane za koordinatorje, prek službe za pomoč uporabnikom v zvezi z obveznostmi poročanja na podlagi člena 14 nudijo podporo proizvajalcem, zlasti tistim, ki se štejejo za mikropodjetja ali mala ali srednja podjetja.

Člen 18

Pooblaščeni zastopniki

1. Proizvajalec lahko s pisnim pooblastilom imenuje pooblaščenega zastopnika.

2. Obveznosti iz člena 13(1) do (11) in člena 13(12), prvi pododstavek, in člena 13(14) niso del pooblastila pooblaščenega zastopnika.

3. Pooblaščeni zastopnik izvaja naloge, določene v pooblastilu, ki ga prejme od proizvajalca. Pooblaščeni zastopnik organom za nadzor trga na zahtevo predloži kopijo pooblastila. Pooblastilo pooblaščenemu zastopniku omogoča, da izvaja vsaj naslednje naloge:

(a) hrani EU izjavo o skladnosti iz člena 28 in tehnično dokumentacijo iz člena 31 ter organom za nadzor trga omogoči dostop do njiju vsaj še deset let po tem, ko je bil izdelek z digitalnimi elementi dan na trg ali v obdobju podpore, pri čemer se upošteva daljše obdobje;

(b) organu za nadzor trga na podlagi njegove utemeljene zahteve zagotovi vse informacije in dokumentacijo, potrebne za dokazovanje skladnosti izdelka z digitalnimi elementi;

(c) na zahtevo organov za nadzor trga z njimi sodeluje pri vseh ukrepih, sprejetih za odpravo tveganj, ki jih predstavlja izdelek z digitalnimi elementi, v okviru pooblastila pooblaščenega zastopnika.

Člen 19

Obveznosti uvoznikov

1. Uvozniki dajo na trg samo izdelke z digitalnimi elementi, ki so skladni z bistvenimi zahtevami glede kibernetske varnosti iz dela I Priloge I in kadar so postopki, ki jih je vzpostavil proizvajalec, skladni z bistvenimi zahtevami glede kibernetske varnosti iz dela II Priloge I.

2. Preden uvozniki dajo izdelek z digitalnimi elementi na trg, zagotovijo, da:

(a) je proizvajalec izvedel ustrezne postopke ugotavljanja skladnosti iz člena 32;

(b) je proizvajalec pripravil tehnično dokumentacijo;

(c) je izdelek z digitalnimi elementi opremljen z oznako CE iz člena 30 ter so mu priloženi EU izjava o skladnosti iz člena 13(20) ter informacije in navodila uporabniku iz Priloge II v jeziku, ki ga uporabniki in organi za nadzor trga zlahka razumejo;

(d) Proizvajalec izpolnjuje zahteve iz člena 13(15), (16) in (19).

Za namene tega odstavka lahko uvozniki predložijo potrebne dokumente, ki dokazujejo, da so zahteve iz tega člena izpolnjene.

3. Kadar uvoznik meni ali upravičeno domneva, da izdelek z digitalnimi elementi ali postopki, ki jih je vzpostavil proizvajalec, niso skladni s to uredbo, izdelka ne da na trg, dokler se ne zagotovi skladnost tega izdelka ali postopkov, ki jih je vzpostavil proizvajalec, s to uredbo. Kadar izdelek z digitalnimi elementi predstavlja povečano tveganje za kibernetsko varnost, uvoznik o tem obvesti proizvajalca in organe za nadzor trga.

Kadar uvoznik utemeljeno domneva, da bi izdelek z digitalnimi elementi lahko pomenil znatno tveganje za kibernetsko varnost zaradi netehničnih dejavnikov tveganja, o tem obvesti organe za nadzor trga. Organi za nadzor trga po prejemu takih informacij upoštevajo postopke iz člena 54(2).

4. Uvozniki navedejo svoje ime, registrirano trgovsko ime ali registrirano znamko, poštni naslov, e-poštni naslov ali drugi digitalni kontakt in po potrebi spletno mesto, na katerem so dosegljivi, na izdelku z digitalnimi elementi ali pa na embalaži izdelka ali v dokumentu, priloženem izdelku z digitalnimi elementi. Kontaktni podatki so v jeziku, ki ga uporabniki in organi za nadzor trga zlahka razumejo.

5. Uvozniki, ki ugotovijo ali upravičeno domnevajo, da izdelek z digitalnimi elementi, ki so ga dali na trg, ni skladen s to uredbo, nemudoma sprejmejo potrebne popravne ukrepe, da zagotovijo skladnost tega izdelka z digitalnimi elementi s to uredbo ali po potrebi umaknejo izdelek s trga ali ga odpokličejo.

Uvozniki po tem, ko se seznanijo z ranljivostjo pri izdelku z digitalnimi elementi, o njej brez nepotrebnega odlašanja obvestijo proizvajalca. Kadar izdelek z digitalnimi elementi predstavlja povečano tveganje za kibernetsko varnost, uvozniki o tem nemudoma obvestijo organe za nadzor trga držav članic, v katerih je izdelek z digitalnimi elementi dostopen na trgu, pri čemer navedejo zlasti podrobnosti o neskladnosti in morebitnih sprejetih popravnih ukrepih.

6. Uvozniki vsaj še deset let po tem, ko je bil izdelek z digitalnimi elementi dan na trg ali v obdobju podpore, pri čemer se upošteva daljše obdobje, hranijo kopijo EU izjave o skladnosti in organom za nadzor trga omogočijo dostop do nje ter zagotovijo, da je tehnična dokumentacija na zahtevo na voljo tem organom.

7. Uvozniki organu za nadzor trga na njegovo utemeljeno zahtevo predložijo vse informacije in dokumentacijo v papirni ali elektronski obliki, ki so potrebne za dokazovanje skladnosti izdelka z digitalnimi elementi z bistvenimi zahtevami glede kibernetske varnosti iz dela I Priloge I ter skladnosti postopkov, ki jih je vzpostavil proizvajalec, z bistvenimi zahtevami glede kibernetske varnosti iz dela II Priloge I, in to v jeziku, ki ga ta organ zlahka razume. Na

zahtevo tega organa z njim sodelujejo pri vseh ukrepih, sprejetih za odpravo tveganj za kibernetsko varnost, prisotnih pri izdelku z digitalnimi elementi, ki so ga dali na trg.

8. Kadar se uvoznik izdelka z digitalnimi elementi seznani s tem, da je proizvajalec navedenega izdelka prenehal opravljati dejavnosti, in zato ne more izpolniti obveznosti iz te uredbe, o tem obvesti ustrezne organe za nadzor trga, na kakršen koli možen način in kolikor je mogoče pa tudi uporabnike izdelkov z digitalnimi elementi, danimi na trg.

Člen 20

Obveznosti distributerjev

1. Distributerji pri omogočanju dostopnosti izdelka z digitalnimi elementi na trgu skrbno upoštevajo zahteve iz te uredbe.

2. Preden distributerji omogočijo dostopnost izdelka z digitalnimi elementi na trgu, preverijo, ali:

(a) je izdelek z digitalnimi elementi opremljen z oznako CE;

(b) sta proizvajalec in uvoznik izpolnila obveznosti iz člena 13(15), (16), (18), (19) in (20) in člena 19(4) ter distributerju zagotovila vso potrebno dokumentacijo.

3. Kadar distributer na podlagi informacij, ki jih ima na voljo, meni ali upravičeno domneva, da izdelek z digitalnimi elementi ali postopki, ki jih je vzpostavil proizvajalec, niso skladni z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I, ne omogoči dostopnosti izdelka z digitalnimi elementi na trgu, dokler se ne zagotovi skladnost navedenega izdelka ali postopkov, ki jih je vzpostavil proizvajalec, s to uredbo. Kadar izdelek z digitalnimi elementi predstavlja povečano tveganje za kibernetsko varnost, distributer o tem brez nepotrebnega odlašanja obvesti proizvajalca in organe za nadzor trga.

4. Distributerji, ki na podlagi informacij, ki jih imajo na voljo, ugotovijo ali upravičeno domnevajo, da izdelek z digitalnimi elementi, za katerega so omogočili dostopnost na trgu, ali postopki, ki jih je vzpostavil proizvajalec, niso skladni s to uredbo, zagotovijo sprejetje popravnih ukrepov, potrebnih za zagotovitev skladnosti navedenega izdelka z digitalnimi elementi ali postopkov, ki jih je vzpostavil proizvajalec, ali po potrebi za umik izdelka s trga ali njegov odpoklic.

Distributerji po tem, ko se seznanijo z ranljivostjo pri izdelku z digitalnimi elementi, o njej brez nepotrebnega odlašanja obvestijo proizvajalca. Kadar izdelek z digitalnimi elementi predstavlja povečano tveganje za kibernetsko varnost, distributerji o tem nemudoma obvestijo organe za nadzor trga držav članic, v katerih so omogočili dostopnost izdelka z digitalnimi elementi na trgu, pri čemer navedejo zlasti podrobnosti o neskladnosti in morebitnih sprejetih popravnih ukrepih.

5. Distributerji organu za nadzor trga na njegovo utemeljeno zahtevo predložijo vse informacije in dokumentacijo v papirni ali elektronski obliki, ki so potrebne za dokazovanje skladnosti izdelka z digitalnimi elementi in postopkov, ki jih je vzpostavil proizvajalec s to uredbo in to v jeziku, ki ga navedeni organ zlahka razume. Na zahtevo tega organa z njim sodelujejo pri vseh ukrepih, sprejetih za odpravo tveganj za kibernetsko varnost, prisotnih pri izdelku z digitalnimi elementi, za katerega so omogočili dostopnost na trgu.

6. Ko se distributer izdelka z digitalnimi elementi na podlagi informacij, ki jih ima na voljo, seznani s tem, da je proizvajalec tega izdelka prenehal opravljati dejavnosti, in zato ne more izpolniti obveznosti iz te uredbe, o tem brez nepotrebnega odlašanja obvesti ustrezne organe za nadzor trga, na kakršen koli možen način in kolikor je mogoče pa tudi uporabnike izdelkov z digitalnimi elementi, danimi na trg.

Člen 21

Primeri, v katerih se obveznosti izdelovalcev uporabljajo za uvoznike in distributerje

Uvoznik ali distributer se šteje za proizvajalca za namene te uredbe in zanj veljata člena 13 in 14, kadar ta uvoznik ali distributer da izdelek z digitalnimi elementi na trg pod svojim imenom ali znamko ali bistveno spremeni izdelek z digitalnimi elementi, ki je že bil dan na trg.

Člen 22

Drugi primeri, v katerih se uporabljajo obveznosti izdelovalcev

1. Fizična ali pravna oseba, ki ni proizvajalec, uvoznik ali distributer in ki bistveno spremeni izdelek z digitalnimi elementi ter omogoči dostopnost tega izdelka na trgu, se šteje za proizvajalca za namene te uredbe.

2. Za osebo iz odstavka 1 tega člena veljajo obveznosti iz člena 13 in 14 za del izdelka z digitalnimi elementi, na katerega vpliva bistvena sprememba, ali za celotni izdelek, če bistvena sprememba vpliva na kibernetsko varnost izdelka z digitalnimi elementi kot celoto.

Člen 23

Identifikacija gospodarskih subjektov

1. Gospodarski subjekti organom za nadzor trga na zahtevo predložijo naslednje informacije:

(a) ime in naslov vsakega gospodarskega subjekta, ki jim je dobavil izdelek z digitalnimi elementi;

(b) ime in naslov vsakega gospodarskega subjekta, ki so mu dobavili izdelek z digitalnimi elementi, kadar sta na voljo.

2. Gospodarski subjekti lahko predložijo informacije iz odstavka 1 še deset let po tem, ko jim je bil dobavljen izdelek z digitalnimi elementi, oziroma deset let po tem, ko so dobavili izdelek z digitalnimi elementi.

Člen 24

Obveznosti upravljavcev odprtokodne programske opreme

1. Upravljavci odprtokodne programske opreme vzpostavijo in na preverljiv način dokumentirajo politiko kibernetske varnosti, da bi pospešili razvoj varnega izdelka z digitalnimi elementi in spodbujali učinkovito obravnavanje ranljivosti s strani razvijalcev tega izdelka. Ta politika spodbuja tudi prostovoljno poročanje razvijalcev tega izdelka o ranljivostih, kakor je določeno v členu 15, in upošteva posebno naravo upravljavca odprtokodne programske opreme ter pravne in organizacijske ureditve, ki veljajo zanj. Zajema zlasti vidike, povezane z dokumentiranjem, obravnavanjem in odpravljanjem ranljivosti, ter spodbuja izmenjavo informacij o ranljivostih, odkritih znotraj odprtokodne skupnosti.

2. Upravljavci odprtokodne programske opreme na zahtevo organov za nadzor trga sodelujejo z njimi, da bi zmanjšali tveganja za kibernetsko varnost, ki jih predstavlja izdelek z digitalnimi elementi, ki se šteje za prosto in odprtokodno programsko opremo.

Na podlagi utemeljene zahteve organa za nadzor trga mu upravljavci odprtokodne programske opreme v jeziku, ki ga ta organ zlahka razume, zagotovijo dokumentacijo iz odstavka 1 v papirni ali elektronski obliki.

3. Obveznosti iz člena 14(1) se uporabljajo za upravljavce odprtokodne programske opreme, če sodelujejo pri razvoju izdelkov z digitalnimi elementi. Obveznosti iz člena 14(3) in (8) se uporabljajo za upravljavce odprtokodne programske opreme, če resni incidenti, ki ogrozijo varnost izdelkov z digitalnimi elementi, vplivajo na omrežja in informacijske sisteme, ki jih za razvoj takih izdelkov zagotavljajo upravljavci odprtokodne programske opreme.

Člen 25

Potrdilo o varnosti proste in odprtokodne programske opreme

Da bi olajšali izpolnjevanje obveznosti potrebne skrbnosti iz člena 13(5), zlasti v zvezi s proizvajalci, ki v svoje izdelke vključujejo sestavne dele proste in odprtokodne programske opreme z digitalnimi elementi, se na Komisijo prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 61 za dopolnitev te uredbe z vzpostavitvijo prostovoljnih programov varnostnih potrdil, ki razvijalcem ali uporabnikom izdelkov z digitalnimi elementi, ki se štejejo za prosto in odprtokodno programsko opremo, ter drugim tretjim osebam omogočajo, da ocenijo skladnost takih izdelkov z vsemi ali nekaterimi bistvenimi zahtevami glede kibernetske varnosti ali drugimi obveznostmi iz te uredbe.

Člen 26

Usmeritve

1. Da bi olajšali izvajanje in zagotovili doslednost takega izvajanja, Komisija objavi usmeritve za pomoč gospodarskim subjektom pri uporabi te uredbe s posebnim poudarkom na lajšanju zagotavljanja skladnosti mikropodjetij ter malih in srednjih podjetij.

2. Kadar Komisija namerava zagotoviti usmeritve iz odstavka 1, obravnava vsaj naslednje vidike:

(a) področje uporabe te uredbe s posebnim poudarkom na rešitvah za obdelavo podatkov na daljavo ter prosti in odprtokodni programski opremi;

(b) uporabo obdobij podpore v zvezi s posebnimi kategorijami izdelkov z digitalnimi elementi;

(c) usmeritve, namenjene proizvajalcem, za katere veljata ta uredba in harmonizacijska zakonodaja Unije, ki ni ta uredba ali drugi povezani pravni akti Unije;

(d) pojem bistvene spremembe.

Komisija vodi tudi lahko dostopen seznam delegiranih in izvedbenih aktov, sprejetih na podlagi te uredbe.

3. Komisija se pri pripravi usmeritev na podlagi tega člena posvetuje z zadevnimi deležniki.

POGLAVJE III

SKLADNOST IZDELKA Z DIGITALNIMI ELEMENTI

Člen 27

Domneva o skladnosti

1. Za izdelke z digitalnimi elementi in postopke, ki jih je vzpostavil proizvajalec in ki so v skladu s harmoniziranimi standardi ali njihovimi deli, katerih sklici so bili objavljeni v *Uradnem listu Evropske unije*, se domneva, da so skladni z bistvenimi zahtevami glede kibernetske varnosti, določenimi v Prilogi I, iz teh standardov ali njihovih delov.

Komisija v skladu s členom 10(1) Uredbe (EU) št. 1025/2012 od ene ali več evropskih organizacij za standardizacijo zahteva pripravo harmoniziranih standardov za bistvene zahteve glede kibernetske varnosti iz Priloge I k tej uredbi. Pri pripravi zahtev za standardizacijo za to uredbo si Komisija prizadeva upoštevati obstoječe evropske in mednarodne standarde za kibernetsko varnost, ki se že izvajajo ali so v pripravi, da bi poenostavila pripravo harmoniziranih standardov v skladu z Uredbo (EU) št. 1025/2012.

2. Komisija lahko sprejme izvedbene akte, s katerimi določi skupne specifikacije, ki zajemajo tehnične zahteve, s katerimi se zagotavlja način za izpolnjevanje bistvenih zahtev glede kibernetske varnosti iz Priloge I za izdelke z digitalnimi elementi, ki spadajo na področje uporabe te uredbe.

Ti izvedbeni akti se sprejmejo le, kadar so izpolnjeni naslednji pogoji:

(a) Komisija je na podlagi člena 10(1) Uredbe (EU) št. 1025/2012 od ene ali več evropskih organizacij za standardizacijo zahtevala pripravo harmoniziranih standardov za bistvene zahteve glede kibernetske varnosti iz Priloge I in:

(i) zahteva ni bila sprejeta;

(ii) harmonizirani standardi, ki so bili predmet te zahteve, niso bili predloženi v roku, določenem v skladu s členom 10 (1) Uredbe (EU) št. 1025/2012, ali

(iii) harmonizirani standardi niso skladni z zahtevo ter

(b) v *Uradnem listu Evropske unije* v skladu z Uredbo (EU) št. 1025/2012 ni objavljen sklic na harmonizirane standarde, ki zajemajo ustrezne bistvene zahteve glede kibernetske varnosti iz Priloge I k tej uredbi, in njegova objava se v razumnem roku tudi ne pričakuje.

Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 62(2).

3. Komisija pred pripravo osnutka izvedbenega akta iz odstavka 2 tega člena obvesti odbor iz člena 22 Uredbe (EU) št. 1025/2012, da meni, da so pogoji iz odstavka 2 tega člena izpolnjeni.

4. Komisija pri pripravi osnutka izvedbenega akta iz odstavka 2 upošteva mnenja zadevnih organov in se ustrezno posvetuje z vsemi zadevnimi deležniki.

5. Za izdelke z digitalnimi elementi in postopke, ki jih je vzpostavil proizvajalec in ki so v skladu s skupnimi specifikacijami, določenimi z izvedbenimi akti iz odstavka 2 tega člena ali njihovimi deli, se domneva, da so skladni z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I, zajetimi v navedenih skupnih specifikacijah ali delih teh specifikacij.

6. Kadar harmoniziran standard sprejme evropska organizacija za standardizacijo in se predlaga Komisiji z namenom objave sklica nanj v *Uradnem listu Evropske unije*, Komisija oceni harmonizirani standard v skladu z Uredbo (EU) št. 1025/2012. Ko se sklic na harmonizirani standard objavi v *Uradnem listu Evropske unije*, Komisija razveljavi izvedbene akte iz odstavka 2 tega člena ali njihove dele, ki zajemajo enake bistvene zahteve glede kibernetske varnosti kot tiste v harmoniziranem standardu.

7. Kadar država članica meni, da skupna specifikacija ne izpolnjuje v celoti bistvenih zahtev glede kibernetske varnosti iz Priloge I, o tem s predložitvijo podrobne obrazložitve obvesti Komisijo. Komisija te podrobne obrazložitve oceni in po potrebi lahko spremeni izvedbeni akt, ki določa zadevno skupno specifikacijo.

8. Za izdelke z digitalnimi elementi in postopke, ki jih je vzpostavil proizvajalec, za katere sta bila EU izjava o skladnosti ali certifikat izdana na podlagi evropske certifikacijske sheme kibernetske varnosti, sprejete na podlagi Uredbe (EU) 2019/881, se domneva, da so skladni z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I, kolikor se EU izjava o skladnosti ali evropski certifikat kibernetske varnosti ali njuni deli nanašajo na navedene zahteve.

9. Na Komisijo se prenese pooblastilo, da sprejme delegirane akte v skladu s členom 61 te uredbe, tako da določi evropske certifikacijske sheme kibernetske varnosti, sprejete na podlagi Uredbe (EU) 2019/881, ki jih je mogoče uporabiti za dokazovanje skladnosti izdelkov z digitalnimi elementi z bistvenimi zahtevami glede kibernetske varnosti ali njihovimi deli, kot je določeno v Prilogi I k tej uredbi. Nadalje izdaja evropskega certifikata kibernetske varnosti na podlagi takih shem, na ravni zanesljivosti vsaj „znatno“, oprosti proizvajalca obveznosti zagotoviti ugotavljanje skladnosti z ustreznimi zahtevami, ki ga opravi tretja oseba, kakor je določeno v členu 32(2), točki (a) in (b), ter členu 32(3), točki (a) in (b), te uredbe.

Člen 28

EU izjava o skladnosti

1. Proizvajalci pripravijo EU izjavo o skladnosti v skladu s členom 13(12) in navedejo, da je bilo dokazano izpolnjevanje veljavnih bistvenih zahtev glede kibernetske varnosti iz Priloge I.

2. EU izjava o skladnosti ima vzorčno strukturo, navedeno v Prilogi V, in vsebuje elemente, opredeljene v ustreznih postopkih ugotavljanja skladnosti iz Priloge VIII. Taka izjava se po potrebi posodablja. Na voljo je v jezikih, ki jih zahteva država članica, v kateri se izdelek z digitalnimi elementi da na trg ali na voljo na trgu.

Poenostavljena EU izjava o skladnosti iz člena 13(20) ima vzorčno strukturo, določeno v Prilogi VI. Na voljo je v jezikih, ki jih zahteva država članica, v kateri se izdelek z digitalnimi elementi da na trg ali na voljo na trgu.

3. Kadar se za izdelek z digitalnimi elementi uporablja več kot en pravni akt Unije, ki zahteva EU izjavo o skladnosti, se v zvezi z vsemi takimi pravnimi akti Unije pripravi enotna EU izjava o skladnosti. V tej izjavi se opredelijo zadevni pravni akti Unije, vključno z navedbo objave.

4. Proizvajalec s pripravo EU izjave o skladnosti prevzame odgovornost za skladnost izdelka z digitalnimi elementi.

5. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 61, s katerimi se zaradi upoštevanja tehnološkega napredka ta uredba dopolni z dodajanjem elementov minimalni vsebini EU izjave o skladnosti, kakor je določena v Prilogi V.

Člen 29

Splošna načela oznake CE

Za oznako CE se uporabljajo splošna načela iz člena 30 Uredbe (ES) št. 765/2008.

Člen 30

Pravila in pogoji za namestitev oznake CE

1. Oznaka CE se vidno, čitljivo in neizbrisno namesti na izdelek z digitalnimi elementi. Kadar to zaradi narave izdelka z digitalnimi elementi ni mogoče ali upravičeno, se namesti na embalažo in na EU izjavo o skladnosti iz člena 28, priloženo izdelku z digitalnimi elementi. Pri izdelkih z digitalnimi elementi v obliki programske opreme se oznaka CE namesti na EU izjavo o skladnosti iz člena 28 ali na spletno mesto, povezano z izdelkom programske opreme. V slednjem primeru mora biti ustrezen razdelek spletnega mesta potrošnikom enostavno in neposredno dostopen.

2. Glede na naravo izdelka z digitalnimi elementi je lahko višina oznake CE, nameščene na izdelek z digitalnimi elementi, manj kot 5 mm, če ob tem ostane vidna in čitljiva.

3. Oznaka CE se namesti, preden se izdelek z digitalnimi elementi da na trg. Lahko ji sledi piktogram ali katera koli druga oznaka, ki označuje posebno tveganje za kibernetsko varnost ali uporabo, določeno v izvedbenih aktih iz odstavka 6.

4. Oznaki CE sledi identifikacijska številka priglašenega organa, kadar je ta vključen v postopek ugotavljanja skladnosti na podlagi popolnega zagotavljanja kakovosti (na podlagi modula H) iz člena 32.

Identifikacijsko številko priglašenega organa namesti organ sam ali jo na podlagi njegovih navodil namesti proizvajalec ali njegov pooblaščeni zastopnik.

5. Države članice nadgrajujejo obstoječe mehanizme, da zagotovijo pravilno uporabo sistema za označevanje z oznako CE, in sprejmejo ustrezne ukrepe v primeru nepravilne rabe te oznake. Kadar izdelek z digitalnimi elementi poleg te uredbe ureja harmonizacijska zakonodaja Unije, ki prav tako določa namestitev oznake CE, taka oznaka kaže, da izdelek izpolnjuje tudi zahteve, določene v drugi taki harmonizacijski zakonodaji Unije.

6. Komisija lahko z izvedbenimi akti določi tehnične specifikacije glede označb, piktogramov ali katerih koli drugih oznak, ki se nanašajo na varnost izdelkov z digitalnimi elementi, obdobja podpore in mehanizme za spodbujanje njihove uporabe ter povečanje ozaveščenosti javnosti o varnosti izdelkov z digitalnimi elementi. Komisija se pri pripravi osnutkov izvedbenih aktov posvetuje z ustreznimi deležniki in, če je že bila ustanovljena na podlagi člena 52(15), s skupino ADCO. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 62(2).

Člen 31

Tehnična dokumentacija

1. Tehnična dokumentacija vsebuje vse ustrezne podatke ali podrobnosti o sredstvih, ki jih je proizvajalec uporabil za zagotovitev, da so izdelek z digitalnimi elementi in postopki, ki jih je vzpostavil proizvajalec, skladni z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I. Vsebuje vsaj elemente iz Priloge VII.

2. Tehnična dokumentacija se pripravi, preden se izdelek z digitalnimi elementi da na trg, in se stalno posodablja, kadar je ustrezno, in sicer vsaj v obdobju podpore.

3. Za izdelke z digitalnimi elementi iz člena 12, za katere se uporabljajo tudi drugi pravni akti Unije, ki zagotavljajo tehnično dokumentacijo, se pripravi enoten sklop tehnične dokumentacije, ki vsebuje informacije iz Priloge VII in informacije, ki jih zahtevajo navedeni pravni akti Unije.

4. Tehnična dokumentacija in korespondenca, ki se nanašata na kateri koli postopek ugotavljanja skladnosti, se pripravita v uradnem jeziku države članice, v kateri je sedež priglašenega organa, ali v jeziku, sprejemljivem za navedeni organ.

5. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 61, s katerimi se zaradi upoštevanja tehnološkega napredka in razvoja dogodkov pri izvajanju te uredbe ta uredba dopolni z elementi, ki jih je treba vključiti v tehnično dokumentacijo iz Priloge VII. V ta namen si Komisija prizadeva zagotoviti sorazmerno upravno breme za mikropodjetja ter mala in srednja podjetja.

Člen 32

Postopki ugotavljanja skladnosti za izdelke z digitalnimi elementi

1. Proizvajalec opravi ugotavljanje skladnosti izdelka z digitalnimi elementi in postopkov, ki jih je vzpostavil, da se preveri izpolnjevanje bistvenih zahtev glede kibernetske varnosti iz Priloge I. Proizvajalec dokazuje skladnost z bistvenimi zahtevami glede kibernetske varnosti z uporabo katerega koli od naslednjih postopkov:

(a) postopka notranje kontrole (na podlagi modula A) iz Priloge VIII;

(b) EU-pregleda tipa (na podlagi modula B) iz Priloge VIII, ki mu sledi skladnost s tipom EU na podlagi notranje kontrole proizvodnje (na podlagi modula C) iz Priloge VIII;

(c) ugotavljanja skladnosti na podlagi popolnega zagotavljanja kakovosti (na podlagi modula H) iz Priloge VIII ali

(d) kadar je na voljo in je ustrezno, evropske certifikacijske sheme kibernetske varnosti na podlagi člena 27(9).

2. Kadar proizvajalec pri ugotavljanju skladnosti pomembnega izdelka z digitalnimi elementi, ki sodi v razred I, kot je določen v Prilogi III, in postopkov, ki jih je vzpostavil proizvajalec, z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I ne uporabi ali le delno uporabi harmonizirane standarde, skupne specifikacije ali evropske certifikacijske sheme kibernetske varnosti na ravni zanesljivosti vsaj „znatno“ iz člena 27 ali kadar taki harmonizirani standardi, skupne specifikacije ali evropske certifikacijske sheme kibernetske varnosti ne obstajajo, se za zadevni izdelek z digitalnimi elementi in postopke, ki jih je vzpostavil proizvajalec, glede teh bistvenih zahtev glede kibernetske varnosti uporabi kateri koli naslednji postopek:

(a) EU-pregled tipa (na podlagi modula B) iz Priloge VIII, ki mu sledi skladnost s tipom EU na podlagi notranje kontrole proizvodnje (na podlagi modula C) iz Priloge VIII, ali

(b) ugotavljanje skladnosti na podlagi popolnega zagotavljanja kakovosti (na podlagi modula H) iz Priloge VIII.

3. Kadar je izdelek pomemben izdelek z digitalnimi elementi, ki sodi v razred II, kakor je določen v Prilogi III, proizvajalec dokazuje skladnost z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I z uporabo katerega koli od naslednjih postopkov:

(a) EU-pregleda tipa (na podlagi modula B) iz Priloge VIII, ki mu sledi skladnost s tipom EU na podlagi notranje kontrole proizvodnje (na podlagi modula C) iz Priloge VIII;

(b) ugotavljanja skladnosti na podlagi popolnega zagotavljanja kakovosti (na podlagi modula H) iz Priloge VIII ali

(c) kadar je na voljo in kadar je ustrezno, evropske certifikacijske sheme kibernetske varnosti, kot je določena na podlagi člena 27(9) te uredbe, na ravni zanesljivosti vsaj „znatno“ na podlagi Uredbe (EU) 2019/881.

4. Kritični izdelki z digitalnimi elementi, navedeni v Prilogi IV, dokazujejo skladnost z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I z uporabo enega od naslednjih postopkov:

(a) evropske certifikacijske sheme kibernetske varnosti, sprejete v skladu s členom 8(1) ali

(b) kadar pogoji iz člena 8(1) niso izpolnjeni, katerega koli postopka iz odstavka 3 tega člena.

5. Proizvajalci izdelkov z digitalnimi elementi, ki se štejejo za prosto in odprtokodno programsko opremo, ki spadajo v kategorije iz Priloge III, lahko dokažejo skladnost z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I z enim od postopkov iz odstavka 1 tega člena, če je tehnična dokumentacija iz člena 31 dostopna javnosti ob dajanju teh izdelkov na trg.

6. Pri določanju pristojbin za izvajanje postopkov ugotavljanja skladnosti se upoštevajo posebni interesi in potrebe mikropodjetij ter malih in srednjih podjetij, vključno z zagonskimi podjetji, te pristojbine pa se znižajo sorazmerno s temi posebnimi interesi in potrebami.

Člen 33

Podporni ukrepi za mikropodjetja ter mala in srednja podjetja, vključno z zagonskimi podjetji

1. Države članice, kadar je primerno, sprejmejo naslednje ukrepe, prilagojene potrebam mikropodjetij in malih podjetij:

(a) organizirajo posebne dejavnosti ozaveščanja in usposabljanja o uporabi te uredbe;

(b) vzpostavijo namenski kanal za komunikacijo z mikropodjetji in malimi podjetji ter po potrebi lokalnimi javnimi organi, da zagotovijo svetovanje in odgovore na vprašanja o izvajanju te uredbe;

(c) podpirajo dejavnosti preskušanja in ugotavljanja skladnosti, po potrebi tudi s podporo Evropskega strokovnega centra za kibernetsko varnost.

2. Države članice lahko po potrebi vzpostavijo regulativne peskovnike za kibernetsko odpornost. Taki regulativni peskovniki zagotavljajo nadzorovana okolja za preskušanje inovativnih izdelkov z digitalnimi elementi, da se olajša njihov razvoj, zasnova, potrjevanje in preskušanje za namene skladnosti s to uredbo za omejeno obdobje pred dajanjem na trg. Komisija in po potrebi agencija ENISA lahko zagotavljata tehnično podporo, svetovanje in orodja za vzpostavitev in delovanje regulativnih peskovnikov. Regulativni peskovniki se vzpostavijo pod neposrednim nadzorom, vodstvom in s podporo organov za nadzor trga. Države članice obvestijo Komisijo in druge organe za nadzor trga o vzpostavitvi regulativnega peskovnika prek skupine ADCO. Regulativni peskovniki ne vplivajo na pooblastila pristojnih organov za nadzor in popravne ukrepe. Države članice zagotovijo odprt, pravičen in pregleden dostop do regulativnih peskovnikov ter zlasti olajšajo dostop mikropodjetjem in malim podjetjem, vključno z zagonskimi podjetji.

3. Komisija v skladu s členom 26 pripravi usmeritve za mikropodjetja ter mala in srednja podjetja v zvezi z izvajanjem te uredbe.

4. Komisija obvešča o finančni podpori, ki je na voljo v regulativnem okviru obstoječih programov Unije, zlasti za zmanjšanje finančnega bremena za mikropodjetja in mala podjetja.

5. Mikropodjetja in mala podjetja lahko vse elemente tehnične dokumentacije iz Priloge VII predložijo v poenostavljeni obliki. V ta namen Komisija z izvedbenimi akti določi poenostavljen obrazec tehnične dokumentacije, prilagojen potrebam mikropodjetij in malih podjetij, vključno s tem, kako je treba zagotoviti elemente iz Priloge VII. Kadar se mikropodjetje ali malo podjetje odloči za predložitev informacij, določenih v Prilogi VII, na poenostavljen način, uporabi obrazec iz tega odstavka. Priglašeni organi sprejmejo ta obrazec za namene ugotavljanja skladnosti.

Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 62(2).

Člen 34

Sporazumi o vzajemnem priznavanju

Ob upoštevanju stopnje tehničnega razvoja in pristopa k ugotavljanju skladnosti tretje države lahko Unija sklene sporazume o medsebojnem priznavanju s tretjimi državami v skladu s členom 218 PDEU, da bi spodbudila in olajšala mednarodno trgovino.

POGLAVJE IV

PRIGLASITEV ORGANOV ZA UGOTAVLJANJE SKLADNOSTI

Člen 35

Priglasitev

1. Države članice Komisiji in drugim državam članicam priglasijo organe, ki so pooblaščeni za izvajanje ugotavljanja skladnosti v skladu s to uredbo.

2. Države članice si prizadevajo zagotoviti, da je do 11. decembra 2026 v Uniji dovolj priglašenih organov za ugotavljanje skladnosti, da se preprečijo ozka grla in ovire za vstop na trg.

Člen 36

Priglasitveni organi

1. Vsaka država članica določi priglasitveni organ, ki je odgovoren za vzpostavitev in izvajanje potrebnih postopkov za ocenjevanje, določitev in priglasitev organov za ugotavljanje skladnosti ter za njihovo spremljanje, vključno s skladnostjo s členom 41.

2. Države članice lahko odločijo, da ocenjevanje in spremljanje iz odstavka 1izvaja nacionalni akreditacijski organ v smislu Uredbe (ES) št. 765/2008 in v skladu z njo.

3. Kadar priglasitveni organ za ocenjevanje, priglasitev ali spremljanje iz odstavka 1 tega člena pooblasti organ, ki ni vladni organ, ali mu drugače zaupa opravljanje teh nalog, je navedeni organ pravna oseba in smiselno izpolnjuje člen 37. Poleg tega mora imeti tak organ urejeno zavarovanje odgovornosti, ki izhajajo iz njegovih dejavnosti.

4. Priglasitveni organ je v celoti odgovoren za naloge, ki jih izvaja organ iz odstavka 3.

Člen 37

Zahteve v zvezi s priglasitvenimi organi

1. Priglasitveni organ se ustanovi tako, da ne pride do nasprotja interesov z organi za ugotavljanje skladnosti.

2. Priglasitveni organ je organiziran in deluje tako, da se zaščitita objektivnost in nepristranskost njegovih dejavnosti.

3. Priglasitveni organ je organiziran tako, da vsako odločitev v zvezi s priglasitvijo organa za ugotavljanje skladnosti sprejmejo pristojne osebe, ki niso tiste, ki so izvedle ocenjevanje.

4. Priglasitveni organ ne ponuja ali izvaja nobenih dejavnosti, ki jih izvajajo organi za ugotavljanje skladnosti, ali storitev svetovanja na komercialni ali konkurenčni podlagi.

5. Priglasitveni organ zagotavlja zaupnost pridobljenih informacij.

6. Priglasitveni organ ima na voljo zadostno število strokovnega osebja za pravilno izvajanje svojih nalog.

Člen 38

Obveznosti priglasitvenih organov glede obveščanja

1. Države članice obvestijo Komisijo o svojih postopkih ocenjevanja in priglasitve organov za ugotavljanje skladnosti ter spremljanja priglašenih organov, pa tudi o vseh spremembah v zvezi s tem.

2. Komisija zagotovi, da so informacije iz odstavka 1 javno dostopne.

Člen 39

Zahteve v zvezi s priglašenimi organi

1. Za namene priglasitve organ za ugotavljanje skladnosti izpolnjuje zahteve iz odstavkov 2 do 12.

2. Organ za ugotavljanje skladnosti se ustanovi na podlagi nacionalnega prava in je pravna oseba.

3. Organ za ugotavljanje skladnosti je organ tretje strani, neodvisen od organizacije ali izdelka z digitalnimi elementi, ki ga ocenjuje.

Organ, ki je del poslovnega združenja ali strokovne zveze, ki zastopa podjetja, vključena v zasnovo, razvoj, proizvodnjo, dobavo, sestavljanje, uporabo ali vzdrževanje izdelkov z digitalnimi elementi, ki jih ocenjuje, se lahko šteje za tak organ tretje strani, če se dokažeta njegova samostojnost in neobstoj nasprotja interesov.

4. Organ za ugotavljanje skladnosti, njegovo najvišje vodstvo in osebje, odgovorno za izvajanje nalog ugotavljanja skladnosti, ne smejo biti oblikovalci, razvijalci, proizvajalci, dobavitelji, uvozniki, distributerji, monterji, kupci, lastniki, uporabniki ali vzdrževalci izdelkov z digitalnimi elementi, ki jih ocenjujejo, niti pooblaščeni zastopniki katere koli izmed teh oseb. To ne onemogoča uporabe ocenjevanih izdelkov, ki so nujni za delovanje organa za ugotavljanje skladnosti, ali uporabe takih izdelkov za osebne namene.

Organ za ugotavljanje skladnosti, njegovo najvišje vodstvo in osebje, odgovorno za izvajanje nalog ugotavljanja skladnosti, ne sodelujejo neposredno pri zasnovi, razvoju, proizvodnji, uvozu, distribuciji, trženju, vgradnji, uporabi ali vzdrževanju izdelkov z digitalnimi elementi, ki jih ocenjujejo, ali zastopajo strank, ki se ukvarjajo s temi dejavnostmi. Ne sodelujejo pri nobenih dejavnostih, ki bi lahko bile v nasprotju z njihovo neodvisno presojo ali integriteto v zvezi z dejavnostmi ugotavljanja skladnosti, za katere so priglašeni. To še zlasti velja za svetovalne storitve.

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

5. Organi za ugotavljanje skladnosti in njihovo osebje izvajajo dejavnosti ugotavljanja skladnosti z najvišjo stopnjo poklicne integritete in potrebno strokovno usposobljenostjo na posameznem področju, brez pritiskov in spodbud, zlasti finančnih, ki bi lahko vplivali na njihovo presojo ali rezultate njihovih dejavnosti ugotavljanja skladnosti, predvsem v zvezi z osebami ali skupinami oseb, za katere so rezultati navedenih dejavnosti pomembni.

6. Organ za ugotavljanje skladnosti je sposoben izvajati vse naloge ugotavljanja skladnosti iz Priloge VIII, za katere je bil priglašen, ne glede na to, ali navedene naloge izvaja sam ali se izvajajo v njegovem imenu in pod njegovo odgovornostjo.

Organ za ugotavljanje skladnosti ima vedno ter za vsak postopek ugotavljanja skladnosti in vsako vrsto ali kategorijo izdelka z digitalnimi elementi, v zvezi s katerim je bil priglašen, na razpolago:

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

(b) potrebne opise postopkov, v skladu s katerimi naj se izvaja ugotavljanje skladnosti, da se zagotovita preglednost in zmožnost ponovitve teh postopkov. Vzpostavljene ima ustrezne politike in postopke za razlikovanje med nalogami, ki jih izvaja kot priglašeni organ, in drugimi dejavnostmi;

(c) potrebne postopke za izvajanje dejavnosti, pri katerih so ustrezno upoštevani velikost podjetja, sektor, v katerem deluje, njegova struktura, stopnja zahtevnosti tehnologije zadevnega izdelka in masovna ali serijska narava proizvodnega postopka.

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

7. Osebje, odgovorno za izvajanje dejavnosti ugotavljanja skladnosti:

(a) je dobro tehnično in poklicno usposobljeno, kar vključuje vse dejavnosti ugotavljanja skladnosti, za katere je organ za ugotavljanje skladnosti priglašen;

(b) ima zadovoljivo znanje o zahtevah glede ugotavljanja skladnosti, ki ga izvaja, in ustrezna pooblastila za izvajanje tega ugotavljanja skladnosti;

(c) ima primerno znanje in razumevanje bistvenih zahtev glede kibernetske varnosti iz Priloge I, veljavnih harmoniziranih standardov in skupnih specifikacij ter ustreznih določb harmonizacijske zakonodaje Unije in njenih izvedbenih aktov;

(d) ima zmožnost priprave certifikatov, zapisov in poročil, ki dokazujejo, da so bila ugotavljanja skladnosti izvedena.

8. Zagotovi se nepristranskost organov za ugotavljanje skladnosti, njihovega najvišjega vodstva in osebja, ki izvaja ugotavljanje skladnosti.

Plačilo najvišjega vodstva in osebja, ki izvaja ugotavljanje skladnosti, organa za ugotavljanje skladnosti ni odvisno od števila izvedenih ugotavljanj skladnosti ali od rezultatov teh ugotovitev.

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

10. Osebje organa za ugotavljanje skladnosti je zavezano k poklicni molčečnosti v zvezi z vsemi informacijami, pridobljenimi med izvajanjem nalog na podlagi Priloge VIII ali katere koli določbe nacionalnega prava, na podlagi katere se ta izvaja, razen glede organov za nadzor trga države članice, v kateri izvaja svoje dejavnosti. Lastniške pravice so zaščitene. Organ za ugotavljanje skladnosti vzpostavi dokumentirane postopke, s katerimi se zagotavlja skladnost s tem odstavkom.

11. Organi za ugotavljanje skladnosti sodelujejo pri ustreznih dejavnostih standardizacije in dejavnostih skupine za koordinacijo priglašenih organov, ustanovljene na podlagi člena 51, ali zagotovijo, da je njihovo osebje za ugotavljanje skladnosti obveščeno o teh dejavnostih, ter kot splošne usmeritve uporabljajo upravne odločbe in dokumente, ki so rezultat dela navedene skupine.

12. Organi za ugotavljanje skladnosti delujejo v skladu z vrsto doslednih, pravičnih, sorazmernih in razumnih pogojev, pri tem pa se izognejo nepotrebni obremenitvi gospodarskih subjektov, zlasti ob upoštevanju interesov mikropodjetij ter malih in srednjih podjetij v zvezi s pristojbinami.

Člen 40

Domneva o skladnosti priglašenih organov

Kadar organ za ugotavljanje skladnosti dokaže skladnost z merili, določenimi v ustreznih harmoniziranih standardih ali njihovih delih, katerih sklici so bili objavljeni v *Uradnem listu Evropske unije*, se domneva, da izpolnjuje zahteve iz člena 39, če veljavni harmonizirani standardi zajemajo te zahteve.

Člen 41

Odvisna podjetja in podizvajalci priglašenih organov

1. Kadar priglašeni organ za določene naloge, povezane z ugotavljanjem skladnosti, sklene pogodbo s podizvajalcem ali jih prenese na odvisno podjetje, zagotovi, da podizvajalec ali odvisno podjetje izpolnjuje zahteve iz člena 39, ter o tem obvesti priglasitveni organ.

2. Priglašeni organi so v celoti odgovorni za naloge, ki jih izvajajo podizvajalci ali odvisna podjetja, ne glede na to, kje imajo sedež.

3. Dejavnosti se lahko prenesejo na podizvajalca ali odvisno podjetje le, če proizvajalec s tem soglaša.

4. Priglašeni organi hranijo zadevne dokumente v zvezi z ocenjevanjem usposobljenosti podizvajalca ali odvisnega podjetja ter nalogami, ki jih izvajajo na podlagi te uredbe, ter omogočajo priglasitvenemu organu dostop do njih.

Člen 42

Vloga za priglasitev

1. Organ za ugotavljanje skladnosti predloži vlogo za priglasitev priglasitvenemu organu države članice, v kateri ima sedež.

2. Tej vlogi se priloži opis dejavnosti ugotavljanja skladnosti, postopka ali postopkov ugotavljanja skladnosti ter izdelka ali izdelkov z digitalnimi elementi, za katere je ta organ po lastnih trditvah pristojen, po potrebi pa se priloži tudi morebitno certifikat o akreditaciji, ki ga izda nacionalni akreditacijski organ in ki potrjuje, da organ za ugotavljanje skladnosti izpolnjuje zahteve iz člena 39.

3. Kadar zadevni organ za ugotavljanje skladnosti ne more zagotoviti certifikata o akreditaciji, priglasitvenemu organu predloži vse listinske dokaze, potrebne za preverjanje, priznavanje in redno spremljanje njegove skladnosti z zahtevami iz člena 39.

Člen 43

Postopek priglasitve

1. Priglasitveni organi priglasijo samo tiste organe za ugotavljanje skladnosti, ki izpolnjujejo zahteve iz člena 39.

2. Priglasitveni organ obvesti Komisijo in druge države članice prek informacijskega sistema o priglašenih in določenih organih novega pristopa, ki ga je razvila in ki ga vodi Komisija.

3. Priglasitev vključuje vse podrobnosti o dejavnostih ugotavljanja skladnosti, modul ali module za ugotavljanje skladnosti in zadevni izdelek ali izdelke z digitalnimi elementi ter ustrezno potrdilo o usposobljenosti.

4. Kadar priglasitev ne temelji na certifikatu o akreditaciji iz člena 42(2), priglasitveni organ Komisiji in drugim državam članicam predloži listinske dokaze, ki potrjujejo usposobljenost organa za ugotavljanje skladnosti in vzpostavljene ureditve za zagotovitev, da bo organ pod rednim nadzorom in bo stalno izpolnjeval zahteve iz člena 39.

5. Zadevni organ lahko izvaja dejavnosti priglašenega organa le, kadar Komisija ali druge države članice ne predložijo ugovora v dveh tednih od priglasitve, kadar se uporabi certifikat o akreditaciji, ali v dveh mesecih od priglasitve, kadar certifikat o akreditaciji ni uporabljen.

Samo tak organ se šteje za priglašeni organ za namene te uredbe.

6. Komisija in druge države članice so uradno obveščene o vseh nadaljnjih zadevnih spremembah priglasitve.

Člen 44

Identifikacijske številke in seznami priglašenih organov

1. Komisija priglašenemu organu dodeli identifikacijsko številko.

Dodeli mu samo eno tako številko, tudi kadar je organ priglašen na podlagi več pravnih aktov Unije.

2. Komisija javno objavi seznam organov, priglašenih na podlagi te uredbe, vključno z identifikacijskimi številkami, ki so jim bile dodeljene, in dejavnostmi, za katere so bili priglašeni.

Komisija zagotovi, da se ta seznam posodablja.

Člen 45

Spremembe priglasitev

1. Kadar priglasitveni organ ugotovi ali je obveščen, da priglašeni organ ne izpolnjuje več zahtev iz člena 39 ali ne izpolnjuje svojih obveznosti, omeji, začasno prekliče ali prekliče priglasitev, kot je ustrezno glede na resnost neizpolnjevanja teh zahtev ali nespoštovanja teh obveznosti. O tem takoj obvesti Komisijo in druge države članice.

2. V primeru omejitve, začasnega preklica ali preklica priglasitve ali kadar je priglašeni organ prenehal opravljati dejavnost, država članica priglasiteljica sprejme ustrezne ukrepe za zagotovitev, da zadeve tega organa obravnava drug priglašeni organ ali da so na zahtevo na voljo pristojnim priglasitvenim organom in organom za nadzor trga.

Člen 46

Izpodbijanje usposobljenosti priglašenih organov

1. Komisija razišče vse primere, v katerih dvomi oziroma kadar je bila opozorjena na dvom v usposobljenost priglašenega organa ali v to, da ta še izpolnjuje zahteve in obveznosti, ki veljajo zanj.

2. Država članica priglasiteljica Komisiji na zahtevo predloži vse informacije v zvezi s podlago za priglasitev ali ohranjanjem usposobljenosti zadevnega organa.

3. Komisija zagotovi, da se vse občutljive informacije, pridobljene v okviru njenih preiskav, obravnavajo zaupno.

4. Kadar Komisija ugotovi, da priglašeni organ ne izpolnjuje ali ne izpolnjuje več zahtev za priglasitev, o tem obvesti državo članico priglasiteljico in od nje zahteva, naj sprejme potrebne popravne ukrepe, vključno z umikom priglasitve, če je to potrebno.

Člen 47

Obveznosti priglašenih organov glede njihovega dela

1. Priglašeni organi izvajajo ugotavljanje skladnosti v skladu s postopki ugotavljanja skladnosti iz člena 32 in Priloge VIII.

2. Ugotavljanje skladnosti se izvaja sorazmerno, tako da se prepreči nepotrebna obremenitev gospodarskih subjektov. Organi za ugotavljanje skladnosti pri izvajanju svojih dejavnosti upoštevajo velikost podjetja, zlasti kar zadeva mikropodjetja ter mala in srednja podjetja, sektor, v katerem delujejo, njihovo strukturo, stopnjo zahtevnosti in raven tveganja za kibernetsko varnost zadevnih izdelkov z digitalnimi elementi in tehnologije in masovno ali serijsko naravo proizvodnega postopka.

3. Vendar priglašeni organi upoštevajo stopnjo strogosti in raven zaščite, ki sta potrebni za skladnost izdelkov z digitalnimi elementi s to uredbo.

4. Kadar priglašeni organ ugotovi, da proizvajalec ni izpolnil zahtev, določenih v Prilogi I, ali v ustreznih harmoniziranih standardih ali skupnih specifikacijah iz člena 27, od njega zahteva, naj sprejme ustrezne popravne ukrepe, in ne izda certifikata o skladnosti.

5. Kadar priglašeni organ med postopkom spremljanja skladnosti po izdaji certifikata o skladnosti ugotovi, da izdelek z digitalnimi elementi ni več skladen z zahtevami iz te uredbe, od proizvajalca zahteva, naj sprejme ustrezne popravne ukrepe, in po potrebi začasno prekliče ali prekliče potrdilo.

6. Kadar popravni ukrepi niso sprejeti ali nimajo zahtevanega učinka, priglašeni organ omeji, začasno prekliče ali prekliče katera koli potrdila, kakor je ustrezno.

Člen 48

Pritožba zoper odločitve priglašenih organov

Države članice zagotovijo, da je na voljo pritožbeni postopek zoper odločitve priglašenih organov.

Člen 49

Obveznosti priglašenih organov glede obveščanja

1. Priglašeni organi obvestijo priglasitveni organ o:

(a) vseh zavrnitvah, omejitvah, začasnih preklicih ali preklicih certifikatov;

(b) vseh okoliščinah, ki vplivajo na področje uporabe priglasitve in pogoje za priglasitev;

(c) vseh zahtevah po informacijah v zvezi z dejavnostmi ugotavljanja skladnosti, ki so jih prejeli od organov za nadzor trga;

(d) dejavnostih ugotavljanja skladnosti, izvedenih v okviru njihove priglasitve, in kakršnih koli drugih izvedenih dejavnostih, vključno s čezmejnimi dejavnostmi in sklepanjem pogodb s podizvajalci, če se to zahteva.

2. Priglašeni organi drugim organom, ki so priglašeni na podlagi te uredbe in izvajajo podobne dejavnosti ugotavljanja skladnosti, ki se nanašajo na enake izdelke z digitalnimi elementi, zagotavljajo ustrezne informacije o vprašanjih v zvezi z negativnimi in, na zahtevo, pozitivnimi rezultati ugotavljanja skladnosti.

Člen 50

Izmenjava izkušenj

Komisija organizira izmenjavo izkušenj med nacionalnimi organi držav članic, ki so pristojni za politiko priglasitev.

Člen 51

Usklajevanje priglašenih organov

1. Komisija zagotovi vzpostavitev in pravilno delovanje ustreznega usklajevanja in sodelovanja med priglašenimi organi v obliki medsektorske skupine priglašenih organov.

2. Države članice zagotovijo, da organi, ki jih priglasijo, neposredno ali po pooblaščenih predstavnikih sodelujejo pri delu te skupine.

POGLAVJE V

NADZOR TRGA IN IZVRŠEVANJE

Člen 52

Nadzor trga in nadzor izdelkov z digitalnimi elementi na trgu Unije

1. Uredba (EU) 2019/1020 se uporablja za izdelke z digitalnimi elementi, ki spadajo na področje uporabe te uredbe.

2. Vsaka država članica imenuje enega ali več organov za nadzor trga, da se zagotovi učinkovito izvajanje te uredbe. Države članice lahko imenujejo obstoječi ali nov organ, ki bo deloval kot organ za nadzor trga za potrebe te uredbe.

3. Organi za nadzor trga, imenovani na podlagi odstavka 2 tega člena, so odgovorni tudi za izvajanje dejavnosti nadzora trga v zvezi z obveznostmi za upravljavce odprtokodne programske opreme iz člena 24. Kadar organ za nadzor trga ugotovi, da upravljavec odprtokodne programske opreme ne izpolnjuje obveznosti iz navedenega člena, od njega zahteva, da sprejme vse ustrezne popravne ukrepe. Upravljavci odprtokodne programske opreme zagotovijo, da se sprejmejo vsi ustrezni popravni ukrepi v zvezi z njihovimi obveznostmi na podlagi te uredbe.

4. Kadar je ustrezno, organi za nadzor trga sodelujejo z nacionalnimi certifikacijskimi organi za kibernetsko varnost, imenovanimi na podlagi člena 58 Uredbe (EU) 2019/881, in si z njimi redno izmenjujejo informacije. Glede nadzora nad izvajanjem obveznosti poročanja na podlagi člena 14 te uredbe imenovani organi za nadzor trga sodelujejo in redno izmenjujejo informacije s skupinami CSIRT, ki so imenovane za koordinatorje, in agencijo ENISA.

5. Organi za nadzor trga lahko skupino CSIRT, ki je imenovana za koordinatorja, ali agencijo ENISA prosijo za tehnično svetovanje o zadevah, povezanih z izvajanjem in izvrševanjem te uredbe. Pri izvajanju preiskave na podlagi člena 54 lahko organi za nadzor trga skupino CSIRT, ki je imenovana za koordinatorja, ali agencijo ENISA zaprosijo za analizo v podporo ocenam skladnosti izdelkov z digitalnimi elementi.

6. Kadar je ustrezno, organi za nadzor trga sodelujejo z drugimi organi za nadzor trga, imenovanimi na podlagi harmonizacijske zakonodaje Unije, ki ni ta uredba, in si z njimi redno izmenjujejo informacije.

7. Organi za nadzor trga sodelujejo, kakor je ustrezno, z organi za nadzor prava Unije o varstvu podatkov. Tako sodelovanje vključuje obveščanje teh organov o vseh ugotovitvah, pomembnih za izpolnjevanje njihovih pristojnosti, tudi ko izdajajo usmeritve in nasvete na podlagi odstavka 10, če se take usmeritve in nasveti nanašajo na obdelavo osebnih podatkov.

Organi za nadzor prava Unije o varstvu podatkov lahko zahtevajo vso dokumentacijo, ki se ustvari ali hrani na podlagi te uredbe, in dostopajo do nje, če je dostop do take dokumentacije potreben za izpolnjevanje njihovih nalog. O vseh takih zahtevah obvestijo imenovane organe za nadzor trga zadevne države članice.

8. Države članice zagotovijo, da imajo imenovani organi za nadzor trga na voljo ustrezne finančne in tehnične vire, kadar je primerno tudi orodja za avtomatično obdelavo, ter človeške vire s potrebnimi veščinami na področju kibernetske varnosti za izpolnjevanje svojih nalog na podlagi te uredbe.

9. Komisija spodbuja in olajša izmenjavo izkušenj med imenovanimi organi za nadzor trga.

10. Organi za nadzor trga lahko zagotavljajo usmeritve in nasvete gospodarskim subjektom glede izvajanja te uredbe, ob podpori Komisije in po potrebi skupin CSIRT in agencije ENISA.

11. Organi za nadzor trga v skladu s členom 11 Uredbe (EU) 2019/1020 obvestijo potrošnike, kje lahko vložijo pritožbe, ki bi lahko kazale na neskladnost s to uredbo, in potrošnikom zagotovijo informacije o tem, kje in kako lahko dostopajo do mehanizmov za lažje poročanje o ranljivostih, incidentih in kibernetskih grožnjah, ki lahko vplivajo na izdelke z digitalnimi elementi.

12. Organi za nadzor trga, kadar je ustrezno, olajšajo sodelovanje z ustreznimi deležniki, vključno z znanstvenimi, raziskovalnimi in potrošniškimi organizacijami.

13. Organi za nadzor trga Komisiji letno poročajo o izidih zadevnih dejavnosti nadzora trga. Imenovani organi za nadzor trga Komisiji in zadevnim nacionalnim organom za varstvo konkurence brez odlašanja sporočijo vse informacije, ugotovljene med dejavnostmi nadzora trga, ki bi lahko bile pomembne za uporabo prava Unije s področja konkurence.

14. Glede izdelkov z digitalnimi elementi, ki spadajo na področje uporabe te uredbe, ki so na podlagi člena 6 Uredbe (EU) 2024/1689 razvrščeni kot visokotvegani sistemi UI, so organi za nadzor trga, imenovani za namene navedene uredbe, organi, ki so odgovorni za dejavnosti nadzora trga, ki se zahtevajo na podlagi te uredbe. Organi za nadzor trga, imenovani na podlagi Uredbe (EU) 2024/1689, sodelujejo, kakor je ustrezno, z organi za nadzor trga, imenovanimi na podlagi te uredbe, v zvezi z nadzorom izvajanja obveznosti poročanja na podlagi člena 14 te uredbe, pa tudi s skupinami CSIRT, ki so imenovane za koordinatorje, in z agencijo ENISA. Organi za nadzor trga, imenovani na podlagi Uredbe (EU) 2024/1689, zlasti obveščajo organe za nadzor trga, imenovane na podlagi te uredbe, o vseh ugotovitvah, ki so pomembne za izpolnjevanje njihovih nalog v zvezi z izvajanjem te uredbe.

15. Na podlagi člena 30(2) Uredbe (EU) 2019/1020 se ustanovi skupina ADCO za enotno uporabo te uredbe. Skupino ADCO sestavljajo predstavniki imenovanih organov za nadzor trga in, če je ustrezno, predstavniki enotnih povezovalnih organov. Skupina ADCO obravnava tudi posebna vprašanja v zvezi z dejavnostmi nadzora trga glede obveznosti upravljavcev odprtokodne programske opreme.

16. Organi za nadzor trga spremljajo, kako proizvajalci uporabljajo merila iz člena 13(8), ko določajo obdobje podpore za svoje izdelke z digitalnimi elementi.

Skupina ADCO v javno dostopni in uporabniku prijazni obliki objavi ustrezne statistične podatke o kategorijah izdelkov z digitalnimi elementi, vključno s povprečnimi obdobji podpore, kot jih določi proizvajalec na podlagi člena 13(8), ter zagotovi usmeritve z okvirnimi obdobji podpore za kategorije izdelkov z digitalnimi elementi.

Kadar podatki pokažejo, da so obdobja podpore za določene kategorije izdelkov z digitalnimi elementi neustrezna, lahko skupina ADCO organom za nadzor trga priporoči, naj svoje dejavnosti osredotočijo na take kategorije izdelkov z digitalnimi elementi.

Člen 53

Dostop do podatkov in dokumentacije

Kadar je treba oceniti skladnost izdelkov z digitalnimi elementi in postopkov, ki so jih vzpostavili njihovi proizvajalci, z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I, se organom za nadzor trga na njihovo obrazloženo zahtevo omogoči dostop do podatkov, v jeziku, ki ga zlahka razumejo, ki so potrebni za ocenjevanje zasnove, razvoja, proizvodnje in obravnavanja ranljivosti takih izdelkov, vključno z zadevno interno dokumentacijo zadevnih gospodarskih subjektov.

Člen 54

Postopek na nacionalni ravni glede izdelkov z digitalnimi elementi, ki pomenijo povečano tveganje za kibernetsko varnost

1. Kadar ima organ za nadzor trga države članice zadostne razloge za mnenje, da izdelek z digitalnimi elementi, vključno z obravnavanjem njegove ranljivosti, pomeni povečano tveganje za kibernetsko varnost, brez nepotrebnega odlašanja in po potrebi v sodelovanju z zadevno skupino CSIRT opravi oceno zadevnega izdelka z digitalnimi elementi glede njegove skladnosti z vsemi zahtevami iz te uredbe. Zadevni gospodarski subjekti sodelujejo z organi za nadzor trga, kakor je potrebno.

Kadar med navedenim ocenjevanjem organ za nadzor trga ugotovi, da izdelek z digitalnimi elementi ne izpolnjuje zahtev iz te uredbe, od zadevnega gospodarskega subjekta brez odlašanja zahteva, naj sprejme vse ustrezne popravne ukrepe za zagotovitev, da izdelek z digitalnimi elementi izpolnjuje navedene zahteve, ga umakne s trga oziroma ga odpokliče v razumnem roku, ki je sorazmeren z naravo tveganja za kibernetsko varnost in ki ga lahko določi organ za nadzor trga.

Organ za nadzor trga o tem obvesti zadevni priglašeni organ. Člen 18 Uredbe (EU) 2019/1020 se uporablja za popravne ukrepe.

2. Organi za nadzor trga pri določanju pomembnosti tveganja za kibernetsko varnost iz odstavka 1 tega člena upoštevajo tudi netehnične dejavnike tveganja, zlasti tiste, ki so bili ugotovljeni na podlagi usklajenih ocen tveganja za varnost kritičnih dobavnih verig na ravni Unije, izvedenih v skladu s členom 22 Direktive (EU) 2022/2555. Kadar ima organ za nadzor trga zadostne razloge za domnevo, da izdelek z digitalnimi elementi predstavlja povečano tveganje za kibernetsko varnost zaradi netehničnih dejavnikov tveganja, o tem obvesti pristojne organe, imenovane ali ustanovljene na podlagi člena 8 Direktive (EU) 2022/2555 in po potrebi sodeluje s temi organi.

3. Kadar organ za nadzor trga meni, da neskladnost ni omejena na njegovo nacionalno ozemlje, Komisijo in druge države članice obvesti o rezultatih ocenjevanja in ukrepih, ki jih je zahteval od gospodarskega subjekta.

4. Gospodarski subjekt zagotovi izvedbo vseh ustreznih popravnih ukrepov glede vseh zadevnih izdelkov z digitalnimi elementi, katerih dostopnost na trgu je omogočil kjer koli v Uniji.

5. Kadar gospodarski subjekt v roku iz odstavka 1, drugi pododstavek, ne sprejme zadostnih popravnih ukrepov, organ za nadzor trga sprejme vse ustrezne začasne ukrepe za prepoved ali omejitev dostopnosti izdelka z digitalnimi elementi na svojem nacionalnem trgu oziroma za njegov umik ali odpoklic s trga.

Ta organ o navedenih ukrepih nemudoma uradno obvesti Komisijo in druge države članice.

6. Informacije iz odstavka 5 vsebujejo vse razpoložljive podrobnosti, zlasti podatke, potrebne za identifikacijo neskladnega izdelka z digitalnimi elementi, poreklo tega izdelka z digitalnimi elementi, vrsto domnevne neskladnosti in tveganja, vrsto in trajanje sprejetih nacionalnih ukrepov ter argumente zadevnega gospodarskega subjekta. Organ za nadzor trga zlasti navede, ali je neskladnost posledica naslednjega:

(a) izdelek z digitalnimi elementi ali postopki, ki jih je vzpostavil proizvajalec, ne izpolnjujejo bistvenih zahtev glede kibernetske varnosti iz Priloge I;

(b) obstajajo pomanjkljivosti v harmoniziranih standardih, evropskih certifikacijskih shemah kibernetske varnosti ali skupnih specifikacijah, navedenih v členu 27.

7. Organi za nadzor trga držav članic, razen organa za nadzor trga države članice, ki je začel postopek, brez odlašanja obvestijo Komisijo in druge države članice o vseh sprejetih ukrepih in vseh dodatnih informacijah, ki so jim na voljo v zvezi z neskladnostjo zadevnega izdelka z digitalnimi elementi, ter o svojih ugovorih v primeru nestrinjanja s priglašenim nacionalnim ukrepom.

8. Kadar države članice ali Komisija v treh mesecih po prejemu obvestila iz odstavka 5 tega člena ne vložijo ugovora zoper začasni ukrep, ki ga je sprejela posamezna država članica, se šteje, da je ukrep upravičen. To ne posega v postopkovne pravice zadevnega gospodarskega subjekta v skladu s členom 18 Uredbe (EU) 2019/1020.

9. Organi za nadzor trga vseh držav članic zagotovijo, da se brez odlašanja sprejmejo ustrezni omejevalni ukrepi v zvezi z zadevnim izdelkom z digitalnimi elementi, na primer umik tega izdelka z njihovega trga.

Člen 55

Zaščitni postopek Unije

1. Kadar država članica v treh mesecih od prejema uradnega obvestila iz člena 54(5) poda ugovor proti ukrepu, ki ga je sprejela druga država članica, ali kadar Komisija meni, da je ukrep v nasprotju s pravom Unije, se Komisija brez odlašanja posvetuje z zadevno državo članico in gospodarskim subjektom ali gospodarskimi subjekti ter oceni nacionalni ukrep. Komisija na podlagi rezultatov tega ocenjevanja v devetih mesecih od uradnega obvestila iz člena 54(5) odloči, ali je nacionalni ukrep upravičen ali ne, in o tej odločitvi uradno obvesti zadevno državo članico.

2. Če se nacionalni ukrep šteje za upravičenega, vse države članice sprejmejo potrebne ukrepe za zagotovitev, da se neskladni izdelek z digitalnimi elementi umakne z njihovega trga, in o tem obvestijo Komisijo. Če se ugotovi, da je nacionalni ukrep neupravičen, zadevna država članica ukrep umakne.

3. Kadar se nacionalni ukrep šteje za upravičenega, vzrok za neskladnost izdelka z digitalnimi elementi pa so pomanjkljivosti v harmoniziranih standardih, Komisija uporabi postopek iz člena 11 Uredbe (EU) št. 1025/2012.

4. Kadar se nacionalni ukrep šteje za upravičenega, vzrok za neskladnost izdelka z digitalnimi elementi pa so pomanjkljivosti v evropski certifikacijski shemi kibernetske varnosti, kot je navedena v členu 27, Komisija prouči, ali naj spremeni ali razveljavi vsak delegirani akt, sprejet na podlagi člena 27(9), ki določa domnevo o skladnosti v zvezi s tako certifikacijsko shemo.

5. Kadar se nacionalni ukrep šteje za upravičenega, vzrok za neskladnost izdelka z digitalnimi elementi pa so pomanjkljivosti v skupnih specifikacijah iz člena 27, Komisija prouči, ali naj spremeni ali razveljavi vsak izvedbeni akt, sprejet na podlagi člena 27(2), v katerem so določene navedene skupne specifikacije.

Člen 56

Postopek na ravni Unije glede izdelkov z digitalnimi elementi, ki pomenijo povečano tveganje za kibernetsko varnost

1. Kadar Komisija utemeljeno domneva, tudi na podlagi informacij, ki jih zagotovi agencija ENISA, da izdelek z digitalnimi elementi, ki pomeni povečano tveganje za kibernetsko varnost, ni skladen z zahtevami iz te uredbe, obvesti zadevne organe za nadzor trga. Kadar organi za nadzor trga opravijo oceno tega izdelka z digitalnimi elementi, ki lahko pomeni povečano tveganje za kibernetsko varnost v smislu njegove skladnosti z zahtevami iz te uredbe, se uporabijo postopki iz členov 54 in 55.

2. Kadar Komisija utemeljeno domneva, da izdelek z digitalnimi elementi predstavlja povečano tveganje za kibernetsko varnost zaradi netehničnih dejavnikov tveganja, o tem obvesti ustrezne organe za nadzor trga in, kadar je primerno, pristojne organe, imenovane ali ustanovljene na podlagi člena 8 Direktive (EU) 2022/2555, ter po potrebi sodeluje s temi organi. Komisija upošteva tudi ustreznost ugotovljenih tveganj za ta izdelek z digitalnimi elementi glede na svoje naloge, povezane z usklajenimi ocenami tveganja za varnost kritičnih dobavnih verig na ravni Unije iz člena 22 Direktive (EU) 2022/2555 ter se po potrebi posvetuje s skupino za sodelovanje, ustanovljeno na podlagi člena 14 Direktive (EU) 2022/2555, in agencijo ENISA.

3. V okoliščinah, ki zahtevajo takojšnje ukrepanje za ohranitev pravilnega delovanja notranjega trga, in kadar ima Komisija zadostne razloge za mnenje, da izdelek z digitalnimi elementi iz odstavka 1 še vedno ni skladen z zahtevami iz te uredbe, zadevni organi za nadzor trga pa niso sprejeli učinkovitih ukrepov, Komisija opravi oceno skladnosti in lahko od agencije ENISA zahteva, da zagotovi analizo v podporo tej oceni. Komisija o tem obvesti zadevne organe za nadzor trga. Zadevni gospodarski subjekti sodelujejo z agencijo ENISA, kakor je potrebno.

4. Komisija lahko na podlagi ocene iz odstavka 3 določi, da je na ravni Unije potreben popravni ali omejevalni ukrep. V ta namen se brez odlašanja posvetuje z zadevnimi državami članicami in gospodarskim subjektom ali subjekti.

5. Na podlagi posvetovanja iz odstavka 4 tega člena lahko Komisija sprejme izvedbene akte, s katerimi zagotovi popravne ali omejevalne ukrepe na ravni Unije, vključno z odreditvijo umika zadevnega izdelka z digitalnimi elementi s trga ali odpoklica v razumnem roku, ki je sorazmeren z naravo tveganja. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 62(2).

6. Komisija izvedbeni akt iz odstavka 5 takoj sporoči zadevnemu gospodarskemu subjektu ali subjektom. Države članice te izvedbene akte brez odlašanja izvedejo in o tem obvestijo Komisijo.

7. Odstavki 3 do 6 se uporabljajo, dokler trajajo izredne razmere, ki upravičujejo poseg Komisije, pod pogojem, da ni zagotovljena skladnost zadevnega izdelka z digitalnimi elementi s to uredbo.

Člen 57

Skladni izdelki z digitalnimi elementi, ki pomenijo povečano tveganje za kibernetsko varnost

1. Organ za nadzor trga države članice od gospodarskega subjekta zahteva, da sprejme vse ustrezne ukrepe, kadar po izvedbi ocene na podlagi člena 54 ugotovi, da so izdelek z digitalnimi elementi in postopki, ki jih je vzpostavil proizvajalec, sicer skladni s to uredbo, vendar kljub temu pomenijo povečano tveganje za kibernetsko varnost, poleg tega pa pomenijo tudi tveganje za:

(a) zdravje ali varnost oseb;

(b) skladnost z obveznostmi na podlagi prava Unije ali nacionalnega prava, namenjenega varstvu temeljnih pravic;

(c) razpoložljivost, avtentičnost, celovitost ali zaupnost storitev, ki jih z uporabo elektronskega informacijskega sistema zagotavljajo bistveni subjekti iz člena 3(1) Direktive (EU) 2022/2555, ali

(d) druge vidike zaščite javnega interesa.

Ukrepi iz prvega pododstavka lahko vključujejo ukrepe za zagotovitev, da zadevni izdelek z digitalnimi elementi in postopki, ki jih je vzpostavil proizvajalec, ko so dani na trg, ne pomenijo več ustreznih tveganj, umik izdelka z digitalnimi elementi s trga ali odpoklic v razumnem roku, ki je sorazmeren z naravo teh tveganj.

2. Proizvajalec ali drugi zadevni gospodarski subjekti zagotovijo izvedbo popravnih ukrepov glede zadevnih izdelkov z digitalnimi elementi, katerih dostopnost na trgu so omogočili kjer koli v Uniji, v roku, ki ga predpiše organ za nadzor trga države članice iz odstavka 1.

3. Država članica takoj obvesti Komisijo in druge države članice o ukrepih, sprejetih na podlagi odstavka 1. Te informacije vsebujejo vse razpoložljive podrobnosti, zlasti podatke, potrebne za identifikacijo zadevnih izdelkov z digitalnimi elementi, poreklo in dobavno verigo navedenih izdelkov z digitalnimi elementi, naravo tveganja ter vrsto in trajanje sprejetih nacionalnih ukrepov.

4. Komisija se brez odlašanja posvetuje z državami članicami in zadevnim gospodarskim subjektom ter oceni sprejete nacionalne ukrepe. Na podlagi rezultatov navedenega ocenjevanja odloči, ali je ukrep upravičen ali ne, in po potrebi predlaga ustrezne ukrepe.

5. Komisija odločitev iz odstavka 4 naslovi na države članice.

6. Kadar Komisija utemeljeno domneva, tudi na podlagi informacij, ki jih zagotovi agencija ENISA, da izdelek z digitalnimi elementi, ki je sicer skladen s to uredbo, pomeni tveganja iz odstavka 1 tega člena, obvesti zadevni organ ali organe za nadzor trga in od njih zahteva, naj opravijo oceno in izvedejo postopke iz člena 54 ter iz odstavkov 1, 2 in 3 tega člena.

7. V okoliščinah, ki zahtevajo takojšnje ukrepanje za ohranitev dobrega delovanja notranjega trga, in kadar ima Komisija zadostne razloge za mnenje, da izdelek z digitalnimi elementi iz odstavka 6 še vedno pomeni tveganja iz odstavka 1, zadevni nacionalni organi za nadzor trga pa niso sprejeli nobenih učinkovitih ukrepov, opravi oceno tveganj tega izdelka z digitalnimi elementi in lahko od agencije ENISA zahteva, da zagotovi analizo v podporo tej oceni, ter o tem obvesti zadevne organe za nadzor trga. Zadevni gospodarski subjekti sodelujejo z agencijo ENISA, kakor je potrebno.

8. Komisija lahko na podlagi ocene iz odstavka 7 določi, da je na ravni Unije potreben popravni ali omejevalni ukrep. V ta namen se brez odlašanja posvetuje z zadevnimi državami članicami in gospodarskim subjektom ali subjekti.

9. Na podlagi posvetovanja iz odstavka 8 tega člena lahko Komisija sprejme izvedbene akte, s katerimi odloči o popravnih ali omejevalnih ukrepih na ravni Unije, vključno z odreditvijo umika zadevnega izdelka z digitalnimi elementi s trga ali odpoklica v razumnem roku, ki je sorazmeren z naravo tveganja. Ti izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 62(2).

10. Komisija izvedbene akte iz odstavka 9 takoj sporoči zadevnemu gospodarskemu subjektu ali subjektom. Države članice te izvedbene akte brez odlašanja izvedejo in o tem obvestijo Komisijo.

11. Odstavki 6 do 10 se uporabljajo, dokler trajajo izredne razmere, ki upravičujejo poseg Komisije, in dokler zadevni izdelek z digitalnimi elementi še pomeni tveganja iz odstavka 1.

Člen 58

Formalna neskladnost

1. Kadar organ za nadzor trga države članice ugotovi eno od naslednjih dejstev, od zadevnega proizvajalca zahteva, naj zadevno neskladnost odpravi:

(a) oznaka CE ni nameščena v skladu s členoma 29 in 30;

(b) oznaka CE ni nameščena;

(c) EU izjava o skladnosti ni pripravljena;

(d) EU izjava o skladnosti ni pravilno pripravljena;

(e) identifikacijska številka priglašenega organa, ki je, kadar je ustrezno, vključen v postopek ugotavljanja skladnosti, ni nameščena;

(f) tehnična dokumentacija ni na voljo ali ni popolna.

2. Kadar se neskladnost iz odstavka 1 nadaljuje, zadevna država članica sprejme vse ustrezne ukrepe za omejitev ali prepoved dostopnosti izdelka z digitalnimi elementi na trgu ali pa zagotovi njegov odpoklic oziroma umik s trga.

Člen 59

Skupne dejavnosti organov za nadzor trga

1. Organi za nadzor trga se lahko z drugimi zadevnimi organi dogovorijo za izvajanje skupnih dejavnosti, katerih cilj je zagotoviti kibernetsko varnost in varstvo potrošnikov glede posameznih izdelkov z digitalnimi elementi, ki se dajo na trg ali katerih dostopnost se zagotovi na trgu, zlasti izdelkov z digitalnimi elementi, pri katerih se pogosto ugotovi, da pomenijo tveganje za kibernetsko varnost.

2. Komisija ali agencija ENISA predlaga skupne dejavnosti za preverjanje skladnosti s to uredbo, ki jih izvedejo organi za nadzor trga na podlagi znakov ali informacij o morebitni neskladnosti izdelkov z digitalnimi elementi, ki spadajo na področje uporabe te uredbe, z zahtevami iz te uredbe v več državah članicah.

3. Organi za nadzor trga in Komisija, kadar je ustrezno, zagotovijo, da sporazum o izvajanju skupnih dejavnosti ne povzroči nelojalne konkurence med gospodarskimi subjekti ter ne vpliva negativno na objektivnost, neodvisnost in nepristranskost strank sporazuma.

4. Organ za nadzor trga lahko v okviru vsake preiskave, ki jo izvaja, uporabi vse informacije, pridobljene iz skupnih dejavnosti.

5. Zadevni organ za nadzor trga in Komisija, kadar je ustrezno, omogočita dostop javnosti do sporazuma o skupnih dejavnostih, vključno z imeni strank.

Člen 60

Usklajene preiskave

1. Organi za nadzor trga izvajajo sočasne usklajene kontrolne ukrepe (v nadaljnjem besedilu: usklajene preiskave) posameznih izdelkov z digitalnimi elementi ali njihovih kategorij, da se preveri njihova skladnost s to uredbo ali da se odkrijejo kršitve te uredbe. Te usklajene preiskave lahko vključujejo inšpekcijske preglede izdelkov z digitalnimi elementi, pridobljenih na podlagi skrivne identitete.

2. Če se vključeni organi za nadzor trga ne dogovorijo drugače, usklajene preiskave usklajuje Komisija. Koordinator usklajenih preiskav, kadar je ustrezno, javno objavi zbirne rezultate.

3. Kadar agencija ENISA pri izvajanju svojih nalog, tudi na podlagi obvestil, prejetih na podlagi člena 14(1) in (3), opredeli kategorije izdelkov z digitalnimi elementi, glede katerih je mogoče organizirati usklajene preiskave, koordinatorju iz odstavka 2 tega člena predloži predlog za usklajeno preiskavo, da bi ga organi za nadzor trga obravnavali.

4. Pri izvajanju usklajenih preiskav lahko vključeni organi za nadzor trga uporabijo preiskovalna pooblastila iz členov 52 do 58 in vsa druga pooblastila, ki so jim podeljena z nacionalnim pravom.

5. Organi za nadzor trga lahko k sodelovanju pri usklajenih preiskavah povabijo uradnike Komisije in drugo spremljevalno osebje, ki ga je pooblastila Komisija.

POGLAVJE VI

PRENESENA POOBLASTILA IN POSTOPEK V ODBORU

Člen 61

Izvajanje prenosa pooblastila

1. Pooblastilo za sprejemanje delegiranih aktov je preneseno na Komisijo pod pogoji, določenimi v tem členu.

2. Pooblastilo za sprejemanje delegiranih aktov iz člena 2(5), drugi pododstavek, člena 7(3), člena 8(1) in (2), člena 13(8), četrti pododstavek, člena 14(9), člena 25, člena 27(9), člena 28(5) in člena 31(5) se prenese na Komisijo za obdobje petih let od 10. decembra 2024. Komisija pripravi poročilo o prenosu pooblastila najpozneje devet mesecev pred koncem petletnega obdobja. Prenos pooblastila se samodejno podaljšuje za enako dolga obdobja, razen če Evropski parlament ali Svet nasprotuje temu podaljšanju najpozneje tri mesece pred koncem vsakega obdobja.

3. Prenos pooblastila iz člena 2(5), drugi pododstavek, člena 7(3), člena 8(1) in (2), člena 13(8), četrti pododstavek, člena 14(9), člena 25, člena 27(9), člena 28(5) ter člena 31(5) lahko kadar koli prekliče Evropski parlament ali Svet. S sklepom o preklicu preneha veljati prenos pooblastila iz navedenega sklepa. Sklep začne učinkovati dan po njegovi objavi v *Uradnem listu Evropske unije* ali na poznejši dan, ki je določen v navedenem sklepu. Sklep ne vpliva na veljavnost že veljavnih delegiranih aktov.

4. Komisija se pred sprejetjem delegiranega akta posvetuje s strokovnjaki, ki jih imenujejo države članice, v skladu z načeli, določenimi v Medinstitucionalnem sporazumu z dne 13. aprila 2016 o boljši pripravi zakonodaje.

5. Komisija takoj po sprejetju delegiranega akta o njem sočasno uradno obvesti Evropski parlament in Svet.

6. Delegirani akt, sprejet na podlagi člena 2(5), drugi pododstavek, členom 7(3), členom 8(1) ali (2), členom 13(8), četrti pododstavek, členom 14(9), členom 25, členom 27(9), členom 28(5) ali členom 31(5), začne veljati le, če mu niti Evropski parlament niti Svet ne nasprotuje v roku dveh mesecev od uradnega obvestila Evropskemu parlamentu in Svetu o tem aktu ali če pred iztekom tega roka tako Evropski parlament kot Svet obvestita Komisijo, da mu ne bosta nasprotovala. Ta rok se na pobudo Evropskega parlamenta ali Sveta podaljša za dva meseca.

Člen 62

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 člen 5 Uredbe (EU) št. 182/2011.

3. Kadar je treba pridobiti mnenje odbora na podlagi pisnega postopka, se ta postopek zaključi brez izida, ko v roku za izdajo mnenja tako odloči predsednik odbora ali to zahteva član odbora.

POGLAVJE VII

ZAUPNOST IN KAZNI

Člen 63

Zaupnost

1. Vse strani, ki so vključene v uporabo te uredbe, spoštujejo zaupnost informacij in podatkov, pridobljenih pri opravljanju svojih nalog in dejavnosti, tako da varujejo zlasti:

(a) pravice intelektualne lastnine in zaupne poslovne informacije ali poslovne skrivnosti fizične ali pravne osebe, vključno z izvorno kodo, razen v primerih iz člena 5 Direktive (EU) 2016/943 Evropskega parlamenta in Sveta ([37]);

(b) učinkovito izvajanje te uredbe, zlasti za namene inšpekcijskih pregledov, preiskav ali presoj;

(c) javne interese in interese nacionalne varnosti;

(d) celovitost kazenskih ali upravnih postopkov.

2. Brez poseganja v odstavek 1 se informacije, ki si jih zaupno izmenjajo organi za nadzor trga ter organi za nadzor trga in Komisija, ne razkrijejo brez predhodnega dogovora z organom za nadzor trga, ki jih je sporočil.

3. Odstavka 1 in 2 ne vplivata na pravice in obveznosti Komisije, držav članic in priglašenih organov v zvezi z izmenjavo informacij in razširjanjem opozoril ali na obveznosti zadevnih oseb, da zagotovijo podatke na podlagi kazenskega prava držav članic.

4. Komisija in države članice lahko izmenjajo, kadar je potrebno, občutljive informacije z zadevnimi organi tretjih držav, s katerimi so sklenile dvostranske ali večstranske dogovore o zaupnosti, ki zagotavljajo ustrezno raven varstva.

Člen 64

Kazni

1. Države članice določijo pravila o kaznih, ki se uporabljajo za kršitve te uredbe, in sprejmejo vse potrebne ukrepe za zagotovitev, da se te kazni izvajajo. Te kazni morajo biti učinkovite, sorazmerne in odvračilne. Države članice o teh pravilih in ukrepih uradno obvestijo Komisijo brez odlašanja in jo uradno obvestijo o vsakršni naknadni spremembi, ki nanje vpliva.

2. Neskladnost z bistvenimi zahtevami glede kibernetske varnosti, določenimi v Prilogi I, ter neizpolnjevanje obveznosti iz členov 13 in 14 se kaznuje z upravno globo v višini do 15 000 000 EUR ali, če je kršitelj podjetje, v višini do 2,5 % njegovega skupnega svetovnega letnega prometa v preteklem poslovnem letu, pri čemer se upošteva višji znesek.

3. Neizpolnjevanje obveznosti iz členov 18 do 23, člena 28, člena 30(1) do (4), člena 31(1) do (4), člena 32(1), (2) in (3), člena 33(5) ter členov 39, 41, 47, 49 in 53 se kaznuje z upravno globo v višini do 10 000 000 EUR ali, če je kršitelj podjetje, v višini do 2 % njegovega skupnega svetovnega letnega prometa v preteklem poslovnem letu, pri čemer se upošteva višji znesek.

4. Predložitev netočnih, nepopolnih ali zavajajočih informacij priglašenim organom in organom za nadzor trga v odgovor na njihovo zahtevo se kaznuje z upravno globo v višini do 5 000 000 EUR ali, če je kršitelj podjetje, v višini do 1 % njegovega skupnega svetovnega letnega prometa v preteklem poslovnem letu, pri čemer se upošteva višji znesek.

([37]) Direktiva (EU) 2016/943 Evropskega parlamenta in Sveta z dne 8. junija 2016 o varstvu nerazkritega strokovnega znanja in izkušenj ter poslovnih informacij (poslovnih skrivnosti) pred njihovo protipravno pridobitvijo, uporabo in razkritjem (UL L 157, 15.6.2016, str. 1).

5. Pri odločanju o znesku upravne globe v vsakem posameznem primeru se upoštevajo vse zadevne okoliščine konkretnega primera, pri tem pa se ustrezno upošteva tudi naslednje:

(a) vrsta, resnost in trajanje kršitve ter njenih posledic;

(b) ali so isti ali drugi organi za nadzor trga istemu gospodarskemu subjektu za podobno kršitev že naložili upravne globe;

(c) velikost, zlasti kar zadeva mikropodjetja, mala in srednja podjetja, vključno z zagonskimi podjetji, in tržni delež gospodarskega subjekta, ki je storil kršitev.

6. Organi za nadzor trga, ki naložijo upravne globe, o naložitvi globe obvestijo organe za nadzor trga drugih držav članic prek informacijskega in komunikacijskega sistema iz člena 34 Uredbe (EU) 2019/1020.

7. Vsaka država članica določi pravila o tem, ali in v kolikšni meri se lahko javnim organom in javnim telesom s sedežem v zadevni državi članici naložijo upravne globe.

8. Glede na pravni sistem držav članic se lahko pravila o upravnih globah uporabljajo tako, da globe naložijo pristojna nacionalna sodišča ali drugi organi v skladu s pristojnostmi, ki so jim na nacionalni ravni dodeljene v teh državah članicah. Uporaba takih pravil v teh državah članicah ima enakovreden učinek.

9. Glede na okoliščine posamezne zadeve se lahko upravne globe naložijo poleg katerih koli drugih popravnih ali omejevalnih ukrepov, ki jih za isto kršitev naložijo organi za nadzor trga.

10. Z odstopanjem od odstavkov 3 do 9 se upravne globe iz navedenih odstavkov ne uporabljajo za:

(a) proizvajalce, ki se štejejo za mikropodjetja ali mala podjetja, v zvezi z neupoštevanjem roka iz člena 14(2), točka (a), ali člena 14(4), točka (a);

(b) vsako kršitev te uredbe, ki jo storijo upravljavci odprtokodne programske opreme.

Člen 65

Zastopniške tožbe

Direktiva (EU) 2020/1828 se uporablja za zastopniške tožbe zoper kršitve določb te uredbe, ki jih storijo gospodarski subjekti in škodujejo ali bi lahko škodovale kolektivnim interesom potrošnikov.

POGLAVJE VIII

PREHODNE IN KONČNE DOLOČBE

Člen 66

Sprememba Uredbe (EU) 2019/1020

V Prilogi I k Uredbi (EU) 2019/1020 se doda naslednja točka:

„72. Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta (*).

(*) Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) (UL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).“

Člen 67

Sprememba Direktive (EU) 2020/1828

V Prilogi I k Direktivi (EU) 2020/1828 se doda naslednja točka:

„69. Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta (*).

(*) Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) (UL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).“

Člen 68

Sprememba Uredbe (EU) št. 168/2013

V delu C1 se v preglednici Priloge II k Uredbi (EU) št. 168/2013 Evropskega parlamenta in Sveta ([38]) doda naslednji vnos:

„

16	18	zaščita vozila pred kibernetskimi napadi		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

“

Člen 69

Prehodne določbe

1. Potrdila o EU-pregledu tipa in sklepi o odobritvi, izdani v zvezi z zahtevami glede kibernetske varnosti za izdelke z digitalnimi elementi, za katere se uporablja druga harmonizacijska zakonodaja Unije, ki ni ta uredba, ostanejo veljavni do 11. junija 2028, razen če potečejo pred tem datumom ali če je drugače določeno v tej drugi harmonizacijski zakonodaji Unije, pri čemer v takem primeru ostanejo veljavni, kakor je določeno v navedeni zakonodaji.

2. Za izdelke z digitalnimi elementi, ki so bili dani na trg pred 11. decembrom 2027, se zahteve, določene v tej uredbi, uporabljajo le, če se navedeni izdelki po navedenem datumu bistveno spremenijo.

3. Z odstopanjem od odstavka 2 tega člena se obveznosti iz člena 14 uporabljajo za vse izdelke z digitalnimi elementi na področju uporabe te uredbe, ki so bili dani na trg pred 11. decembrom 2027.

Člen 70

Ocena in pregled

1. Komisija do 11. decembra 2030 ter potem vsaka štiri leta Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu te uredbe. Ta poročila se objavijo.

2. Komisija do 11. septembra 2028 po posvetovanju z agencijo ENISA in mrežo skupin CSIRT Evropskemu parlamentu in Svetu predloži poročilo, v katerem oceni učinkovitost enotne platforme za poročanje iz člena 16 ter učinek uporabe razlogov, povezanih s kibernetsko varnostjo, iz člena 16(2) s strani skupin CSIRT, ki so imenovani za koordinatorje, na učinkovitost enotne platforme za poročanje v zvezi s pravočasnim razširjanjem prejetih obvestil drugim ustreznim skupinam CSIRT.

Člen 71

Začetek veljavnosti in uporaba

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

([38]) Uredba (EU) št. 168/2013 Evropskega parlamenta in Sveta z dne 15. januarja 2013 o odobritvi in tržnem nadzoru dvo- ali trikolesnih vozil in štirikolesnikov (UL L 60, 2.3.2013, str. 52).

2. Ta uredba se uporablja od 11. decembra 2027.

Člen 14 pa se uporablja od 11. septembra 2026 in Poglavje IV (členi 35 do 51) od 11. junija 2026.

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

V Strasbourgu, 23. oktobra 2024

Za Evropski parlament	*Za Svet*
predsednica	*predsednik*
R. METSOLA	ZSIGMOND B. P.

PRILOGA I

BISTVENE ZAHTEVE GLEDE KIBERNETSKE VARNOSTI

Del I Zahteve glede kibernetske varnosti, ki se nanašajo na lastnosti izdelkov z digitalnimi elementi

(1) Izdelki z digitalnimi elementi so zasnovani, razviti in proizvedeni tako, da zagotavljajo ustrezno raven kibernetske varnosti glede na tveganja.

(2) Na podlagi ocene tveganja za kibernetsko varnost iz člena 13(2) in kadar je ustrezno, za izdelke z digitalnimi elementi velja naslednje:

(a) so dostopni na trgu brez znanih ranljivosti, ki jih je mogoče izrabljati;

(b) so dostopni na trgu s konfiguracijo po načelu privzete varnosti, razen če se proizvajalec in poslovni uporabnik v zvezi s prilagojenim izdelkom z digitalnimi elementi dogovorita drugače, vključno z možnostjo ponastavitve izdelka v prvotno stanje;

(c) zagotavljajo, da je ranljivosti mogoče odpraviti z varnostnimi posodobitvami, po potrebi tudi s samodejnimi varnostnimi posodobitvami, nameščenimi v ustreznem časovnem okviru v skladu s privzeto nastavitvijo, z jasnim in enostavnim mehanizmom za zavrnitev, ki je enostaven za uporabo, z obveščanjem uporabnikov o razpoložljivih posodobitvah in možnostjo začasne odložitve;

(d) z ustreznimi nadzornimi mehanizmi zagotavljajo zaščito pred nepooblaščenim dostopom, med drugim tudi s sistemi avtentikacije, upravljanja identitete ali upravljanja dostopa, ter poročajo o morebitnem nepooblaščenem dostopu;

(e) varujejo zaupnost shranjenih, prenesenih ali drugače obdelanih podatkov, osebnih ali drugih, na primer s šifriranjem zadevnih podatkov v mirovanju ali pri prenosu z najnovejšimi mehanizmi in z uporabo drugih tehničnih sredstev;

(f) varujejo celovitost shranjenih, prenesenih ali drugače obdelanih podatkov, osebnih ali drugih, ukazov, programov in nastavitev pred kakršnim koli poseganjem ali spreminjanjem, ki ga ne odobri uporabnik, ter poročajo o okvarah podatkov;

(g) obdelujejo le tiste podatke, osebne ali druge, ki so ustrezni, relevantni in omejeni na tisto, kar je potrebno glede na predvideni namen izdelka z digitalnimi elementi (najmanjši obseg podatkov);

(h) varujejo razpoložljivost ključnih in osnovnih funkcij, tudi po incidentu, vključno z odpornostjo proti napadom za zavrnitev storitve in ukrepi za zmanjšanje negativnih vplivov takih napadov;

(i) zmanjšujejo negativni vpliv samih izdelkov ali povezanih naprav na razpoložljivost storitev, ki jih zagotavljajo druge naprave ali omrežja;

(j) zasnovani, razviti in izdelani so tako, da se omejijo napadne površine, vključno z zunanjimi vmesniki;

(k) zasnovani, razviti in izdelani so tako, da se zmanjša vpliv incidenta z uporabo ustreznih mehanizmov in tehnik za zmanjšanje negativnih vplivov izrabljanja;

(l) zagotavljajo informacije, ki se nanašajo na varnost, in sicer z beleženjem in spremljanjem zadevnih internih dejavnosti, vključno z dostopom do podatkov, storitev ali funkcij ali njihovim spreminjanjem, z mehanizmom odklonitve za uporabnika;

(m) uporabnikom omogočajo, da varno in enostavno trajno odstranijo vse podatke in nastavitve ter, kadar je te podatke mogoče prenesti v druge izdelke ali sisteme, zagotovijo, da se to izvede na varen način.

Del II Zahteve glede obravnavanja ranljivosti

Proizvajalci izdelkov z digitalnimi elementi:

(1) opredelijo in dokumentirajo ranljivosti in sestavne dele izdelkov z digitalnimi elementi, vključno s pripravo kosovnice za programsko opremo v splošno uporabni in strojno berljivi obliki, ki vsebuje vsaj najpomembnejše odvisnosti izdelkov;

(2) brez odlašanja obravnavajo in odpravijo ranljivosti v zvezi s tveganji za izdelke z digitalnimi elementi, tudi z zagotavljanjem varnostnih posodobitev; kadar je to tehnično izvedljivo, se nove varnostne posodobitve zagotovijo ločeno od posodobitev funkcionalnosti;

(3) izvajajo učinkovita in redna preverjanja in preglede varnosti izdelkov z digitalnimi elementi;

(4) ko je na voljo varnostna posodobitev, delijo in javno razkrijejo informacije o odpravljenih ranljivostih, vključno z opisom ranljivosti, informacijami, ki uporabnikom omogočajo opredeliti prizadeti izdelek z digitalnimi elementi, vplivi ranljivosti, njihovo resnostjo ter jasnimi in dostopnimi informacijami, ki uporabnikom omogočajo odpravo ranljivosti; v ustrezno utemeljenih primerih, kadar proizvajalci menijo, da varnostna tveganja razkritja prevladajo nad varnostnimi koristmi, lahko odložijo razkritje informacij o odpravljeni ranljivosti, dokler uporabniki ne dobijo možnosti, da uporabijo ustrezni popravek;

(5) vzpostavijo in izvršujejo politiko usklajenega razkritja ranljivosti;

(6) sprejmejo ukrepe za lajšanje izmenjave informacije o potencialnih ranljivostih svojih izdelkov z digitalnimi elementi ter sestavnih delov tretjih oseb, ki jih taki izdelki vsebujejo, tudi z zagotavljanjem kontaktnega naslova za poročanje o odkritih ranljivostih v izdelkih z digitalnimi elementi;

(7) zagotovijo mehanizme za varno razširjanje posodobitev za izdelke z digitalnimi elementi, da se ranljivosti odpravijo ali zmanjšajo pravočasno in v primeru varnostnih posodobitev po potrebi samodejno;

(8) brez odlašanja in, kadar se proizvajalec in poslovni uporabnik v zvezi z izdelkom po meri z digitalnimi elementi ne dogovorita drugače, brezplačno zagotovijo razširjanje varnostnih posodobitev, kadar so ti na voljo za odpravo zaznanih varnostnih težav, ter jim priložijo nasvete za uporabnike z ustreznimi informacijami, tudi o morebitnih ukrepih, ki jih morajo ti sprejeti.

PRILOGA II

INFORMACIJE IN NAVODILA ZA UPORABNIKA

Ob izdelku z digitalnimi elementi se navedejo vsaj:

1. ime, registrirano trgovsko ime ali registrirana znamka proizvajalca, poštni naslov, elektronski naslov ali drug digitalni stik ter spletno mesto, na katerem je proizvajalec dosegljiv, kadar je na voljo;
2. enotna kontaktna točka, kjer je mogoče sporočiti in prejeti informacije o ranljivostih izdelka z digitalnimi elementi in kjer je mogoče najti politiko proizvajalca o usklajenem razkrivanju ranljivosti;
3. ime, vrsta in vse dodatne informacije, ki omogočajo edinstveno identifikacijo izdelka z digitalnimi elementi;
4. predvideni namen uporabe izdelka z digitalnimi elementi, vključno z varnostnim okoljem, ki ga zagotavlja proizvajalec, ter ključne funkcije in informacije o varnostnih lastnostih;
5. vse znane ali predvidljive okoliščine, povezane z uporabo izdelka z digitalnimi elementi v skladu z njegovim predvidenim namenom ali v razmerah razumno predvidljive napačne uporabe, ki lahko pripeljejo do povečanega tveganja za kibernetsko varnost;
6. kadar je ustrezno, spletni naslov, kjer je na voljo EU izjava o skladnosti;
7. vrsta tehnične varnostne podpore, ki jo ponuja proizvajalec, in končni datum obdobja podpore, v katerem lahko uporabniki pričakujejo odpravo ranljivosti in prejemanje varnostnih posodobitev;
8. podrobna navodila ali spletni naslov s takimi podrobnimi navodili in informacijami o:
   (a) potrebnih ukrepih v času začetne uporabe in v celotnem življenjskem ciklu izdelka z digitalnimi elementi, da se zagotovi njegova varna uporaba;
   (b) tem, kako lahko spremembe izdelka z digitalnimi elementi vplivajo na varnost podatkov;
   (c) nameščanju posodobitev, ki so pomembne za varnost;
   (d) varnem prenehanju uporabe izdelka z digitalnimi elementi, vključno z informacijami o varni odstranitvi podatkov o uporabniku.
   (e) kako se lahko izklopi privzeta nastavitev, ki omogoča samodejno namestitev varnostnih posodobitev, kot se zahteva v delu I, točka (c), Priloge I;
   (f) kadar je izdelek z digitalnimi elementi namenjen vgradnji v druge izdelke z digitalnimi elementi, informacije, ki jih integrator potrebuje za izpolnjevanje bistvenih zahtev glede kibernetske varnosti iz Priloge I, in zahteve glede dokumentacije iz Priloge VII.
9. Če se proizvajalec odloči, da bo uporabniku dal na voljo kosovnico za programsko opremo, informacije o tem, kje je mogoče dobiti dostop do te kosovnice.

PRILOGA III

POMEMBNI IZDELKI Z DIGITALNIMI ELEMENTI

Razred I

1. Programska oprema za sisteme za upravljanje identitete ter programska in strojna oprema za upravljanje privilegiranih dostopov, vključno z bralniki za avtentikacijo uporabnika in nadzor dostopa, vključno z biometričnimi bralniki
2. Samostojni in vgrajeni brskalniki
3. Upravitelji gesel
4. Programska oprema, ki išče, odstranjuje ali daje v karanteno zlonamerno programsko opremo
5. Izdelki z digitalnimi elementi s funkcijo navideznega zasebnega omrežja (VPN)
6. Sistemi za upravljanje omrežja
7. Varnostni sistemi za upravljanje informacij in dogodkov (SIEM)
8. Upravitelji zagona
9. Infrastruktura javnih ključev in programska oprema za izdajanje digitalnih certifikatov
10. Fizični in navidezni omrežni vmesniki
11. Operacijski sistemi
12. Usmerjevalniki, modemi, namenjeni povezovanju z internetom, in stikala
13. Mikroprocesorji z varnostnimi funkcijami
14. Mikrokrmilniki z varnostnimi funkcijami
15. Integrirana vezja za določen namen (ASIC) in programljive matrike logičnih vrat (FPGA) z varnostnimi funkcijami
16. Splošni virtualni pomočniki za pametni dom
17. Izdelki za pametni dom z varnostnimi funkcijami, vključno s pametnimi ključavnicami, varnostnimi kamerami, sistemi za spremljanje dojenčkov in alarmnimi sistemi
18. Z internetom povezane igrače, zajete v Direktivi 2009/48/ES Evropskega parlamenta in Sveta ([1]), ki imajo funkcije socialne interakcije (npr. govorjenje ali snemanje) ali imajo funkcije za sledenje lokaciji
19. Osebni nosljivi izdelki, ki so namenjeni nošenju ali namestitvi na človeško telo za namene spremljanja zdravja (kot je sledenje) in za katere se ne uporablja Uredba (EU) 2017/745 ali (EU) 2017/746, ali osebni nosljivi izdelki, namenjeni uporabi pri otrocih in za otroke

Razred II

1. Hipernadzorniki in izvajalni sistemi vsebnika, ki podpirajo virtualizirano delovanje operacijskih sistemov in podobnih okolij
2. Požarni zidovi, sistemi za zaznavanje in preprečevanje vdorov
3. Mikroprocesorji, zavarovani pred nepooblaščenimi posegi
4. Mikrokrmilniki, zavarovani pred nepooblaščenimi posegi

([1]) Direktiva 2009/48/ES Evropskega parlamenta in Sveta z dne 18. junija 2009 o varnosti igrač (UL L 170, 30.6.2009, str. 1).

PRILOGA IV

KRITIČNI IZDELKI Z DIGITALNIMI ELEMENTI

1. Naprave strojne opreme z varnostnimi napravami
2. Vstopne točke za napredne števce v sistemih naprednega merjenja, kot so opredeljeni v členu 2, točka 23, Direktive (EU) 2019/944 Evropskega parlamenta in Sveta ([1]), in druge naprave za napredne varnostne namene, tudi za varno obdelavo kriptosredstev
3. Pametne kartice ali podobne naprave, vključno z varnimi elementi

([1]) Direktiva (EU) 2019/944 Evropskega parlamenta in Sveta z dne 5. junija 2019 o skupnih pravilih notranjega trga električne energije in spremembi Direktive 2012/27/EU (UL L 158, 14.6.2019, str. 125).

PRILOGA V

EU IZJAVA O SKLADNOSTI

EU izjava o skladnosti iz člena 28 vsebuje vse naslednje informacije:

1. ime, vrsto in vse dodatne informacije, ki omogočajo edinstveno identifikacijo izdelka z digitalnimi elementi
2. ime in naslov proizvajalca ali njegovega pooblaščenega zastopnika
3. izjavo, da je za izdajo EU izjave o skladnosti odgovoren izključno proizvajalec
4. predmet izjave (identifikacija izdelka z digitalnimi elementi, ki omogoča sledljivost; kadar je ustrezno, se lahko priloži fotografija)
5. izjavo, da je predmet zgoraj navedene izjave skladen z ustrezno harmonizacijsko zakonodajo Unije
6. sklice na morebitne uporabljene ustrezne harmonizirane standarde ali druge skupne specifikacije ali certifikacijske sheme kibernetske varnosti, v zvezi s katerimi se zatrjuje skladnost
7. kadar je ustrezno, ime in številko priglašenega organa, opis opravljenega postopka ugotavljanja skladnosti in identifikacijo izdanega potrdila
8. dodatne informacije:

   Podpisano v imenu in za račun:

   (kraj in datum izdaje):

   (ime, funkcija) (podpis):

PRILOGA VI

POENOSTAVLJENA EU IZJAVA O SKLADNOSTI

Poenostavljena EU izjava o skladnosti iz člena 13(20) se predloži na naslednji način:

… [ime proizvajalca] izjavlja, da je izdelek z digitalnimi elementi … [oznaka tipa izdelka z digitalnim elementom] skladen z Uredbo (EU) 2024/2847 ([1]).

Celotno besedilo EU izjave o skladnosti je na voljo na naslednjem spletnem naslovu: …

([1]) UL L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

PRILOGA VII

VSEBINA TEHNIČNE DOKUMENTACIJE

Tehnična dokumentacija iz člena 31 vsebuje vsaj naslednje informacije, kakor velja za zadevni izdelek z digitalnimi elementi:

1. splošni opis izdelka z digitalnimi elementi, ki vključuje:
   (a) njegov predvideni namen;
   (b) različice programske opreme, ki vplivajo na skladnost z bistvenimi zahtevami glede kibernetske varnosti;
   (c) kadar je izdelek z digitalnimi elementi izdelek strojne opreme, fotografije ali ilustracije, ki prikazujejo zunanje značilnosti, oznake in notranjo razporeditev;
   (d) informacije za uporabnika in navodila, kakor so navedena v Prilogi II;
2. opis zasnove, razvoja in proizvodnje izdelka z digitalnimi elementi ter postopkov obravnavanja ranljivosti, ki vključuje:
   (a) potrebne informacije o zasnovi in razvoju izdelka z digitalnimi elementi, vključno z, kadar je ustrezno, risbami in shemami in opisom strukture sistema, iz katerega izhaja, kako sestavni deli programske opreme temeljijo drug na drugem oziroma kako se dopolnjujejo ter kako se vključujejo v celotno delovanje;
   (b) potrebne informacije in specifikacije postopkov obravnavanja ranljivosti, ki jih je vzpostavil proizvajalec, vključno s kosovnico za programsko opremo, usklajeno politiko razkrivanja ranljivosti, dokazilom o zagotavljanju kontaktnega naslova za poročanje o ranljivostih ter opisom tehničnih rešitev, izbranih za varno razširjanje posodobitev;
   (c) potrebne informacije in specifikacije postopkov proizvodnje in spremljanja izdelka z digitalnimi elementi ter preverjanja teh postopkov;
3. oceno tveganja za kibernetsko varnost, ki je upoštevana pri zasnovi, razvoju, proizvodnji, dobavi in vzdrževanju izdelka z digitalnimi elementi na podlagi člena 13, vključno s tem, kako se uporabljajo bistvene zahteve glede kibernetske varnosti iz dela I Priloge I;
4. ustrezne informacije, ki so bile upoštevane pri določitvi obdobja podpore na podlagi člena 13(8) izdelka z digitalnimi elementi;
5. Seznam harmoniziranih standardov, ki se uporabljajo v celoti ali delno in katerih sklici so bili objavljeni v *Uradnem listu Evropske unije*, skupnih specifikacij, kakor so določene v členu 27 te uredbe, ali evropskih certifikacijskih shem kibernetske varnost, sprejetih na podlagi Uredba (EU) 2019/881 na podlagi člena 27(8) te uredbe ter, kadar ti harmonizirani standardi, skupne specifikacije ali evropske certifikacijske sheme kibernetske varnosti niso bili uporabljeni, opis rešitev, sprejetih za izpolnitev bistvenih zahtev glede kibernetske varnosti iz delov I in II Priloge I, vključno s seznamom drugih ustreznih tehničnih specifikacij, ki so bile uporabljene. V primeru delne uporabe harmoniziranih standardov, skupnih specifikacij ali evropskih certifikacijskih shem kibernetske varnosti se v tehnični dokumentaciji navedejo deli, ki so bili uporabljeni;
6. poročila o preskusih, opravljenih za preverjanje skladnosti izdelka in postopkov obravnavanja ranljivosti z veljavnimi bistvenimi zahtevami glede kibernetske varnosti, kakor so določene v delih I in II Priloge I;
7. izvod EU izjave o skladnosti;
8. kadar je ustrezno, kosovnico za programsko opremo na podlagi obrazložene zahteve organa za nadzor trga, če je to potrebno, da lahko navedeni organ preveri skladnost z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I.

PRILOGA VIII

POSTOPKI UGOTAVLJANJA SKLADNOSTI

Del I Postopek ugotavljanja skladnosti, ki temelji na notranjem nadzoru (na podlagi modula A)

1. Notranji nadzor je postopek ugotavljanja skladnosti, pri katerem proizvajalec izpolni obveznosti iz točk 2, 3 in 4 tega dela ter zagotovi in na podlagi izključne odgovornosti izjavi, da izdelki z digitalnimi elementi izpolnjujejo vse bistvene zahteve glede kibernetske varnosti iz dela I Priloge I ter da proizvajalec izpolnjuje bistvene zahteve glede kibernetske varnosti iz dela II Priloge I.

2. Proizvajalec pripravi tehnično dokumentacijo, navedeno v Prilogi VII.

3. Zasnova, razvoj, proizvodnja in obravnavanje ranljivosti izdelkov z digitalnimi elementi

   Proizvajalec sprejme vse potrebne ukrepe, da postopki zasnove, razvoja, proizvodnje in obravnavanja ranljivosti ter njihovo spremljanje zagotavljajo skladnost izdelanih ali razvitih izdelkov z digitalnimi elementi in postopkov, ki jih je vzpostavil proizvajalec, z bistvenimi zahtevami glede kibernetske varnosti iz delov I in II Priloge I.

4. Oznaka skladnosti in izjava o skladnosti

   4.1 Proizvajalec na vsak posamezen izdelek z digitalnimi elementi, ki izpolnjuje veljavne zahteve določene v tej uredbi, namesti oznako CE.

   4.2 Proizvajalec za vsak izdelek z digitalnimi elementi pripravi pisno EU izjavo o skladnosti v skladu s členom 28 in jo za nacionalne organe skupaj s tehnično dokumentacijo hrani še deset let po tem, ko je bil izdelek z digitalnimi elementi dan na trg, ali v obdobju podpore, pri čemer se upošteva daljše obdobje. V EU izjavi o skladnosti se opredeli izdelek z digitalnimi elementi, za katerega je bila pripravljena. Na zahtevo se pristojnim organom predloži izvod EU izjave o skladnosti.

5. Pooblaščeni zastopniki

   Obveznosti proizvajalca iz točke 4 lahko v njegovem imenu in na njegovo odgovornost izpolni pooblaščeni zastopnik, pod pogojem, da so zadevne obveznosti navedene v pooblastilu.

Del II EU-pregled tipa (na podlagi modula B)

1. EU-pregled tipa je del postopka ugotavljanja skladnosti, pri katerem priglašeni organ pregleda tehnično zasnovo in razvoj izdelka z digitalnimi elementi ter postopke obravnavanja ranljivosti, ki jih je vzpostavil proizvajalec, ter potrdi, da izdelek z digitalnimi elementi izpolnjuje bistvene zahteve glede kibernetske varnosti iz dela I Priloge I, in da proizvajalec izpolnjuje bistvene zahteve glede kibernetske varnosti iz dela II Priloge I.

2. EU-pregled tipa se izvede z ugotavljanjem ustreznosti tehnične zasnove in razvoja izdelka z digitalnimi elementi s pregledom tehnične dokumentacije in dodatnih dokazil iz točke 3 ter s pregledom vzorcev enega ali več kritičnih delov izdelka (kombinacija tipa proizvodnje in tipa zasnove).

3. Proizvajalec vloži vlogo za EU-pregled tipa pri enem priglašenem organu po svoji izberi.

   Vloga vsebuje:

   3.1 ime in naslov proizvajalca ter, če je zahtevek vložil pooblaščeni zastopnik, ime in naslov tega pooblaščenega zastopnika;

   3.2 pisno izjavo, da enaka vloga ni bila vložena pri nobenem drugem priglašenem organu;

   3.3 tehnično dokumentacijo, ki omogoča ugotavljanje skladnosti izdelka z digitalnimi elementi z veljavnimi bistvenimi zahtevami glede kibernetske varnosti, kakor so določene v delu I Priloge I, in proizvajalčevih postopkov obravnavanja ranljivosti, kot je določeno v delu II Priloge I, ter vključuje ustrezno analizo in oceno tveganj. Tehnična dokumentacija opredeljuje veljavne zahteve in vključuje, če je to pomembno za ugotavljanje skladnosti, zasnovo, izdelavo in delovanje izdelka z digitalnimi elementi. Če je ustrezno, tehnična dokumentacija vsebuje vsaj elemente iz Priloge VII;

3.4 dodatna dokazila glede ustreznosti tehnične zasnove in razvojnih rešitev ter postopkov obravnavanja ranljivosti. V teh dodatnih dokazilih so navedeni vsi uporabljeni dokumenti, zlasti kadar ustrezni harmonizirani standardi ali tehnične specifikacije niso bili uporabljeni v celoti. Dodatna dokazila, kadar je potrebno, po potrebi vključujejo rezultate preskusov, ki jih je izvedel ustrezni laboratorij proizvajalca ali drug preskuševalni laboratorij v njegovem imenu in na njegovo odgovornost.

4. Priglašeni organ:

4.1 pregleda tehnično dokumentacijo in dodatna dokazila, da oceni ustreznost tehnične zasnove in razvoja izdelka z digitalnimi elementi glede na bistvene zahteve glede kibernetske varnosti iz dela I Priloge I ter postopkov obravnavanja ranljivosti, ki jih je vzpostavil proizvajalec, glede na bistvene zahteve glede kibernetske varnosti iz dela II Priloge I;

4.2 preveri, ali so bili vzorci razviti ali izdelani v skladu s tehnično dokumentacijo, ter določi elemente, ki so bili zasnovani in razviti v skladu z veljavnimi določbami ustreznih harmoniziranih standardov ali tehničnih specifikacij, pa tudi elemente, ki so bili zasnovani in razviti, ne da bi bile upoštevane ustrezne določbe navedenih standardov;

4.3 izvede ali naroči ustrezne preglede in preskuse, s katerimi preveri, ali je proizvajalec, kadar se je odločil za uporabo rešitev iz ustreznih harmoniziranih standardov ali tehničnih specifikacij za zahteve iz Priloge I, te pravilno upošteval;

4.4 izvede ali naroči ustrezne preglede in preskuse, s katerimi preveri, ali v primeru neuporabe rešitev iz ustreznih harmoniziranih standardov ali tehničnih specifikacij za zahteve iz Priloge I, rešitve, ki jih je uporabil proizvajalec, izpolnjujejo ustrezne bistvene zahteve glede kibernetske varnosti;

4.5 se dogovori z proizvajalcem o kraju, kjer bodo opravljeni pregledi in preskusi.

5. Priglašeni organ sestavi poročilo o ocenjevanju, ki vsebuje dejavnosti, opravljene v skladu s točko 4, in njihove rezultate. Brez poseganja v obveznosti do priglasitvenih organov priglašeni organ objavi vsebino navedenega poročila v celoti ali delno le v dogovoru z proizvajalcem.

6. Kadar tip in postopki obravnavanja ranljivosti izpolnjujejo bistvene zahteve glede kibernetske varnosti iz Priloge I, priglašeni organ proizvajalcu izda potrdilo o EU-pregledu tipa. Potrdilo vsebuje ime in naslov proizvajalca, ugotovitve pregleda, pogoje (če obstajajo) njegove veljavnosti in potrebne podatke za identifikacijo odobrenega tipa in postopka obravnavanja ranljivosti. Potrdilu je lahko priložena ena ali več prilog.

Potrdilo in njegove priloge vsebujejo vse potrebne informacije, da se lahko ocenijo skladnost izdelanih ali razvitih izdelkov z digitalnimi elementi s preskušenim tipom in postopki obravnavanja ranljivosti ter omogoči nadzor med uporabo.

Kadar tip in postopki obravnavanja ranljivosti ne izpolnjujejo veljavnih bistvenih zahtev glede kibernetske varnosti iz Priloge I, priglašeni organ zavrne izdajo potrdila o EU-pregledu tipa in o tem obvesti vložnika s podrobno utemeljitvijo zavrnitve.

7. Priglašeni organ spremlja spremembe v splošno priznanem najnovejšem tehnološkem razvoju, iz katerih izhaja, da odobreni tip in postopki obravnavanja ranljivosti ne izpolnjujejo več veljavnih bistvenih zahtev glede kibernetske varnosti iz Priloge I, ter določi, ali je zaradi takih sprememb potrebna nadaljnja preiskava. V takem primeru priglašeni organ o tem obvesti proizvajalca.

Proizvajalec obvesti priglašeni organ, ki hrani tehnično dokumentacijo o potrdilu o EU-pregledu tipa, o vseh spremembah odobrenega tipa in postopkov obravnavanja ranljivosti, ki bi lahko vplivali na skladnost z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I ali s pogoji veljavnosti potrdila. Take spremembe zahtevajo dodatno odobritev v obliki dodatka k izvirnemu potrdilu o EU-pregledu tipa.

8. Priglašeni organ izvaja redne presoje skladnosti, da zagotovi ustrezno izvajanje postopkov obravnavanja ranljivosti iz dela II Priloge I.

9. Vsak priglašeni organ obvesti svoje priglasitvene organe o izdanih ali preklicanih potrdilih o EU-pregledu tipa in dodatkih k takim potrdilom ter redno ali na zahtevo da na voljo priglasitvenim organom seznam zavrnjenih, začasno preklicanih ali drugače omejenih potrdil in njihovih dodatkov.

   Vsak priglašeni organ obvesti druge priglašene organe o zavrnjenih, umaknjenih, začasno preklicanih ali drugače omejenih potrdilih o EU-pregledu tipa in dodatkih k takim potrdilom ter jih na zahtevo obvesti o izdanih potrdilih in njihovih dodatkih.

   Komisija, države članice in drugi priglašeni organi lahko na zahtevo dobijo izvode potrdil o EU-pregledu tipa in njihovih dodatkov. Komisija in države članice lahko na zahtevo dobijo izvod tehnične dokumentacije in rezultate pregledov, ki jih je izvedel priglašeni organ. Priglašeni organ hrani izvod potrdila o EU-pregledu tipa, njegovih prilog in dodatkov ter tehnični spis, vključno z dokumentacijo, ki jo predloži proizvajalec, do izteka veljavnosti potrdila.

10. Še deset let po tem, ko je bil izdelek z digitalnimi elementi dan na trg ali v obdobju podpore, pri čemer se upošteva daljše obdobje, proizvajalec nacionalnim organom zagotavlja izvod potrdila o EU-pregledu tipa, njegovih prilog in dodatkov, vključno s tehnično dokumentacijo.

11. Pooblaščeni zastopnik proizvajalca lahko vloži vlogo iz točke 3 ter izpolni obveznosti iz točk 7 in 10, če so zadevne obveznosti navedene v pooblastilu.

Del III Skladnost s tipom na podlagi notranje kontrole proizvodnje (na podlagi modula C)

1. Skladnost s tipom na podlagi notranje kontrole proizvodnje je del postopka ugotavljanja skladnosti, s katerim proizvajalec izpolni obveznosti iz točk 2 in 3 tega dela ter zagotovi in izjavi, da so zadevni izdelki z digitalnimi elementi v skladu s tipom, opisanim v potrdilu o EU-pregledu tipa, in da izpolnjujejo bistvene zahteve glede kibernetske varnosti iz dela I Priloge I ter da proizvajalec izpolnjuje bistvene zahteve glede kibernetske varnosti iz dela II Priloge I.

2. Proizvodnja

   Proizvajalec sprejme vse potrebne ukrepe, da se v proizvodnji in njenem spremljanju zagotovi skladnost izdelanih izdelkov z digitalnimi elementi z odobrenim tipom, opisanim v potrdilu o EU-pregledu tipa, in z bistvenimi zahtevami glede kibernetske varnosti iz dela I Priloge I ter zagotovi, da proizvajalec izpolnjuje bistvene zahteve glede kibernetske varnosti iz dela II Priloge I.

3. Oznaka skladnosti in izjava o skladnosti

   3.1 Proizvajalec namesti oznako CE na vsak posamezni izdelek z digitalnimi elementi, ki je skladen s tipom, opisanim v potrdilu o EU-pregledu tipa, in izpolnjuje veljavne zahteve določene v tej uredbi.

   3.2 Proizvajalec za vzorčni izdelek sestavi pisno izjavo o skladnosti in nacionalnim organom omogoča dostop do nje še deset let po tem, ko je bil izdelek z digitalnimi elementi dan na trg ali v obdobju podpore, pri čemer se upošteva daljše obdobje. V izjavi o skladnosti je opredeljen vzorčni izdelek, za katerega je bila pripravljena. Na zahtevo se pristojnim organom predloži izvod izjave o skladnosti.

4. Pooblaščeni zastopnik

   Obveznosti proizvajalca iz točke 3 lahko v njegovem imenu in na njegovo odgovornost izpolni pooblaščeni zastopnik, pod pogojem, da so zadevne obveznosti navedene v pooblastilu.

Del IV Skladnost na podlagi popolnega zagotavljanja kakovosti (na podlagi modula H)

1. Skladnost na podlagi popolnega zagotavljanja kakovosti je postopek ugotavljanja skladnosti, pri katerem proizvajalec izpolni obveznosti določene v točkah 2 in 5 tega dela ter zagotovi in na podlagi izključne odgovornosti izjavi, da zadevni izdelki z digitalnimi elementi ali kategorije izdelkov izpolnjujejo bistvene zahteve glede kibernetske varnosti iz dela I Priloge I, ter da postopki obravnavanja ranljivosti, ki jih je vzpostavil proizvajalec, izpolnjujejo zahteve iz dela II Priloge I.

2. Zasnova, razvoj, proizvodnja in obravnavanje ranljivosti izdelkov z digitalnimi elementi

Proizvajalec glede zasnove, razvoja in pregleda končnega izdelka in preizkušanja zadevnih izdelkov z digitalnimi elementi ter obravnavanja ranljivosti uporablja odobren sistem kakovosti, kot je določen v točki 3, vzdržuje njegovo učinkovitost v celotnem obdobju podpore in se podredi nadzoru, kot je določen v točki 4.

3. Sistem kakovosti

3.1 Proizvajalec vloži vlogo za oceno svojega sistema kakovosti v zvezi z zadevnimi izdelki z digitalnimi elementi pri priglašenem organu, ki ga sam izbere.

Vloga vsebuje:

(a) ime in naslov proizvajalca in, če vlogo vloži pooblaščeni zastopnik, ime in naslov tega pooblaščenega zastopnika;

(b) tehnično dokumentacijo za en model iz vsake kategorije izdelkov z digitalnimi elementi, ki bodo izdelani ali razviti. Če je ustrezno, tehnična dokumentacija vsebuje vsaj elemente iz Priloge VII;

(c) dokumentacijo o sistemu kakovosti ter

(d) pisno izjavo, da enaka vloga ni bila vložena pri nobenem drugem priglašenem organu.

3.2 S sistemom kakovosti se zagotovi skladnost izdelkov z digitalnimi elementi z bistvenimi zahtevami glede kibernetske varnosti iz dela I Priloge I, ter skladnost postopkov obravnavanja ranljivosti, ki jih je vzpostavil proizvajalec, z zahtevami iz dela II Priloge I.

Vsi elementi, zahteve in predpisi, ki jih je sprejel proizvajalec, se sistematično in urejeno pisno dokumentirajo v obliki politik, postopkov in navodil. Navedena dokumentacija o sistemu kakovosti omogoča dosledno razlago programov, načrtov, priročnikov in zapisov o kakovosti.

Zlasti vsebuje ustrezen opis:

(a) ciljev kakovosti in organizacijske strukture, odgovornosti in pristojnosti vodstva glede zasnove, razvoja, kakovosti izdelkov in obravnavanja ranljivosti;

(b) tehničnih specifikacij zasnove in razvoja, vključno s standardi, ki se bodo uporabljali, in kadar se ustrezni harmonizirani standardi in/ali tehnične specifikacije ne bodo uporabljali v celoti, sredstev, ki se bodo uporabljala za zagotavljanje izpolnjevanja bistvenih zahtev glede kibernetske varnosti iz dela I Priloge I, ki se uporabljajo za izdelke z digitalnimi elementi;

(c) postopkovnih specifikacij, vključno s standardi, ki se bodo uporabljali, in kadar se ustrezni harmonizirani standardi ali tehnične specifikacije ne bodo uporabljali v celoti, sredstev, ki se bodo uporabljala za zagotavljanje izpolnjevanja bistvenih zahtev glede kibernetske varnosti iz dela II Priloge I, ki se uporabljajo za proizvajalca;

(d) nadzora zasnove in razvoja ter tehnik, postopkov in sistematičnih ukrepov za preverjanje zasnove in razvoja, ki se bodo uporabljali pri zasnovi in razvoju izdelkov z digitalnimi elementi, ki spadajo v zadevno kategorijo izdelkov;

(e) ustreznih tehnik, postopkov in sistematičnih ukrepov glede proizvodnje, nadzora kakovosti in zagotavljanja kakovosti, ki se bodo uporabljali,

(f) pregledov in preskusov, ki se bodo izvajali pred in med proizvodnjo ter po njej, ter pogostnosti njihovega izvajanja;

(g) zapisov o kakovosti, kakor so poročila o pregledu in podatki o preskusih, podatki o umerjanju opreme in poročila o strokovni usposobljenosti zadevnega osebja;

(h) načinov spremljanja doseganja zahtevane kakovosti zasnove in izdelkov ter učinkovitega delovanja sistema kakovosti.

3.3 Priglašeni organ oceni sistem kakovosti, da ugotovi, ali izpolnjuje zahteve iz točke 3.2.

Ta organ domneva, da so elementi sistema kakovosti, ki so v skladu z ustreznimi specifikacijami nacionalnega standarda, s katerim se izvaja ustrezni harmonizirani standard ali tehnična specifikacija, skladni z navedenimi zahtevami.

Skupina za presojo ima poleg izkušenj s sistemi vodenja kakovosti vsaj enega člana, ki ima izkušnje z ocenjevanjem na ustreznem področju izdelkov in zadevne tehnologije izdelkov ter pozna veljavne zahteve iz te uredbe. Presoja vključuje ocenjevalni obisk prostorov proizvajalca, kadar ti obstajajo. Skupina za presojo pregleda tehnično dokumentacijo iz točke 3.1(b), da ugotovi, ali je proizvajalec zmožen opredeliti veljavne zahteve iz te uredbe in izvesti potrebne preglede za zagotovitev skladnosti izdelka z digitalnimi elementi s temi zahtevami.

Proizvajalec ali njegov pooblaščeni zastopnik je obveščen o odločitvi.

Obvestilo vsebuje rezultate presoje in obrazložitev odločitve o oceni.

3.4 Proizvajalec se zavezuje izpolnjevati obveznosti, ki izhajajo iz odobrenega sistema kakovosti, ter vzdrževati sistem kakovosti tako, da ostane ustrezen in učinkovit.

3.5 Proizvajalec obvešča priglašeni organ, ki je odobril sistem kakovosti, o vseh načrtovanih spremembah sistema kakovosti.

Priglašeni organ oceni predlagane spremembe in se odloči, ali bo spremenjeni sistem kakovosti še naprej izpolnjeval zahteve iz točke 3.2 ali pa je potrebna ponovna ocena.

O svoji odločitvi obvesti izvajalca. Obvestilo vsebuje ugotovitve pregleda in utemeljitev odločitve o oceni.

4. Nadzor, za katerega je odgovoren priglašeni organ

4.1 Namen nadzora je zagotoviti, da proizvajalec ustrezno izpolnjuje obveznosti, ki izhajajo iz odobrenega sistema kakovosti.

4.2 Proizvajalec priglašenemu organu za namene ocene omogoči vstop v prostore za zasnovo, razvoj, proizvodnjo, pregled, preskušanje in skladiščenje ter mu zagotovi vse potrebne informacije, zlasti:

(a) dokumentacijo o sistemu kakovosti;

(b) zapise o kakovosti iz tistega dela sistema kakovosti, ki se nanaša na zasnovo, kakor so rezultati analiz, izračunov in preskusov;

(c) zapise o kakovosti iz tistega dela sistema kakovosti, ki se nanaša na izdelavo, kakor so poročila o pregledu in podatki o preskusih, podatki o umerjanjih opreme ter poročila o strokovni usposobljenosti zadevnega osebja.

4.3 Priglašeni organ redno izvaja presoje, s čimer zagotavlja, da proizvajalec vzdržuje in uporablja sistem kakovosti, ter proizvajalcu izda poročilo o presoji.

5. Oznaka skladnosti in izjava o skladnosti

5.1 Proizvajalec namesti oznako CE in na podlagi odgovornosti priglašenega organa iz točke 3.1 njegovo identifikacijsko številko na vsak posamezni izdelek z digitalnimi elementi, ki izpolnjuje zahteve iz dela I Priloge I.

5.2 Proizvajalec za vsak vzorčni izdelek sestavi pisno izjavo o skladnosti in nacionalnim organom omogoča dostop do nje še deset let po tem, ko je bil izdelek z digitalnimi elementi dan na trg ali v obdobju podpore, pri čemer se upošteva daljše obdobje. V izjavi o skladnosti je opredeljen vzorčni izdelek, za katerega je bila pripravljena.

Na zahtevo se pristojnim organom predloži izvod izjave o skladnosti.

6. Še deset let po tem, ko je izdelek z digitalnimi elementi dan na trg ali v obdobju podpore, pri čemer se upošteva daljše obdobje, proizvajalec zagotavlja, da so nacionalnim organom na voljo:

(a) tehnična dokumentacija iz točke 3.1;

(b) dokumentacija o sistemu kakovosti iz točke 3.1;

(c) sprememba iz točke 3.5, kakor je bila odobrena;

(d) odločbe in poročila priglašenega organa iz točk 3.5 in 4.3.

7. Vsak priglašeni organ obvesti svoje priglasitvene organe o izdanih ali preklicanih odobritvah sistema kakovosti in redno ali na zahtevo zagotavlja svojim priglasitvenim organom seznam zavrnjenih, začasno preklicanih ali drugače omejenih odobritev sistema kakovosti.

Vsak priglašeni organ obvesti druge priglašene organe o odobritvah sistema kakovosti, ki jih je zavrnil, začasno preklical ali preklical, ter jih na zahtevo obvesti o odobritvah sistema kakovosti, ki jih je izdal.

8. Pooblaščeni zastopnik

Obveznosti proizvajalca iz točk 3.1, 3.5, 5 in 6 lahko v njegovem imenu in na njegovo odgovornost izpolni pooblaščeni zastopnik, če so zadevne obveznosti navedene v pooblastilu.

V zvezi s tem aktom je bila podana izjava, ki je na voljo v UL C, 2024/6786, 20.11.2024, ELI: http://data.europa.eu/eli/C/2024/6786/oj.