Svet
Evropske unije

Bruselj, 16. september 2022
(OR. en)

12429/22

Medinstitucionalna zadeva:
2022/0272 (COD)

CYBER 298
JAI 1181
DATAPROTECT 254
TELECOM 369
MI 665
CSC 388
CSCI 133
CODEC 1310
IA 133

PREDLOG

Pošiljatelj:	za generalno sekretarko Evropske komisije: direktorica Martine DEPREZ
Datum prejema:	15. september 2022
Prejemnik:	Thérèse BLANCHET, generalna sekretarka Sveta Evropske unije
Št. dok. Kom.:	COM(2022) 454 final
Zadeva:	Predlog UREDBE EVROPSKEGA PARLAMENTA IN SVETA o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi Uredbe (EU) 2019/1020

Delegacije prejmejo priloženi dokument COM(2022) 454 final.

Priloga: COM(2022) 454 final

EVROPSKA
KOMISIJA

Bruselj, 15.9.2022
COM(2022) 454 final

2022/0272 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi Uredbe (EU) 2019/1020

(Besedilo velja za EGP)

{SEC(2022) 321 final} - {SWD(2022) 282 final} - {SWD(2022) 283 final}

OBRAZLOŽITVENI MEMORANDUM

1. OZADJE PREDLOGA

• Razlogi za predlog in njegovi cilji

Izdelki strojne in programske opreme so vse pogosteje tarča uspešnih kibernetskih napadov, zaradi katerih so letni stroški kibernetske kriminalitete na svetovni ravni do leta 2021 po ocenah znašali 5,5 bilijona EUR. Pri takih izdelkih obstajata dve glavni težavi, zaradi katerih imajo uporabniki in družba dodatne stroške: (1) nizka raven kibernetske varnosti, ki se odraža v splošno razširjenih ranljivostih ter nezadostnem in nedoslednem zagotavljanju varnostnih posodobitev za njihovo odpravljanje, ter (2) nezadostno razumevanje in nezadosten dostop uporabnikov do informacij, ki preprečujeta izbiro izdelkov z ustreznimi lastnostmi kibernetske varnosti ali njihovo varno uporabo. Kibernetski incident pri enem izdelku lahko v povezanem okolju vpliva na celotno organizacijo ali celotno oskrbovalno verigo, pri čemer se pogosto v nekaj minutah razširi čez meje notranjega trga. To lahko povzroči resne motnje v gospodarskih in družbenih dejavnostih ali celo postane življenjsko ogrožajoče.

Kibernetska varnost izdelkov z digitalnimi elementi ima jasno čezmejno razsežnost, saj se izdelki, izdelani v eni državi, pogosto uporabljajo na celotnem notranjem trgu. Poleg tega se incidenti, ki prvotno prizadenejo posamezen subjekt ali državo članico, pogosto v nekaj minutah razširijo na celotni notranji trg.

Čeprav se sedanja zakonodaja o notranjem trgu uporablja za nekatere izdelke z digitalnimi elementi, večina izdelkov strojne in programske opreme trenutno ni vključenih v nobeno zakonodajo EU, ki bi obravnavala njihovo kibernetsko varnost. Zlasti sedanji pravni okvir EU ne obravnava kibernetske varnosti nevgrajene programske opreme, čeprav so kibernetski napadi čedalje pogosteje usmerjeni v ranljivosti teh izdelkov ter povzročajo precejšnje družbene in ekonomske stroške. Primerov omembe vrednih kibernetskih napadov, ki so bili posledica pomanjkljive varnosti izdelkov, je veliko, na primer napad s črvom izsiljevalskega programja WannaCry leta 2017, ki je izrabil ranljivost operacijskega sistema Windows, prizadel 200 000 računalnikov v 150 državah in povzročil škodo v višini več milijard ameriških dolarjev, napad na oskrbovalno verigo Kaseya VSA, pri katerem je bila uporabljena programska oprema podjetja Kaseya za upravljanje omrežja za napad na več kot 1 000 podjetij, veriga supermarketov pa je bila prisiljena zapreti vseh svojih 500 trgovin po vsej Švedski, ter številni incidenti z vdori v aplikacije za bančništvo, pri katerih se ukrade denar nič hudega slutečim potrošnikom.

Določena sta bila dva glavna cilja za zagotovitev ustreznega delovanja notranjega trga: (1) ustvariti pogoje za razvoj varnih izdelkov z digitalnimi elementi z zagotavljanjem, da se na trg dajejo izdelki strojne in programske opreme z manj ranljivostmi in da proizvajalci v celotnem življenjskem ciklu izdelka resno obravnavajo vprašanje varnosti, ter (2) ustvariti pogoje, ki uporabnikom omogočajo upoštevanje kibernetske varnosti pri izbiri in uporabi izdelkov z digitalnimi elementi. Oblikovani so bili štirje specifični cilji: (i) zagotoviti, da proizvajalci izboljšujejo varnost izdelkov z digitalnimi elementi že od faze zasnove in razvoja ter v celotnem življenjskem ciklu izdelka; (ii) zagotoviti skladen okvir kibernetske varnosti, s čimer se olajša zagotavljanje skladnosti za proizvajalce strojne in programske opreme; (iii) izboljšati preglednost varnostnih lastnosti izdelkov z digitalnimi elementi ter (iv) podjetjem in potrošnikom omogočiti varno uporabo izdelkov z digitalnimi elementi.

Očitno čezmejna narava kibernetske varnosti in vse večje število incidentov, katerih učinki segajo čez meje, v razne sektorje in izdelke, pomenita, da države članice ne morejo same

učinkovito doseči navedenih ciljev. Glede na globalno naravo trga izdelkov z digitalnimi elementi se države članice na svojih ozemljih spoprijemajo z istimi tveganji glede istih izdelkov z digitalnimi elementi. Nastajajoči neenotni okvir potencialno različnih nacionalnih pravil lahko ogrozi odprt in konkurenčen enotni trg izdelkov z digitalnimi elementi. Zato je potrebno skupno ukrepanje na ravni EU, da se povečata zaupanje med uporabniki in privlačnost izdelkov z digitalnimi elementi iz EU. To bi tudi koristilo notranjemu trgu, saj bi zagotavljalo pravno varnost in enake konkurenčne pogoje za prodajalce izdelkov z digitalnimi elementi, kakor je poudarjeno tudi v končnem poročilu Konference o prihodnosti Evrope, v katerem državljani zahtevajo večjo vlogo EU pri preprečevanju kibernetskih groženj.

- **Medsebojni vpliv z veljavnimi predpisi s področja zadevne politike**

Okvir EU vključuje več aktov horizontalne zakonodaje, ki zajemajo določene vidike, povezane s kibernetsko varnostjo, z različnih zornih kotov (izdelki, storitve, krizno upravljanje in kazniva dejanja). Leta 2013 je začela veljati direktiva o napadih na informacijske sisteme[1], s katero so bile harmonizirane inkriminacija in kazni za več kaznivih dejanj zoper informacijske sisteme. Avgusta 2016 je začela veljati Direktiva (EU) 2016/1148 o varnosti omrežij in informacijskih sistemov[2] kot prvi zakonodajni akt o kibernetski varnosti na ravni EU. Z njeno revizijo, na podlagi katere je bila pripravljena Direktiva [Direktiva XXX/XXXX (NIS2)], se zvišuje raven ambicije na ravni EU. Leta 2019 je začel veljati akt EU o kibernetski varnosti[3], katerega namen je izboljšati varnost izdelkov IKT, storitev IKT in postopkov IKT z uvedbo prostovoljnega evropskega certifikacijskega okvira za kibernetsko varnost[4].

Kibernetska varnost celotne oskrbovalne verige je zagotovljena le, če so kibernetsko varni vsi njeni sestavni deli. Navedena zakonodaja EU pa vključuje precejšnje vrzeli v zvezi s tem, saj ne vključuje obveznih zahtev za varnost izdelkov z digitalnimi elementi.

Medtem ko predlagani akt o kibernetski odpornosti vključuje izdelke z digitalnimi elementi, danimi na trg, je Direktiva [Direktiva XXX/XXX (NIS2)] namenjena zagotovitvi visoke ravni kibernetske varnosti storitev, ki jih opravljajo bistveni in pomembni subjekti. V skladu z Direktivo [Direktiva XXX/XXXX (NIS2)] morajo države članice zagotoviti, da bistveni in pomembni subjekti, ki spadajo na področje uporabe Direktive, kakor so izvajalci zdravstvene dejavnosti ali ponudniki storitev v oblaku in subjekti javne uprave, sprejmejo ustrezne in sorazmerne tehnične, operativne in organizacijske ukrepe za kibernetsko varnost. To med drugim vključuje zahtevo za zagotovitev varnosti pri pridobivanju, razvoju in vzdrževanju omrežij in informacijskih sistemov, vključno z obravnavanjem in razkrivanjem ranljivosti. V skladu z Direktivo [Direktiva XXX/XXXX (NIS2)] mora Komisija v 21 mesecih od datuma začetka veljavnosti te direktive za nekatere vrste subjektov, kakor so ponudniki storitev računalništva v oblaku, sprejeti izvedbene akte za določitev tehničnih in metodoloških zahtev

---

1 Direktiva 2013/40/EU Evropskega parlamenta in Sveta z dne 12. avgusta 2013 o napadih na informacijske sisteme in nadomestitvi Okvirnega sklepa Sveta 2005/222/PNZ (UL L 218, 14.8.2013, str. 8).

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

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 V skladu z Aktom o kibernetski varnosti se dopušča razvoj namenskih certifikacijskih shem. Vsaka shema vključuje sklice na ustrezne standarde, tehnične specifikacije ali druge zahteve glede kibernetske varnosti, opredeljene v shemi. Odločitev o razvoju certificiranja kibernetske varnosti temelji na tveganju.

za navedene ukrepe. Za vse druge subjekte lahko sprejme izvedbeni akt za določitev tehničnih in metodoloških zahtev ter sektorske zahteve. S tem okvirom se bo zagotovilo, da se tehnične specifikacije in ukrepi, podobni bistvenim zahtevam glede kibernetske varnosti iz akta o kibernetski odpornosti, izvajajo tudi za zasnovo in razvoj programske opreme kot storitve ter obravnavanje ranljivosti navedene programske opreme. To je lahko na primer način za zagotovitev visoke ravni kibernetske varnosti v primerih, kakor so sistemi za vodenje elektronskih zdravstvenih zapisov, tudi kadar se zagotavljajo kot programska oprema kot storitev ali razvijajo v zdravstvenih ustanovah, v skladu s predlagano [uredbo o evropskem zdravstvenem podatkovnem prostoru].

- **Medsebojni vpliv z drugimi politikami Unije**

Kakor je navedeno v sporočilu „Oblikovanje digitalne prihodnosti Evrope“[5], je za EU ključnega pomena, da v varnih in etičnih okvirih izkoristi priložnosti, ki jih nudi digitalna doba, ter okrepi svoje industrijske in inovacijske zmogljivosti. Evropska strategija za podatke določa štiri stebre – varstvo podatkov, temeljne pravice, varnost in kibernetsko varnost – kot ključne predpogoje za družbo, ki izkorišča moč podatkov.

Sedanji okvir EU[6], ki se uporablja za izdelke, ki lahko imajo tudi digitalne elemente, obsega več zakonodajnih aktov, vključno z zakonodajo EU o posebnih izdelkih, ki zajema varnostne vidike, in splošno zakonodajo o odgovornosti za izdelke. Predlog je skladen s sedanjim regulativnim okvirom EU v zvezi z izdelki in nedavnimi zakonodajnimi predlogi, kot je predlog Komisije za uredbo [uredba o umetni inteligenci][7].

Predlagana uredba bi se uporabljala za vso radijsko opremo, ki spada na področje uporabe Delegirane uredbe Komisije (EU) 2022/30. Poleg tega zahteve iz te uredbe vključujejo vse elemente bistvenih zahtev iz člena 3(3), točke (d), (e) in (f), Direktive 2014/53/EU, vključno z glavnimi elementi iz [Izvedbenega sklepa Komisije XXX/2022 o zahtevi za standardizacijo evropskim organizacijam za standardizacijo], izdanimi na podlagi navedene delegirane uredbe. Za preprečitev regulativnega prekrivanja je predvideno, da bo Komisija razveljavila ali spremenila Delegirano uredbo v zvezi z radijsko opremo, zajeto s predlagano uredbo, tako da bi se za navedeno opremo uporabljala predlagana uredba, ko se bo začela uporabljati.

Poleg tega je za preprečitev podvajanja dela predvideno, da Komisija in evropske organizacije za standardizacijo pri pripravi in razvoju harmoniziranih standardov za olajšanje izvajanja Uredbe upoštevajo delo za standardizacijo, opravljeno v okviru Izvedbenega sklepa Komisije C(2022) 5637 o zahtevi za standardizacijo za Delegirano uredbo (EU) 2022/30, sprejeto na podlagi direktive o radijski opremi.

2. PRAVNA PODLAGA, SUBSIDIARNOST IN SORAZMERNOST

- **Pravna podlaga**

Pravna podlaga tega predloga je člen 114 Pogodbe o delovanju Evropske unije (PDEU), ki določa sprejetje ukrepov za zagotovitev vzpostavitve in delovanja notranjega trga. Namen

---

5 Sporočilo Komisije Evropskemu parlamentu, Svetu, Evropskemu ekonomsko-socialnemu odboru in Odboru regij – Oblikovanje digitalne prihodnosti Evrope (COM(2020) 67 final z dne 19. februarja 2020).

6 Predvsem zakonodaja novega zakonodajnega okvira.

7 Predlog uredbe Evropskega parlamenta in Sveta o določitvi harmoniziranih pravil o umetni inteligenci (akt o umetni inteligenci) in spremembi nekaterih zakonodajnih aktov Unije (COM(2021) 206 final z dne 21. aprila 2021).

predloga je uskladiti zahteve glede kibernetske varnosti za izdelke z digitalnimi elementi v vseh državah članicah in odpraviti ovire za prosto gibanje blaga.

Člen 114 PDEU se lahko uporabi kot pravna podlaga za preprečitev, da bi se te ovire pojavile zaradi različnih nacionalnih zakonov in pristopov k obravnavanju pravnih negotovosti in vrzeli v obstoječih pravnih okvirih[8]. Poleg tega je Sodišče priznalo, da bi lahko bila uporaba različnih tehničnih zahtev veljaven razlog za uporabo člena 114 PDEU[9].

Sedanji zakonodajni okvir EU, ki se uporablja za izdelke z digitalnimi elementi, temelji na členu 114 PDEU ter obsega več zakonodajnih aktov, med drugim o posebnih izdelkih in varnostnih vidikih, ali splošno zakonodajo o odgovornosti za izdelke. Vendar pa zajema samo nekatere vidike, povezane s kibernetsko varnostjo materialnih digitalnih izdelkov, po potrebi pa tudi vgrajeno programsko opremo teh izdelkov. Na nacionalni ravni so države članice začele sprejemati nacionalne ukrepe, v skladu s katerimi morajo prodajalci digitalnih izdelkov izboljšati njihovo kibernetsko varnost[10]. Ob tem ima kibernetska varnost digitalnih izdelkov posebno jasno čezmejno razsežnost, saj izdelke, izdelane v eni državi, pogosto uporabljajo organizacije in potrošniki na celotnem notranjem trgu. Incidenti, ki najprej prizadenejo posamezen subjekt ali državo članico, se pogosto v nekaj minutah razširijo na številne organizacije, sektorje in države članice.

Z različnimi akti in pobudami, ki so bili doslej sprejeti na ravni EU in nacionalni ravni, se le delno obravnavajo ugotovljene težave, pri čemer obstaja tveganje nastanka zakonodajnega mozaika na notranjem trgu, povečanja pravne negotovosti za prodajalce in uporabnike teh izdelkov ter nepotrebnega povečanja bremena za podjetja zaradi izpolnjevanja številnih zahtev za podobne vrste izdelkov.

S predlagano uredbo bi se z uvedbo zahtev glede kibernetske varnosti za izdelke z digitalnimi elementi uskladilo in racionaliziralo regulativno okolje EU ter preprečilo prekrivanje zahtev iz različnih zakonodajnih aktov. Tako bi se povečala pravna varnost za gospodarske subjekte in uporabnike po vsej Uniji, bolje uskladil evropski enotni trg ter vzpostavili bolj uresničljivi pogoji za gospodarske subjekte, ki si prizadevajo vstopiti na trg EU.

- **Subsidiarnost (za neizključno pristojnost)**

Očitno čezmejna narava kibernetske varnosti na splošno ter vse večje število tveganj in incidentov, katerih učinki segajo čez meje, v razne sektorje in izdelke, pomenita, da države članice ne morejo same učinkovito doseči ciljev tega ukrepa. Nacionalni pristopi k reševanju težav in zlasti pristopi z uvedbo obveznih zahtev bodo ustvarili dodatno pravno negotovost in pravne ovire. Podjetjem bi se lahko preprečilo nemoteno širjenje v druge države članice, zaradi česar uporabniki ne bi imeli dostopa do prednosti njihovih izdelkov.

Zato je potrebno skupno ukrepanje na ravni EU, da se zagotovi visoka raven zaupanja uporabnikov ter poveča privlačnost izdelkov z digitalnimi elementi iz EU. To bi tudi koristilo digitalnemu enotnemu trgu in notranjemu trgu na splošno, saj bi zagotavljalo pravno varnost in enake konkurenčne pogoje za proizvajalce izdelkov z digitalnimi elementi.

---

8 Sodba Sodišča (veliki senat) z dne 3. decembra 2019, Češka republika/Evropski parlament in Svet Evropske unije, C-482/17, točka 35.

9 Sodba Sodišča (veliki senat) z dne 2. maja 2006, Združeno kraljestvo Velika Britanija in Severna Irska/Evropski parlament in Svet Evropske unije, C-217/04, točki 62 in 63.

10 Na primer, Finska je leta 2019 vzpostavila sistem označevanja, ki temelji na standardih ETSI, za naprave v IoT, kakor so pametne televizije, pametni telefoni in igrače. Nemčija je nedavno uvedla varnostno oznako za potrošnike za širokopasovne usmerjevalnike, pametne televizije, kamere, zvočnike in igrače ter robote za čiščenje in vrtnarjenje.

Končno je Svet v svojih sklepih z dne 23. maja 2022 o oblikovanju stališča Evropske unije glede kibernetskih vprašanj Komisijo pozval, naj do konca leta 2022 predlaga skupne zahteve glede kibernetske varnosti za povezane naprave.

- **Sorazmernost**

Kar zadeva sorazmernost predlagane uredbe, ukrepi v okviru obravnavanih možnosti politike ne bi presegali tistega, kar je potrebno za doseganje splošnih in specifičnih ciljev, niti ne bi povzročili nesorazmernih stroškov. Natančneje, z obravnavanim posredovanjem bi se na podlagi tehnološko nevtralnih zahtev, usmerjenih v cilje, ki so še naprej razumne in na splošno ustrezajo interesom vključenih subjektov, zagotovila varnost izdelkov z digitalnimi elementi v celotnem življenjskem ciklu, ki je sorazmerna z zadevnimi tveganji.

Bistvene zahteve glede kibernetske varnosti iz predloga temeljijo na splošno sprejetih standardih, pri povezanem postopku standardizacije pa bi se upoštevale tehnične posebnosti izdelkov. To pomeni, da bi se prilagodile varnostne kontrole, če bi bile potrebne zaradi določene ravni tveganja. Poleg tega bi predvidena horizontalna pravila določala ugotavljanje skladnosti, ki ga opravi tretja oseba, samo za kritične izdelke. To bi vključevalo le majhen delež trga za izdelke z digitalnimi elementi. Vpliv na MSP bi bil odvisen od njihove prisotnosti na trgu za te posebne kategorije izdelkov.

Kar zadeva sorazmernost stroškov ugotavljanja skladnosti, bi priglašeni organi, ki kot tretje osebe opravljajo ugotavljanje skladnosti, pri določanju pristojbin upoštevali velikost podjetja. Zagotovilo bi se tudi razumno prehodno obdobje 24 mesecev za pripravo na izvajanje, s čimer bi imeli zadevni trgi čas, da se pripravijo, zagotovile pa bi se tudi jasne smernice za naložbe v raziskave in razvoj. Morebitne stroške zagotavljanja skladnosti, ki jih imajo podjetja, bi odtehtale koristi višje ravni varnosti izdelkov z digitalnimi elementi in navsezadnje večjega zaupanja uporabnikov v te izdelke.

- **Izbira instrumenta**

Regulativno posredovanje bi vključevalo sprejetje uredbe in ne direktive. Za to posebno vrsto zakonodaje o izdelkih bi se namreč z uredbo učinkoviteje obravnavale ugotovljene težave in dosegli zastavljeni cilji, saj pomeni posredovanje, ki določa pogoje za dajanje zelo obsežne kategorije izdelkov na notranji trg. V primeru direktive za tako posredovanje bi se lahko pri postopku prenosa v nacionalno zakonodajo dopustile prevelike možnosti za lastno presojo na nacionalni ravni, to pa bi lahko povzročilo neenotnost nekaterih bistvenih zahtev glede kibernetske varnosti, pravno negotovost, dodatno razdrobljenost ali celo primere diskriminacije na čezmejni ravni, zlasti glede na dejstvo, da bi se lahko vključeni izdelki uporabljali za različne namene, proizvajalci pa lahko izdelujejo več kategorij takih izdelkov.

3. REZULTATI NAKNADNIH OCEN, POSVETOVANJ Z DELEŽNIKI IN OCEN UČINKA

- **Posvetovanja z deležniki**

Komisija se je posvetovala z najrazličnejšimi deležniki. Države članice in deležniki so bili povabljeni k sodelovanju pri odprtem javnem posvetovanju ter anketah in delavnicah, organiziranih v okviru študije konzorcija, ki podpira pripravljalno delo Komisije za oceno učinka: Wavestone, Center za evropske politične študije (CEPS) in ICF. Med deležniki, s katerimi je bilo opravljeno posvetovanje, so bili nacionalni organi za nadzor trga, organi Unije, ki se ukvarjajo s kibernetsko varnostjo, proizvajalci strojne in programske opreme, uvozniki in distributerji strojne in programske opreme, panožna združenja, potrošniške organizacije in uporabniki izdelkov z digitalnimi elementi, državljani, raziskovalci in

akademski krogi, priglašeni in akreditacijski organi ter strokovnjaki iz industrije kibernetske varnosti.

Dejavnosti posvetovanja so vključevale:

- prvo študijo, ki je bila objavljena decembra 2021[11], izvedel pa jo je konzorcij, ki so ga sestavljali ICF, Wavestone, Carsa in CEPS. V njej je bilo ugotovljenih več primerov nedelovanja trga, ocenjena pa so bila možna regulativna posredovanja;
- odprto javno posvetovanje, usmerjeno na državljane, deležnike in strokovnjake za kibernetsko varnost. Predloženih je bilo 176 odgovorov. Ti so prispevali k zbiranju raznolikih mnenj in izkušenj vseh skupin deležnikov;
- delavnice, organizirane v okviru študije v podporo pripravljalnemu delu Komisije za akt o kibernetski odpornosti, ki se jih je udeležilo približno 100 predstavnikov različnih deležnikov iz vseh 27 držav članic;
- razgovore s strokovnjaki, namenjene pridobivanju poglobljenega razumevanja sedanjih izzivov na področju kibernetske varnosti, povezanih z izdelki z digitalnimi elementi, in razpravi o možnostih politike za morebitno regulativno posredovanje;
- dvostranske razprave z nacionalnimi organi za kibernetsko varnost, zasebnim sektorjem in potrošniškimi organizacijami;
- ciljno usmerjeno vključevanje MSP, ki so ključni deležniki.

- **Zbiranje in uporaba strokovnih mnenj**

Dejavnosti posvetovanja so bile namenjene pridobivanju prispevkov o petih glavnih merilih vrednotenja na podlagi smernic EU za boljše pravno urejanje (uspešnost, učinkovitost, ustreznost, skladnost in dodana vrednost EU) in morebitnih učinkih možnosti za prihodnost. Izvajalec se je poleg deležnikov, na katere bi predlagana uredba neposredno vplivala, posvetoval tudi z najrazličnejšimi strokovnjaki na področju kibernetske varnosti.

- **Ocena učinka**

Komisija je za ta predlog izvedla oceno učinka, ki jo je proučil njen Odbor za regulativni nadzor. Z navedenim odborom je bil 6. julija 2022 opravljen sestanek, ki mu je sledilo pozitivno mnenje. Ocena učinka je bila prilagojena, da so se upoštevala priporočila in pripombe Odbora za regulativni nadzor.

Komisija je proučila različne možnosti politike za dosego splošnih ciljev predloga:

- pristop mehkega prava in prostovoljne ukrepe (možnost 1): ta možnost ne vključuje obveznega regulativnega posredovanja. Namesto tega bi Komisija izdajala sporočila, smernice, priporočila in morda kodekse ravnanja, da bi spodbujala prostovoljne ukrepe. Za zapolnitev vrzeli zaradi neobstoja horizontalnih pravil EU bi se še naprej razvijale prostovoljne ali obvezne nacionalne sheme;

[11] *Study on the need of Cybersecurity requirements for ICT products* (Študija potrebe po zahtevah glede kibernetske varnosti za izdelke IKT) – št. 2020-0715, končno poročilo o študiji, na voljo na spletni povezavi https://digital-strategy.ec.europa.eu/sl/node/10572.

- *ad hoc* regulativno posredovanje za kibernetsko varnost materialnih izdelkov z digitalnimi elementi in zadevne vgrajene programske opreme (možnost 2): ta možnost bi vključevala *ad hoc* regulativno posredovanje za specifične izdelke, ki bi bilo omejeno na dodajanje in/ali spreminjanje zahtev glede kibernetske varnosti v obstoječi zakonodaji ali uvajanje nove zakonodaje ob pojavu novih tveganj, po možnosti tudi o nevgrajeni programski opremi.

Možnosti 3 in 4 vključujeta horizontalno regulativno posredovanje v različnih obsegih in večinoma v skladu z novim zakonodajnim okvirom. Ta okvir določa bistvene zahteve kot pogoj za dajanje nekaterih izdelkov na notranji trg. Praviloma določa tudi ugotavljanje skladnosti, tj. postopek, ki ga opravi proizvajalec, da dokaže izpolnjevanje predpisanih zahtev v zvezi z izdelkom:

- mešani pristop, vključno s horizontalnimi obveznimi pravili za kibernetsko varnost materialnih izdelkov z digitalnimi elementi in zadevne vgrajene programske opreme ter postopnim pristopom za nevgrajeno programsko opremo (možnost 3): ta možnost bi vključevala uredbo za uvedbo horizontalnih zahtev glede kibernetske varnosti za vse materialne izdelke z digitalnimi elementi in njihovo vgrajeno programsko opremo kot pogoj za dajanje na trg ter dve podmožnosti z obveznim ugotavljanjem skladnosti, ki ga opravi tretja oseba, oziroma brez njega (3i in 3ii). Nevgrajena programska oprema se ne bi urejala;
- horizontalno regulativno posredovanje, na podlagi katerega bi se uvedle zahteve glede kibernetske varnosti za širok nabor materialnih in nematerialnih izdelkov z digitalnimi elementi, vključno z nevgrajeno programsko opremo (možnost 4): ta možnost je podobna možnosti 3, pri čemer se možnosti razlikujeta po obsegu. V skladu z možnostjo 4 bi področje uporabe morebitne uredbe vključevalo nevgrajeno programsko opremo (z dvema podmožnostma – samo kritično programsko opremo (4a) ali vso programsko opremo (4b)). Za vsako podmožnost bi se proučili isti podmožnosti v zvezi z ugotavljanjem skladnosti kot za možnost 3.

Na podlagi ocene uspešnosti glede na specifične cilje in stroškovne učinkovitosti glede na koristi je bila za prednostno možnost določena možnost 4 (s podmožnostma, ki zajemata vso programsko opremo in obvezno ugotavljanje skladnosti, ki ga opravi tretja oseba, za kritične izdelke). V skladu s to možnostjo bi se določile posebne horizontalne zahteve glede kibernetske varnosti za vse izdelke z digitalnimi elementi, ki se dajo na notranji trg ali so dostopni na njem, poleg tega pa je edina možnost, ki zajema celotno digitalno oskrbovalno verigo. Tako regulativno posredovanje bi vključevalo tudi nevgrajeno programsko opremo, ki je pogosto izpostavljena ranljivostim, s tem pa bi se zagotovil usklajen pristop k vsem izdelkom z digitalnimi elementi in jasnim deležem odgovornosti različnih gospodarskih subjektov.

Ta možnost politike ima tudi dodano vrednost, saj zajema vidike dolžnosti skrbnega ravnanja in celotnega življenjskega cikla po dajanju izdelkov z digitalnimi elementi na trg, da se me drugim zagotovita ustrezno obveščanje o podpori varnosti in zagotavljanje varnostnih posodobitev. Poleg tega bi ta možnost politike najučinkoviteje dopolnjevala nedavni pregled okvira za varnost omrežij in informacijskih sistemov, saj bi zagotovila osnovne pogoje za okrepljeno varnost oskrbovalne verige.

Prednostna možnost bi imela pomembne koristi za različne deležnike. Za podjetja bi preprečila različna varnostna pravila glede izdelkov z digitalnimi elementi in znižala stroške zagotavljanja skladnosti z zadevno zakonodajo o kibernetski varnosti. Zmanjšala bi število

kibernetskih incidentov, znižala stroške obvladovanja incidentov in zmanjšala škodo za ugled. Za celotno EU se ocenjuje, da bi se lahko zaradi pobude stroški zaradi incidentov, ki prizadenejo podjetja, znižali za približno 180–290 milijard EUR na leto. S prednostno možnostjo bi se povečal promet zaradi povečanja povpraševanja po izdelkih z digitalnimi elementi. Izboljšal bi se globalni ugled podjetij, zaradi česar bi se povečalo povpraševanje tudi zunaj EU. Za uporabnike bi prednostna možnost izboljšala preglednost varnostnih lastnosti in olajšala uporabo izdelkov z digitalnimi elementi. Potrošniki in državljani bi imeli tudi koristi zaradi boljše zaščite svojih temeljnih pravic, kot sta zasebnost in varstvo podatkov.

Kar zadeva oceno uspešnosti ukrepov politike, so se anketiranci v javnem posvetovanju strinjali, da bi bila možnost 4 najuspešnejši ukrep (na lestvici od 1 do 5 je bila ocenjena s 4,08). Med anketiranci so bili potrošniške organizacije (5,00), anketiranci, ki so se opredelili za uporabnike (4,22), priglašeni organi (4,17), organi za nadzor trga (5,00) in proizvajalci izdelkov z digitalnimi elementi (3,85), vključno z malimi in srednjimi (4,05).

- **Ustreznost in poenostavitev ureditve**

Ta predlog določa zahteve, ki se bodo uporabljale za proizvajalce programske in strojne opreme. Splošna podpora horizontalnemu posredovanju, ki so jo izrazili različni deležniki, dokazuje, da je treba zagotoviti pravno varnost in preprečiti dodatno razdrobljenost zahtev glede kibernetske varnosti, povezanih z izdelki, na notranjem trgu. S predlogom se bo čim bolj zmanjšalo regulativno breme, ki je proizvajalcem naloženo zaradi več aktov o varnosti izdelkov. Uskladitev z novim zakonodajnim okvirom pomeni boljše delovanje in izvrševanje posredovanja. V skladu s predlogom se proizvajalci in države članice vključijo pred priglasitvijo Komisiji, s čimer se racionalizirajo zaščitni postopki. Velik del proizvajalcev, ki spadajo na področje uporabe predloga, že pozna delovanje novega zakonodajnega okvira, kar bo prispevalo k njegovemu razumevanju in izvajanju. Kar zadeva potrošnike in podjetja, bo predlog spodbujal zaupanje v izdelke z digitalnimi elementi.

- **Temeljne pravice**

Vse možnosti politike bodo predvidoma v različnem obsegu izboljšale varstvo temeljnih pravic in svoboščin, kakor so zasebnost, varstvo osebnih podatkov, svoboda gospodarske pobude in varstvo lastnine ali osebnega dostojanstva in celovitosti. Zlasti prednostna možnost politike 4, ki vključuje horizontalne regulativne ukrepe in široko področje uporabe politike, bi bila v zvezi s tem najuspešnejša, saj verjetneje prispeva k zmanjšanju števila in resnosti incidentov, vključno s kršitvami varstva osebnih podatkov Poleg tega bi se z njo povečala pravna varnost in dosegli enaki konkurenčni pogoji za gospodarske subjekte, okrepilo zaupanje uporabnikov in povečala privlačnost vseh izdelkov z digitalnimi elementi iz EU, s čimer bi se zaščitila lastnina in izboljšali pogoji za poslovanje gospodarskih subjektov.

Horizontalne zahteve glede kibernetske varnosti bi prispevale k varnosti osebnih podatkov z varstvom zaupnosti, celovitosti in razpoložljivosti informacij v izdelkih z digitalnimi elementi. Izpolnjevanje navedenih zahtev bo olajšalo izpolnjevanje zahteve po varnosti obdelave osebnih podatkov na podlagi splošne uredbe o varstvu podatkov (Uredba (EU) 2016/679)[12]. S predlogom bi se izboljšala preglednost in obveščanje uporabnikov, vključno s tistimi, ki jim morda primanjkuje veščin za kibernetsko varnost. Poleg tega bi bili uporabniki bolje obveščeni o tveganjih, zmogljivostih in omejitvah izdelkov

[12] 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).

z digitalnimi elementi, s tem pa v boljšem položaju za sprejemanje potrebnih preventivnih in blažilnih ukrepov za zmanjšanje preostalih tveganj.

4. PRORAČUNSKE POSLEDICE

Da bi Agencija Evropske unije za kibernetsko varnost (ENISA) izpolnila naloge, ki se ji dodelijo s to uredbo, bo morala prerazporediti vire v obsegu približno 4,5 EPDČ. Komisija bi morala dodeliti 7 EPDČ, da bi izpolnila odgovornosti v zvezi z izvrševanjem na podlagi te uredbe.

Podroben pregled zadevnih stroškov je na voljo v „oceni finančnih posledic zakonodajnega predloga“, povezani s tem predlogom.

5. DRUGI ELEMENTI

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

Komisija bo spremljala izvajanje in uporabo teh novih določb ter skladnost z njimi, da oceni njihovo uspešnost. V skladu z uredbo bo morala opraviti oceno in revizijo uredbe ter Evropskemu parlamentu in Svetu v 36 mesecih od datuma začetka njene uporabe, nato pa vsaka štiri leta predložiti javno poročilo v zvezi s tem.

- **Natančnejša pojasnitev posameznih določb predloga**

Splošne določbe (poglavje I)

Predlagana uredba določa (a) pravila za dajanje izdelkov z digitalnimi elementi na trg za zagotovitev njihove kibernetske varnosti; (b) bistvene zahteve za zasnovo, razvoj in proizvodnjo izdelkov z digitalnimi elementi ter obveznosti gospodarskih subjektov v zvezi s kibernetsko varnostjo teh izdelkov; (c) bistvene zahteve za postopke obravnavanja ranljivosti, ki jih vzpostavijo proizvajalci, za zagotovitev kibernetske varnosti izdelkov z digitalnimi elementi v celotnem življenjskem ciklu ter obveznosti gospodarskih subjektov v zvezi s temi postopki; (d) pravila o nadzoru trga ter izvrševanju navedenih pravil in zahtev.

Predlagana uredba se bo uporabljala za vse izdelke z digitalnimi elementi, katerih predvidena in razumno predvidljiva uporaba vključuje neposredno ali posredno logično ali fizično podatkovno povezavo z napravo ali omrežjem.

Predlagana uredba se ne bo uporabljala za izdelke z digitalnimi elementi, ki spadajo na področje uporabe Uredbe (EU) 2017/745 [medicinski pripomočki za uporabo v humani medicini in dodatki zanje] in Uredbe (EU) 2017/746 [*in vitro* diagnostični medicinski pripomočki za uporabo v humani medicini in dodatki zanje], saj obe uredbi vsebujeta zahteve glede naprav, vključno s programsko opremo, in splošne obveznosti proizvajalcev, ki zajemajo celotni življenjski cikel izdelkov, ter postopke ugotavljanja skladnosti. Ta uredba se ne bo uporabljala za izdelke z digitalnimi elementi, certificirane v skladu z Uredbo (EU) 2018/1139 [visoka enotna raven varnosti v civilnem letalstvu], niti za izdelke, za katere se uporablja Uredba (EU) 2019/2144 [o zahtevah za homologacijo motornih vozil in njihovih priklopnikov ter sistemov, sestavnih delov in samostojnih tehničnih enot, namenjenih za taka vozila].

Za kritične izdelke z digitalnimi elementi se bodo uporabljali specifični postopki ugotavljanja skladnosti, poleg tega pa bodo taki izdelki razdeljeni v razreda I in II, kot sta določena v Prilogi III, da se izrazi njihova raven tveganja za kibernetsko varnost, pri čemer je tveganje večje pri izdelkih v razredu II. Izdelek z digitalnimi elementi velja za kritičnega in je zato

vključen v Prilogo III na podlagi vpliva morebitnih ranljivosti na področju kibernetske varnosti, povezanih z njim. Pri ugotavljanju tveganja za kibernetsko varnost se upoštevata funkcionalnost izdelka z digitalnimi elementi, povezana s kibernetsko varnostjo, in predvidena uporaba v občutljivih okoljih, kot je industrijsko.

Na Komisijo se prenese tudi pooblastilo za sprejemanje delegiranih aktov za dopolnitev te uredbe z določitvijo kategorij zelo kritičnih izdelkov z digitalnimi elementi, za katere bodo morali proizvajalci pridobiti evropski certifikat kibernetske varnosti na podlagi evropske certifikacijske sheme kibernetske varnosti, da dokažejo skladnost z bistvenimi zahtevami iz Priloge I ali njihovimi deli. Komisija pri določanju takih kategorij zelo kritičnih izdelkov z digitalnimi elementi upošteva raven tveganja za kibernetsko varnost, povezano s kategorijo izdelkov z digitalnimi elementi, glede na eno ali več meril, ki se upoštevajo za uvrstitev kritičnih izdelkov z digitalnimi elementi v Prilogo III, ter glede na presojo, ali navedeno kategorijo izdelkov uporabljajo ali se nanjo zanašajo bistveni subjekti iz Priloge [Priloge I] k Direktivi [Direktiva XXX/XXXX (NIS2)] oziroma bo morda pomembna za dejavnosti navedenih subjektov v prihodnosti, ali je pomembna za odpornost celotne oskrbovalne verige izdelkov z digitalnimi elementi proti dogodkom, ki povzročajo motnje.

Obveznosti gospodarskih subjektov (poglavje II)

Predlog vključuje obveznosti za proizvajalce, uvoznike in distributerje na podlagi referenčnih določb iz Sklepa št. 768/2008/ES. V skladu z bistvenimi zahtevami in obveznostmi glede kibernetske varnosti so lahko vsi izdelki z digitalnimi elementi dostopni na trgu samo, če izpolnjujejo bistvene zahteve glede kibernetske varnosti iz te uredbe, kadar se ustrezno dobavijo, pravilno namestijo, vzdržujejo in uporabljajo za njihov predvideni namen ali pod razumno predvidljivimi pogoji.

V skladu z bistvenimi zahtevami in obveznostmi bi se od izdelovalcev zahtevalo, da upoštevajo kibernetsko varnost pri zasnovi in razvoju ter proizvodnji izdelkov z digitalnimi elementi, izvajajo potrebno skrbnost v zvezi z varnostnimi vidiki pri zasnovi in razvoju svojih izdelkov, zagotovijo preglednost v zvezi z vidiki kibernetske varnosti, o katerih je treba obvestiti stranke, zagotovijo podporo za varnost (posodobitve) na sorazmeren način in izpolnijo zahteve glede obravnavanja ranljivosti.

Za gospodarske subjekte od izdelovalcev do distributerjev in uvoznikov bi se določile obveznosti v zvezi z dajanjem izdelkov z digitalnimi elementi na trg, ki ustrezajo njihovi vlogi in odgovornostim v oskrbovalni verigi.

Skladnost izdelkov z digitalnimi elementi (poglavje III)

Za izdelek z digitalnimi elementi, ki je skladen s harmoniziranimi standardi ali njihovimi deli, na katere so bili objavljeni sklici v *Uradnem listu Evropske unije*, se domneva, da izpolnjuje bistvene zahteve iz te predlagane uredbe. Če harmonizirani standardi ne obstajajo ali so nezadostni ali če se pri postopku standardizacije pojavijo neupravičene zamude ali evropske organizacije za standardizacijo ne sprejmejo zahteve Komisije, lahko Komisija z izvedbenimi akti sprejme skupne specifikacije.

Poleg tega se za izdelke z digitalnimi elementi, ki so bili certificirani ali za katere sta bila izdana izjava EU o skladnosti ali certifikat v okviru evropske certifikacijske sheme kibernetske varnosti v skladu z Uredbo (EU) 2019/881 in za katere je Komisija z izvedbenim aktom določila, da lahko oblikuje domnevo o skladnosti za to uredbo, domneva, da izpolnjujejo bistvene zahteve iz te uredbe ali njihove dele, če izjava EU o skladnosti ali certifikat kibernetske varnosti ali del izjave oziroma certifikata zajema navedene zahteve.

Poleg tega bi morala Komisija za preprečitev nepotrebnega upravnega bremena za proizvajalce po potrebi navesti, ali se s certifikatom kibernetske varnosti, izdanim v okviru

take evropske certifikacijske sheme kibernetske varnosti, odpravi obveznost izdelovalcev, da za ustrezne zahteve zagotovijo ugotavljanje skladnosti, ki ga opravi tretja oseba, kot je določeno v tej uredbi.

Proizvajalec opravi ugotavljanje skladnosti izdelka z digitalnimi elementi in postopke obravnavanja ranljivosti, ki jih je vzpostavil za dokazovanje skladnosti z bistvenimi zahtevami iz Priloge I, v skladu z enim od postopkov iz Priloge VI. Proizvajalci kritičnih izdelkov iz razredov I in II uporabljajo zadevne module, potrebne za skladnost. Proizvajalci kritičnih izdelkov iz razreda II morajo v ugotavljanje skladnosti vključiti tretjo osebo.

Priglasitev organov za ugotavljanje skladnosti (poglavje IV)

Ustrezno delovanje priglašenih organov je ključno za zagotavljanje visoke ravni kibernetske varnosti in za zaupanje vseh zainteresiranih strani v sistem po Novem pristopu. Zato predlog v skladu s Sklepom št. 768/2008/ES določa zahteve za nacionalne organe, pristojne za organe za ugotavljanje skladnosti (priglašene organe). Tako so za imenovanje in spremljanje priglašenih organov končno pristojne države članice. Te imenujejo priglasitveni organ, ki je pristojen za vzpostavitev in izvajanje postopkov, potrebnih za oceno in priglasitev organov za ugotavljanje skladnosti ter spremljanje priglašenih organov.

Nadzor trga in izvrševanje (poglavje V)

V skladu z Uredbo (EU) 2019/1020 nacionalni organi za nadzor trga izvajajo nadzor trga na ozemlju zadevne države članice. Države članice lahko za opravljanje nalog organa za nadzor trga imenujejo kateri koli obstoječi ali nov organ, vključno s pristojnimi nacionalnimi organi iz člena [člen X] Direktive [Direktiva XXX/XXXX (NIS2)] ali imenovanimi nacionalnimi certifikacijskimi organi za kibernetsko varnost iz člena 58 Uredbe (EU) 2019/881. Od gospodarskih subjektov se zahteva, da v celoti sodelujejo z organi za nadzor trga in drugimi pristojnimi organi.

Prenesena pooblastila in postopki v odboru (poglavje VI)

Za zagotovitev, da se lahko regulativni okvir po potrebi prilagodi, se na Komisijo v skladu s členom 290 PDEU prenese pooblastilo za sprejemanje aktov za posodobitev seznama kritičnih izdelkov iz razredov I in II ter določitev opredelitev teh izdelkov; določitev, ali je za izdelke z digitalnimi elementi, zajete z drugimi pravili Unije, ki določajo zahteve, s katerimi se doseže enaka raven varstva kot s to uredbo, potrebna omejitev ali izključitev; določitev obveznosti certificiranja nekaterih zelo kritičnih izdelkov z digitalnimi elementi na podlagi meril iz te uredbe; določitev minimalne vsebine izjave EU o skladnosti in dopolnitev elementov, ki se vključijo v tehnično dokumentacijo.

Na Komisijo se prenese tudi pooblastilo za sprejemanje izvedbenih aktov za: določitev oblike ali elementov obveznosti poročanja in kosovnice za programsko opremo; določitev evropskih certifikacijskih shem kibernetske varnosti, ki se lahko uporabljajo za dokazovanje skladnosti z bistvenimi zahtevami ali njihovimi deli, kakor so določeni v tej uredbi; sprejetje skupnih specifikacij; določitev tehničnih specifikacij za namestitev oznake CE; sprejetje popravnih ali omejevalnih ukrepov na ravni Unije v izjemnih okoliščinah, ki upravičujejo takojšnje ukrepanje za ohranitev dobrega delovanja notranjega trga.

Zaupnost in kazni (poglavje VII)

Vse strani, ki uporabljajo to uredbo, spoštujejo zaupnost informacij in podatkov, ki jih pridobijo med opravljanjem nalog in dejavnosti.

Za zagotovitev učinkovitega izvrševanja obveznosti iz te uredbe bi moral biti vsak organ za nadzor trga pooblaščen, da naloži ali zahteva naložitev upravnih glob. Podobno ta uredba

določa najvišje zneske upravnih glob, ki bi jih bilo treba določiti v nacionalni zakonodaji za neizpolnjevanje obveznosti iz te uredbe.

Prehodne in končne določbe (poglavje VIII)

Da bi imeli proizvajalci, priglašeni organi in države članice čas, da se prilagodijo novim zahtevam, se bo predlagana uredba začela uporabljati [24 mesecev] po začetku njene veljavnosti, razen obveznosti poročanja za proizvajalce, ki bi se začele uporabljati [12 mesecev] po datumu začetka veljavnosti.

2022/0272 (COD)

Predlog

UREDBA EVROPSKEGA PARLAMENTA IN SVETA

o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi Uredbe (EU) 2019/1020

(Besedilo velja za EGP)

EVROPSKI PARLAMENT IN SVET EVROPSKE UNIJE STA –

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

ob upoštevanju predloga Evropske komisije,

po posredovanju osnutka zakonodajnega akta nacionalnim parlamentom,

ob upoštevanju mnenja Evropskega ekonomsko-socialnega odbora[1],

ob upoštevanju mnenja Odbora regij[2],

v skladu z rednim zakonodajnim postopkom,

ob upoštevanju naslednjega:

(1) Delovanje notranjega trga je treba izboljšati 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.

(3) Trenutno veljavna ustrezna zakonodaja 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 oskrbovalne verige. Vendar obstoječa zakonodaja Unije v zvezi s kibernetsko varnostjo, vključno z Direktivo [Direktiva XXX/XXXX (NIS2)] in Uredbo (EU) 2019/881 Evropskega

[1] UL C , , str. .
[2] UL C , , str. .

parlamenta in Sveta[3], ne zajema neposredno obveznih zahtev za varnost izdelkov z digitalnimi elementi.

(4) Medtem ko se obstoječa zakonodaja 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 zaradi izpolnjevanja številnih zahtev za podobne vrste izdelkov. Kibernetska varnost teh izdelkov ima posebno jasno čezmejno razsežnost, saj izdelke, izdelane v eni državi, pogosto uporabljajo organizacije in potrošniki na celotnem notranjem trgu. Zato je treba to področje urejati na ravni Unije. Regulativno okolje Unije bi bilo treba uskladiti z uvedbo zahtev glede kibernetske varnosti za izdelke z digitalnimi elementi. Poleg tega bi bilo treba zagotoviti varnost za gospodarske subjekte in uporabnike po vsej Uniji ter boljšo uskladitev enotnega trga, s tem pa ustvariti bolj uresničljive pogoje za gospodarske subjekte, ki si prizadevajo vstopiti na trg Unije.

(5) Na ravni Unije so različni programski in politični dokumenti, kakor so strategija EU za kibernetsko varnost v digitalnem desetletju[4], sklepi Sveta z dne 2. decembra 2020 in z dne 23. maja 2022 ali resolucija Evropskega parlamenta z dne 10. junija 2021[5], vključevali poziv k uvedbi specifičnih zahtev Unije glede kibernetske varnosti za digitalne ali povezane izdelke, pri čemer je več držav z vsega sveta na lastno pobudo uvedlo ukrepe za obravnavo tega vprašanja. V končnem poročilu Konference o prihodnosti Evrope[6] so državljani pozvali k „večji vlogi EU pri preprečevanju kibernetskih groženj“.

(6) 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.

(7) 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 in možnostjo povezave načrtujejo in razvijajo v skladu z bistvenimi zahtevami iz te uredbe. To vključuje izdelke z možnostjo fizične povezave prek vmesniške strojne opreme in izdelke z možnostjo logične povezave, na primer prek omrežnih vtičnic,

---

[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] JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/SL/ALL/?uri=CELEX:52020JC0018.

[5] 2021/2568(RSP), https://www.europarl.europa.eu/doceo/document/TA-9-2021-0286_SL.html.

[6] *Konferenca o prihodnosti Evrope – poročilo o končnem izidu,* maj 2022, predlog 28(2). Konferenca je potekala med aprilom 2021 in majem 2022. To je bila edinstvena pobuda posvetovalne demokracije na vseevropski ravni pod vodstvom državljanov, ki je vključevala na tisoče evropskih državljanov, pa tudi politične akterje, socialne partnerje, predstavnike civilne družbe in ključne deležnike.

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, ki so zgolj posredno povezani z drugimi napravami ali omrežji.

(8) Z določitvijo zahtev glede kibernetske varnosti za dajanje izdelkov z digitalnimi elementi na trg se bo izboljšala kibernetska varnost teh izdelkov za potrošnike in podjetja. To vključuje tudi zahteve za dajanje potrošniških izdelkov z digitalnimi elementi, ki so namenjeni ranljivim potrošnikom, kakor so igrače in elektronske varuške, na trg.

(9) Ta uredba zagotavlja visoko raven kibernetske varnosti izdelkov z digitalnimi elementi. Z njo se ne urejajo storitve, kot je programska oprema kot storitev, razen rešitev za daljinsko obdelavo podatkov v zvezi z izdelkom z digitalnimi elementi, pri čemer daljinska obdelava podatkov pomeni vsako obdelavo podatkov na daljavo, za katero je programsko opremo zasnoval in razvil proizvajalec zadevnega izdelka ali je bila zasnovana in razvita pod njegovo odgovornostjo ter brez katere zadevni izdelek z digitalnimi elementi ne bi mogel opravljati ene od svojih funkcij. [Direktiva XXX/XXXX (NIS2)] določa zahteve glede poročanja o kibernetski varnosti in incidentih za bistvene in pomembne subjekte, kot je kritična infrastruktura, da bi se izboljšala odpornost storitev, ki jih zagotavljajo. [Direktiva XXX/XXXX (NIS2)] se uporablja za storitve računalništva v oblaku in modele storitev v oblaku, kot je programska oprema kot storitev. Na njeno področje uporabe spadajo vsi subjekti, ki zagotavljajo storitve računalništva v oblaku v Uniji in dosegajo ali presegajo prag za srednja podjetja.

(10) Da se ne bi ovirale inovacije ali raziskave, se ta uredba ne bi smela uporabljati za prosto in odprtokodno programsko opremo, ki se ne razvija ali dobavlja v okviru gospodarske dejavnosti. To zlasti velja za programsko opremo, vključno z njeno izvorno kodo in spremenjenimi različicami, ki je prosto dostopna vsem, je za prosto uporabo ter jo je mogoče spremeniti in ponovno distribuirati. V zvezi s programsko opremo je lahko za gospodarsko dejavnost poleg zaračunavanja cene za izdelek značilno tudi zaračunavanje cene za storitve tehnične podpore, zagotavljanje platforme programske opreme, prek katere proizvajalec monetizira druge storitve, ali uporaba osebnih podatkov za druge namene kot izključno za izboljšanje varnosti, združljivosti ali interoperabilnosti programske opreme.

(11) Varen internet je nepogrešljiv za delovanje kritične infrastrukture in družbe kot celote. [Direktiva XXX/XXXX (NIS2)] je namenjena zagotovitvi visoke ravni kibernetske varnosti storitev, ki jih opravljajo bistveni in pomembni subjekti, vključno s ponudniki digitalne infrastrukture, ki podpirajo osnovne funkcije odprtega interneta ter zagotavljajo dostop do interneta in internetne storitve. Zato je pomembno, da se izdelki z digitalnimi elementi, ki jih ponudniki digitalne infrastrukture potrebujejo za zagotavljanje delovanja interneta, razvijajo varno in dosegajo 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 oskrbovalne verige na podlagi Direktive [Direktiva XXX/XXXX (NIS2)] z zagotavljanjem varnega razvoja izdelkov z digitalnimi elementi, ki jih navedeni ponudniki uporabljajo za zagotavljanje svojih storitev, in njihovega dostopa do pravočasnih varnostnih posodobitev za take izdelke.

(12) Uredba (EU) 2017/745 Evropskega parlamenta in Sveta[7] določa pravila o medicinskih pripomočkih, Uredba (EU) 2017/746 Evropskega parlamenta in Sveta[8] pa pravila o *in vitro* diagnostičnih medicinskih pripomočkih. Z obema 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 navodila za izpolnjevanje vseh ustreznih bistvenih zahtev iz prilog I k navedenima uredbama v zvezi s kibernetsko varnostjo[9]. Zato se ta uredba ne bi smela uporabljati za izdelke z digitalnimi elementi, za katere se uporablja katera koli od navedenih uredb.

(13) Uredba (EU) 2019/2144 Evropskega parlamenta in Sveta[10] določa zahteve za homologacijo vozil ter njihovih sistemov in sestavnih delov, pri čemer uvaja nekatere zahteve glede kibernetske varnosti, med drugim glede delovanja certificiranega sistema za upravljanje kibernetske varnosti in posodobitev programske opreme, zajema politike in postopke organizacij za kibernetska tveganja, povezana s celotnim življenjskim ciklom vozil, opreme in storitev, v skladu z veljavnimi pravilniki Združenih narodov o tehničnih specifikacijah in kibernetski varnosti[11] ter določa posebne postopke ugotavljanja skladnosti. Na področju letalstva je glavni cilj Uredbe (EU) 2018/1139 Evropskega parlamenta in Sveta[12] 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, opremo, vključno s

---

7 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).

8 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).

9 MDCG 2019-16, ki ga je potrdila Koordinacijska skupina za medicinske pripomočke (MDCG), ustanovljena s členom 103 Uredbe (EU) 2017/745.

10 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).

11 Pravilnik ZN št. 155 – Enotne določbe o homologaciji vozil glede na kibernetsko varnost in sistem za upravljanje kibernetske varnosti [2021/387].

12 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).

programsko opremo, pri katerih se upoštevajo obveznosti zaščite pred tveganji za varnost informacij. Zato se bistvene zahteve in postopki ugotavljanja skladnosti iz te uredbe ne uporabljajo za izdelke z digitalnimi elementi, za katere se uporablja Uredba (EU) 2019/2144, in izdelke, certificirane v skladu z Uredbo (EU) 2018/1139. S postopkom certificiranja na podlagi Uredbe (EU) 2018/1139 se zagotovi raven zanesljivosti, ki je cilj te uredbe.

(14) 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 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 iz Priloge I k tej uredbi, omeji ali izključi, če je taka omejitev ali izključitev v skladu s splošnim regulativnim okvirom, ki se uporablja za navedene izdelke, in se s sektorskimi pravili doseže enaka raven varstva, kot je določena s to uredbo. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov za spremembo te uredbe z opredelitvijo takih izdelkov in pravil. Ta uredba za obstoječo zakonodajo Unije, v zvezi s katero bi se morale uporabljati take omejitve ali izključitve, vsebuje posebne določbe za pojasnitev njene povezave z navedeno zakonodajo Unije.

(15) Delegirana uredba Komisije (EU) 2022/30 določa, da se bistvene zahteve iz člena 3(3), točke (d) (škoda za omrežje in zloraba omrežnih virov), (e) (osebni podatki in zasebnost) in (f) (goljufije), Direktive 2014/53/EU uporabljajo za določeno radijsko opremo. [Izvedbeni sklep Komisije XXX/2022 o zahtevi za standardizacijo evropskim organizacijam za standardizacijo] določa zahteve za razvoj posebnih standardov, s katerimi je podrobneje določeno, kako bi bilo treba obravnavati te tri bistvene zahteve. Bistvene zahteve iz te uredbe vključujejo vse elemente bistvenih zahtev iz člena 3(3), točke (d), (e) in (f), Direktive 2014/53/EU. Poleg tega so bistvene zahteve iz te uredbe usklajene s cilji zahtev za posebne standarde, vključene v navedeno zahtevo za standardizacijo. Če 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 Komisije C(2022) 5637 o zahtevi za standardizacijo za Delegirano uredbo (EU) 2022/30, sprejeto na podlagi direktive o radijski opremi.

(16) Direktiva 85/374/ES[13] 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 izdelovalcev, ki se nanašajo na zagotavljanje takih varnostnih posodobitev.

[13] Direktiva Sveta 85/374/ES z dne 25. julija 1985 o približevanju zakonov in drugih predpisov držav članic v zvezi z odgovornostjo za proizvode z napako (UL L 210, 7.8.1985).

(17) Ta uredba ne bi smela posegati v Uredbo (EU) 2016/679 Evropskega parlamenta in Sveta[14], 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 (ENISA), Evropskim odborom za varstvo podatkov (EOVP), 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 zakonodajo 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 zakonodaje Unije o varstvu podatkov. Slednji bi morali imeti tudi dostop do informacij, pomembnih za opravljanje njihovih nalog.

(18) Izdajatelji evropske denarnice za digitalno identiteto iz člena [člen 6a(2) Uredbe (EU) št. 910/2014, kakor je bila spremenjena s predlogom uredbe o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo okvira za evropsko digitalno identiteto] bi morali izpolnjevati horizontalne bistvene zahteve iz te uredbe in posebne varnostne zahteve, določene s členom [člen 6a Uredbe (EU) št. 910/2014, kakor je bila spremenjena s predlogom uredbe o spremembi Uredbe (EU) št. 910/2014 v zvezi z vzpostavitvijo okvira za evropsko digitalno identiteto], če njihovi izdelki spadajo na področje uporabe te uredbe. Za olajšanje zagotavljanja skladnosti bi morali imeti izdajatelji denarnice možnost, da dokažejo skladnost evropskih denarnic za digitalno identiteto z zahtevami iz obeh aktov s certificiranjem svojih izdelkov v okviru evropske certifikacijske sheme kibernetske varnosti, vzpostavljene na podlagi Uredbe (EU) 2019/881, za katero je Komisija z izvedbenim aktom oblikovala domnevo o skladnosti za to uredbo, kolikor certifikat ali njegovi deli zajemajo navedene zahteve.

(19) Nekatere naloge iz te uredbe bi morala opravljati agencija ENISA v skladu s členom 3(2) Uredbe (EU) 2019/881. Zlasti bi morala agencija ENISA prejemati uradna obvestila izdelovalcev o aktivno izrabljenih ranljivostih v izdelkih z digitalnimi elementi in incidentih, ki vplivajo na varnost navedenih izdelkov. Ta uradna obvestila bi morala tudi posredovati zadevnim skupinam za odzivanje na incidente na področju računalniške varnosti (CSIRT) oziroma zadevnim enotnim kontaktnim točkam držav članic, imenovanim v skladu s členom [člen X] Direktive [Direktiva XXX/XXXX (NIS2)], ter o sporočeni ranljivosti obvestiti ustrezne organe za nadzor trga. 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 iz Direktive [Direktiva XXX/XXXX (NIS2)]. Poleg tega bi morala biti glede na svoje strokovno znanje in mandat sposobna

[14] 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).

podpirati postopek za izvajanje te uredbe. Zlasti bi morala biti 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 opredeliti kategorije izdelkov, za katere bi bilo treba organizirati sočasne usklajene kontrolne ukrepe. Agencija ENISA bi morala biti sposobna v izjemnih okoliščinah na zahtevo Komisije opraviti ocene v zvezi s posameznimi izdelki z digitalnimi elementi, ki pomenijo povečano tveganje za kibernetsko varnost, če je potrebno takojšnje ukrepanje, da se ohrani dobro delovanje notranjega trga.

(20) Izdelki z digitalnimi elementi bi morali imeti oznako CE, ki 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.

(21) Da bi lahko proizvajalci pred ugotavljanjem skladnosti njihovih izdelkov 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 zadevna različica 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 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.

(22) Za zagotovitev, da izdelki z digitalnimi elementi, dani na trg, ne pomenijo tveganja za kibernetsko varnost za osebe in organizacije, bi bilo treba za take izdelke določiti bistvene zahteve. Ko se izdelki pozneje fizično ali digitalno spremenijo na način, ki ga izdelovalec ni predvidel in ki bi lahko pomenil, da ne izpolnjujejo več ustreznih bistvenih zahtev, bi bilo treba spremembo šteti za bistveno. Na primer, posodobitve ali popravila programske opreme se lahko štejejo za enakovredne vzdrževalnim postopkom, če izdelka, ki je že na trgu, ne spremenijo tako, da bi to vplivalo na skladnost z veljavnimi zahtevami ali da bi se lahko spremenila predvidena uporaba, za katero je bil izdelek ocenjen. Podobno kot pri fizičnih popravilih ali spremembah bi bilo treba šteti, da je izdelek z digitalnimi elementi bistveno spremenjen s spremembo programske opreme, če se s posodobitvijo programske opreme spremenijo prvotno predvidene funkcije, vrsta ali delovanje izdelka in te spremembe niso bile predvidene v začetni oceni tveganja ali če se zaradi posodobitve programske opreme spremeni narava nevarnosti ali poviša raven tveganja.

(23) 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 vsaki bistveni spremembi, ki bi lahko vplivala na skladnost izdelka s to uredbo, ali ob spremembi predvidenega namena navedenega izdelka preveri skladnost izdelka z digitalnimi elementi in po potrebi izvede novo ugotavljanje skladnosti. Če proizvajalec opravi ugotavljanje skladnosti, pri katerem sodeluje tretja oseba, bi bilo treba tretjo osebo obvestiti o spremembah, ki lahko pomenijo bistvene spremembe.

(24) Prenovitev, vzdrževanje in popravilo izdelka z digitalnimi elementi, kakor so opredeljeni v Uredbi [uredba o okoljsko primerni zasnovi], ne povzročijo nujno bistvene spremembe izdelka, če se na primer predvidena uporaba in funkcije ter raven tveganja ne spremenijo. Nadgradnja izdelka, ki jo izvede proizvajalec, pa lahko

povzroči spremembe zasnove in razvoja izdelka ter tako vpliva na predvideno uporabo in skladnost izdelka z zahtevami iz te uredbe.

(25) Izdelke z digitalnimi elementi bi bilo treba šteti za kritične, če je lahko negativni vpliv izrabljanja morebitnih ranljivosti izdelka v zvezi s kibernetsko varnostjo resen, na primer zaradi funkcij, povezanih s kibernetsko varnostjo, ali predvidene uporabe. Zlasti lahko ranljivosti izdelkov z digitalnimi elementi, ki vključujejo funkcije, povezane s kibernetsko varnostjo, kakor so varnostni elementi, povzročijo širjenje varnostnih težav po vsej oskrbovalni verigi. Poleg tega se lahko resnost vpliva kibernetskega incidenta poveča, če se upošteva predvidena uporaba izdelka, na primer v industrijskem okolju ali v okviru bistvenega subjekta iz Priloge [Priloga I] k Direktivi [Direktiva XXX/XXXX (NIS2)] ali za opravljanje kritičnih ali občutljivih funkcij, kot je obdelava osebnih podatkov.

(26) Za kritične izdelke 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 kritične izdelke z digitalnimi elementi razdeliti v dva razreda, da se izrazi raven tveganja za kibernetsko varnost, povezana s temi kategorijami izdelkov. Morebiten kibernetski incident v zvezi z izdelki iz razreda II bi lahko imel večje negativne učinke kot incident v zvezi z izdelki iz razreda I, na primer zaradi narave njihove funkcije, povezane s kibernetsko varnostjo, ali predvidene uporabe v občutljivih okoljih, zato bi se moral v zvezi s takimi izdelki izvajati strožji postopek ugotavljanja skladnosti.

(27) Kategorije kritičnih izdelkov z digitalnimi elementi iz Priloge III k tej uredbi bi bilo treba razumeti kot izdelke z osnovnimi funkcijami, ki spadajo med osnovne funkcije, navedene v Prilogi III k tej uredbi. Na primer, v Prilogi III k tej uredbi so v razredu II navedeni izdelki, ki so na podlagi svoje osnovne funkcije opredeljeni kot mikroprocesorji za splošno uporabo. Zato se v zvezi z mikroprocesorji za splošno uporabo izvaja obvezno ugotavljanje skladnosti, ki ga opravi tretja oseba. To ne velja za druge izdelke, ki niso izrecno navedeni v Prilogi III k tej uredbi in v katere se lahko vgradi mikroprocesor za splošno uporabo. Komisija bi morala v [12 mesecih od začetka veljavnosti te uredbe] sprejeti delegirane akte za opredelitev kategorij izdelkov, vključenih v razreda I in II, kot sta navedena v Prilogi III.

(28) Ta uredba obravnava tveganja za kibernetsko varnost na ciljno usmerjen način. Izdelki z digitalnimi elementi pa lahko povzročajo tudi druga varnostna tveganja, ki niso povezana s kibernetsko varnostjo. Navedena tveganja bi se morala še naprej urejati z drugo ustrezno zakonodajo Unije o izdelkih. Če se druga harmonizacijska zakonodaja Unije ne uporablja, bi se morala v zvezi z njimi uporabljati Uredba [uredba o splošni varnosti proizvodov]. Zaradi ciljno usmerjene narave te uredbe bi se morala z odstopanjem od člena 2(1), tretji pododstavek, točka (b), Uredbe [uredba o splošni varnosti proizvodov] poglavje III, oddelek 1, poglavji V in VII ter poglavja IX do XI Uredbe [uredba o splošni varnosti proizvodov] 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 v smislu [člena 3, točka (25), uredbe o splošni varnosti proizvodov].

(29) Izdelki z digitalnimi elementi, ki so opredeljeni kot umetnointeligenčni sistemi velikega tveganja v skladu s členom 6 Uredbe[15] [uredba o umetni inteligenci] in spadajo na področje uporabe te uredbe, bi morali izpolnjevati bistvene zahteve iz te

[15] Uredba [uredba o umetni inteligenci].

uredbe. Kadar navedeni umetnointeligenčni sistemi velikega tveganja izpolnjujejo bistvene zahteve iz te uredbe, bi bilo treba šteti, da izpolnjujejo zahteve glede kibernetske varnosti iz člena [člena 15] Uredbe [uredba o umetni inteligenci], kolikor so navedene zahteve zajete z izjavo EU o skladnosti, izdano na podlagi te uredbe, ali njenimi deli. Kar zadeva postopke ugotavljanja skladnosti v zvezi z bistvenimi zahtevami glede kibernetske varnosti izdelka z digitalnimi elementi, zajetega s to uredbo in opredeljenega kot umetnointeligenčni sistem velikega tveganja, bi se praviloma morale namesto zadevnih določb te uredbe uporabljati ustrezne določbe člena 43 Uredbe [uredba o umetni inteligenci]. Vendar se zaradi tega pravila ne bi smela znižati potrebna raven zanesljivosti za kritične izdelke z digitalnimi elementi, zajete s to uredbo. Zato bi se morale z odstopanjem od tega pravila za umetnointeligenčne sisteme velikega tveganja, ki spadajo na področje uporabe Uredbe [uredba o umetni inteligenci] in so opredeljeni tudi kot 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 [uredba o umetni inteligenci], v zvezi z bistvenimi zahtevami iz te uredbe uporabljati določbe o ugotavljanju skladnosti iz te uredbe. V tem primeru bi se morale za vse druge vidike, zajete z Uredbo [uredba o umetni inteligenci], uporabljati zadevne določbe o ugotavljanju skladnosti na podlagi notranje kontrole, navedene v Prilogi VI k Uredbi [uredba o umetni inteligenci].

(30) Za stroje in strojno opremo, ki spadajo na področje uporabe Uredbe [uredba o strojih in strojni opremi] in so izdelki z digitalnimi elementi v smislu te uredbe ter za katere je bila izdana izjava o skladnosti na podlagi te uredbe, bi bilo treba šteti, da so v skladu z bistvenimi zdravstvenimi in varnostnimi zahtevami iz [Priloga III, oddelka 1.1.9 in 1.2.1] k Uredbi [uredba o strojih in strojni opremi] v zvezi z zaščito pred zlorabo ter varnostjo in zanesljivostjo krmilnih sistemov, če izjava EU o skladnosti, izdana na podlagi te uredbe, dokazuje skladnost za navedenimi zahtevami.

(31) Uredba [predlog uredbe o evropskem zdravstvenem podatkovnem prostoru] dopolnjuje bistvene zahteve iz te uredbe. Zato bi morali tudi sistemi za vodenje elektronskih zdravstvenih zapisov, ki spadajo na področje uporabe Uredbe [predlog uredbe o evropskem zdravstvenem podatkovnem prostoru] in so izdelki z digitalnimi elementi v smislu te uredbe, izpolnjevati bistvene zahteve iz te uredbe. Proizvajalci takih sistemov bi morali dokazati skladnost, kot se zahteva z Uredbo [predlog uredbe o evropskem zdravstvenem podatkovnem prostoru]. Za olajšanje zagotavljanja skladnosti lahko pripravijo enotno tehnično dokumentacijo z elementi, ki se zahtevajo z obema pravnima aktoma. Ker ta uredba ne zajema programske opreme kot storitve kot take, sistemi za vodenje elektronskih zdravstvenih zapisov, ki se zagotavljajo na podlagi modela licenciranja in zagotavljanja programske opreme kot storitve, ne spadajo na področje uporabe te uredbe. Prav tako na področje uporabe te uredbe ne spadajo sistemi za vodenje elektronskih zdravstvenih zapisov, ki se razvijajo in uporabljajo v organizaciji, saj se ne dajo na trg.

(32) Za zagotovitev, da so izdelki z digitalnimi elementi varni, ko se dajo na trg in v celotnem življenjskem ciklu, je treba določiti bistvene zahteve 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 v zvezi z obravnavanjem ranljivosti in zagotoviti, da se vsi njihovi izdelki zagotovijo brez znanih ranljivosti, ki jih je mogoče izrabljati, poleg tega pa bi morali ugotoviti, katere druge bistvene zahteve v zvezi z lastnostmi izdelkov so pomembne za zadevno vrsto izdelka. Zato bi morali oceniti tveganja za kibernetsko varnost,

povezana z izdelkom z digitalnimi elementi, da ugotovijo zadevna tveganja in bistvene zahteve ter ustrezno uporabijo primerne harmonizirane standarde ali skupne specifikacije.

(33) Za izboljšanje varnosti izdelkov z digitalnimi elementi, ki se dajo na notranji trg, je treba določiti bistvene zahteve. Te ne bi smele vplivati na usklajene ocene tveganja v EU za kritične oskrbovalne verige iz [člen X] Direktive [Direktiva XXX/XXXX(NIS2)][16], pri katerih se upoštevajo tehnični in po potrebi netehnični dejavniki tveganja, kot je neupravičen vpliv tretje države na dobavitelje. Poleg tega ne bi smele vplivati na pravice držav članic, da določijo dodatne zahteve za zagotovitev visoke ravni odpornosti, pri katerih se upoštevajo netehnični dejavniki, vključno z dejavniki, opredeljenimi v Priporočilu (EU) 2019/534, iz usklajene ocene tveganj za varnost omrežij 5G na ravni Unije in zbirke orodij za kibernetsko varnost 5G, o kateri se je dogovorila skupina za sodelovanje na področju varnosti omrežij in informacijskih sistemov iz [Direktiva XXX/XXXX (NIS2)].

(34) Za zagotovitev, da nacionalne skupine CSIRT in enotne kontaktne točke, imenovane v skladu s členom [člen X] Direktive [Direktiva XX/XXXX (NIS2)], prejmejo informacije, potrebne za opravljanje njihovih nalog in povišanje splošne ravni kibernetske varnosti bistvenih in pomembnih subjektov, ter za zagotovitev učinkovitega delovanja organov za nadzor trga bi morali proizvajalci izdelkov z digitalnimi elementi agencijo ENISA uradno obvestiti o aktivno izrabljenih ranljivostih. 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. Proizvajalci bi morali razmisliti tudi o razkritju odpravljenih ranljivosti v evropski zbirki podatkov o ranljivostih, vzpostavljeni na podlagi Direktive [Direktiva XX/XXXX (NIS2)], ki jo upravlja agencija ENISA, ali v kateri koli drugi javno dostopni zbirki podatkov o ranljivostih.

(35) Proizvajalci bi morali agenciji ENISA sporočiti tudi vsak incident, ki vpliva na varnost izdelka z digitalnimi elementi. Ne glede na obveznosti poročanja o incidentih iz Direktive [Direktiva XX/XXXX (NIS2)], ki veljajo za bistvene in pomembne subjekte, je za agencijo ENISA, enotne kontaktne točke, ki jih države članice imenujejo v skladu s členom [člen X] Direktive [Direktiva XXX/XXXX (NIS2)], ter organe za nadzor trga ključno, da od izdelovalcev izdelkov z digitalnimi elementi prejmejo informacije, na podlagi katerih lahko ocenijo varnost teh izdelkov. Da bi se lahko uporabniki hitro odzvali na incidente, ki vplivajo na varnost njihovih izdelkov z digitalnimi elementi, bi morali proizvajalci tudi obvestiti njihove uporabnike o vseh takih incidentih in po potrebi 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, če ga lahko proizvajalec vzpostavi in tveganja to upravičujejo.

(36) Proizvajalci izdelkov z digitalnimi elementi bi morali vzpostaviti politike usklajenega razkrivanja ranljivosti, da lahko posamezniki ali subjekti lažje poročajo o ranljivostih. 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. Ker se lahko informacije o ranljivostih, ki jih je mogoče

[16] Direktiva XXX Evropskega parlamenta in Sveta z dne [datum] [o ukrepih za visoko skupno raven kibernetske varnosti v Uniji in razveljavitvi Direktive (EU) 2016/1148 (UL L xx, datum, str. x)].

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 (tako imenovane „nagradne programe za prijavljanje hroščev“).

(37) Za olajšanje 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 oskrbovalne verige, kar ima številne koristi, predvsem pa proizvajalcem in uporabnikom pomaga spremljati znane nove ranljivosti in tveganja. Za proizvajalce je pomembno zlasti, da zagotovijo, da njihovi izdelki ne vsebujejo ranljivih sestavnih delov, ki jih razvijajo tretje osebe.

(38) Za olajšanje 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 iz te uredbe prenesejo na podrobne tehnične specifikacije in ki se sprejmejo v skladu z Uredbo (EU) št. 1025/2012 Evropskega parlamenta in Sveta[17]. Uredba (EU) št. 1025/2012 določa postopek za nasprotovanje harmoniziranim standardom, kadar navedeni standardi ne izpolnjujejo zahtev iz te uredbe v celoti.

(39) Z Uredbo (EU) 2019/881 je vzpostavljen prostovoljen evropski certifikacijski okvir za kibernetsko varnost za izdelke, postopke in storitve IKT. Evropske certifikacijske sheme kibernetske varnosti lahko vključujejo izdelke z digitalnimi elementi, zajete s to uredbo. Ta uredba bi morala ustvariti sinergije z Uredbo (EU) 2019/881. Za olajšanje 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 sheme kibernetske varnosti v skladu z Uredbo (EU) 2019/881, pri čemer je Komisija opredelila navedeno shemo v izvedbenem aktu, domneva, da izpolnjujejo bistvene zahteve iz te uredbe, kolikor certifikat kibernetske varnosti ali izjava o skladnosti ali njuni deli zajemajo navedene zahteve. Potrebo po novih evropskih certifikacijskih shemah kibernetske varnosti za izdelke z digitalnimi elementi bi bilo treba oceniti ob upoštevanju te uredbe. Pri takih prihodnjih evropskih certifikacijskih shemah kibernetske varnosti, ki vključujejo izdelke z digitalnimi elementi, bi se morale upoštevati bistvene zahteve iz te uredbe, navedene sheme pa bi morale olajšati skladnost s to uredbo. Na Komisijo bi bilo treba prenesti pooblastilo, da z izvedbenimi akti določi evropske certifikacijske sheme kibernetske varnosti, ki se lahko uporabljajo za dokazovanje skladnosti z bistvenimi zahtevami iz te uredbe. Poleg tega bi morala Komisija za preprečitev nepotrebnega upravnega bremena za proizvajalce po potrebi navesti, ali se s certifikatom kibernetske varnosti, izdanim v okviru takih evropskih certifikacijskih shem kibernetske varnosti, odpravi obveznost izdelovalcev, da za ustrezne zahteve zagotovijo ugotavljanje skladnosti, ki ga opravi tretja oseba, kot je določeno v tej uredbi.

---

[17] 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).

(40) Po začetku veljavnosti izvedbenega akta o določitvi evropske certifikacijske sheme kibernetske varnosti s skupnimi merili [Izvedbena uredba Komisije (EU) …/... z dne XXX o evropski certifikacijski shemi kibernetske varnosti s skupnimi merili], ki se nanaša na izdelke strojne opreme, zajete s to uredbo, kakor so varnostni moduli strojne opreme in mikroprocesorji, lahko Komisija z izvedbenim aktom določi, kako evropska certifikacijska shema kibernetske varnosti s skupnimi merili zagotavlja domnevo o skladnosti z bistvenimi zahtevami iz Priloge I k tej uredbi ali njihovimi deli. Poleg tega se lahko s takim izvedbenim aktom določi, kako se s certifikatom, izdanim v okviru evropske certifikacijske sheme kibernetske varnosti s skupnimi merili, odpravi obveznost izdelovalcev, da za ustrezne zahteve zagotovijo ugotavljanje skladnosti, ki ga opravi tretja oseba, kot se zahteva s to uredbo.

(41) Kadar harmonizirani standardi niso bili sprejeti ali nezadostno obravnavajo bistvene zahteve iz te uredbe, bi morala imeti Komisija možnost, da z izvedbenimi akti sprejme skupne specifikacije. Med razlogi za to, da se namesto harmoniziranih standardov razvijejo take skupne specifikacije, bi lahko bili zavrnitev zahteve za standardizacijo s strani katere od evropskih organizacij za standardizacijo, neupravičene zamude pri določitvi ustreznih harmoniziranih standardov ali neskladnost razvitih standardov z zahtevami iz te uredbe ali zahtevo Komisije. Za olajšanje ugotavljanja skladnosti z bistvenimi zahtevami 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 v skladu s to uredbo za določitev podrobnih tehničnih specifikacij navedenih zahtev.

(42) Proizvajalci bi morali pripraviti izjavo EU o skladnosti, da se zagotovijo informacije, ki se zahtevajo s to uredbo, o skladnosti izdelkov z digitalnimi elementi z bistvenimi zahtevami iz te uredbe in po potrebi druge ustrezne harmonizacijske zakonodaje Unije, ki zajema zadevni izdelek. Priprava izjave EU o skladnosti se lahko od izdelovalcev zahteva tudi z drugo zakonodajo Unije. Da bi se zagotovil učinkovit dostop do informacij za namene nadzora trga, bi bilo treba pripraviti enotno izjavo EU o skladnosti za vse ustrezne akte Unije. Omogočiti bi bilo treba, da je taka enotna izjava EU o skladnosti tudi dosje z zadevnimi posameznimi izjavami o skladnosti, da se zmanjša upravno breme gospodarskih subjektov.

(43) 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[18]. 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.

(44) Da bi lahko gospodarski subjekti dokazali skladnost z bistvenimi zahtevami 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[19] določa module za postopke ugotavljanja skladnosti, ki so sorazmerni z ravnjo tveganja in zahtevano ravnjo varnosti. Za zagotovitev medsektorske skladnosti in preprečitev *ad hoc* različic

---

[18] 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).

[19] 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).

postopki ugotavljanja skladnosti, primerni za preverjanje skladnosti izdelkov z digitalnimi elementi z bistvenimi zahtevami iz te uredbe, temeljijo na navedenih 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.

(45) Splošno pravilo je, da proizvajalec na lastno odgovornost opravi ugotavljanje skladnosti izdelkov z digitalnimi elementi v skladu s postopkom na podlagi modula A iz Sklepa št. 768/2008/ES. Proizvajalec bi moral ohraniti prožnost, da izbere strožji postopek ugotavljanja skladnosti, pri katerem sodeluje tretja oseba. Če je izdelek opredeljen kot kritični izdelek iz razreda I, je potrebno dodatno zagotovilo, da se dokaže skladnost z bistvenimi zahtevami iz te uredbe. Proizvajalec, ki želi na lastno odgovornost opraviti ugotavljanje skladnosti (modul A), bi moral uporabiti harmonizirane standarde, skupne specifikacije ali certifikacijske sheme kibernetske varnosti na podlagi Uredbe (EU) 2019/881, ki jih je Komisija opredelila v izvedbenem aktu. Če ne uporabi takih harmoniziranih standardov, skupnih specifikacij ali certifikacijskih shem kibernetske varnosti, bi moral izvesti ugotavljanje skladnosti, pri katerem sodeluje tretja oseba. 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 + C oziroma modulu H iz Sklepa št. 768/2008/ES, izbrani kot najustreznejši za sorazmerno in učinkovito ugotavljanje skladnosti kritičnih 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 izdelkov, opredeljenih kot kritični izdelki iz razreda II, bi morala pri ugotavljanju skladnosti vselej sodelovati tretja oseba.

(46) Medtem ko so pri ustvarjanju materialnih izdelkov z digitalnimi elementi običajno potrebna precejšnja prizadevanja izdelovalcev 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 iz te uredbe v fazah zasnove, razvoja in proizvodnje.

(47) 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 navzkrižja interesov.

(48) 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.

(49) 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 takem primeru 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.

(50) Organi za ugotavljanje skladnosti za dele svojih dejavnosti, povezanih z ugotavljanjem skladnosti, pogosto najamejo podizvajalca ali jih prenesejo na odvisno družbo. Za ohranitev ravni varstva, ki se zahteva za izdelke z digitalnimi elementi, ki bodo dani na trg, je bistveno, da podizvajalci in odvisne družbe za opravljanje nalog ugotavljanja skladnosti izpolnjujejo iste zahteve kot priglašeni organi.

(51) Priglasitveni organ bi moral Komisiji in drugim državam članicam priglasiti organ za ugotavljanje skladnosti prek informacijskega sistema o priglašenih in imenovanih organih po Novem pristopu (NANDO). Informacijski sistem NANDO je elektronsko orodje za priglasitev, ki ga je razvila in ga upravlja Komisija ter vsebuje seznam vseh priglašenih organov.

(52) Ker lahko priglašeni organi ponujajo svoje storitve po vsej Uniji, je primerno dati drugim državam članicam in Komisiji možnost, da izrazijo nasprotovanje 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.

(53) 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 doslednost pri tehnični uporabi postopkov ugotavljanja skladnosti. To bi bilo mogoče najbolje doseči z ustreznim usklajevanjem in sodelovanjem priglašenih organov.

(54) Nadzor trga je ključno sredstvo za zagotavljanje pravilne in enotne uporabe zakonodaje 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 Evropskega parlamenta in Sveta[20], se uporabljajo za izdelke z digitalnimi elementi, vključene v to uredbo.

(55) V skladu z Uredbo (EU) 2019/1020 organi za nadzor trga izvajajo nadzor trga na ozemlju zadevne države članice. Ta uredba državam članicam ne bi smela preprečevati izbire pristojnih organov za izvedbo navedenih nalog. Vsaka država članica bi morala imenovati en ali več organov za nadzor trga na svojem ozemlju. Države članice lahko za opravljanje nalog organa za nadzor trga imenujejo kateri koli obstoječi ali nov organ, vključno s pristojnimi nacionalnimi organi iz člena [člen X] Direktive [Direktiva XXX/XXXX (NIS2)] ali imenovanimi nacionalnimi certifikacijskimi organi za kibernetsko varnost iz člena 58 Uredbe (EU) 2019/881. Gospodarski subjekti bi morali v celoti sodelovati z organi za nadzor trga in drugimi pristojnimi organi.

[20] 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).

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 v zvezi s to uredbo. V skladu s členom 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.

(56) V skladu s členom 30(2) Uredbe (EU) 2019/1020 bi bilo treba ustanoviti namensko skupino za upravno koordinacijo (ADCO) za enotno uporabo te uredbe. 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, njenih podskupin in zadevne skupine ADCO. Poleg tega bi morala pomagati tej skupini ADCO z izvršnim sekretariatom, ki zagotavlja tehnično in logistično podporo.

(57) Za zagotovitev pravočasnih, sorazmernih in učinkovitih ukrepov v zvezi z izdelki z digitalnimi elementi, ki predstavljajo povečano tveganje za kibernetsko varnost, bi bilo treba predvideti 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.

(58) 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 zakonodaje Unije ali nacionalne zakonodaje, namenjene varstvu temeljnih pravic, tveganje za razpoložljivost, avtentičnost, celovitost ali zaupnost storitev, ki jih z uporabo elektronskega informacijskega sistema zagotavljajo bistveni subjekti iz [Priloge I k Direktivi XXX/XXXX (NIS2)], ali tveganje za druge vidike zaščite javnega interesa. Treba je torej določiti pravila, s katerimi se zmanjšajo navedena tveganja. Zato bi morali organi za nadzor trga sprejeti ukrepe in od gospodarskega subjekta zahtevati, da zagotovi, da izdelek ne predstavlja več tveganja, ga odpokliče ali umakne, odvisno od tveganja. Ko organ za nadzor trga tako omeji ali prepove prosti pretok izdelka, 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, ki predstavljajo tveganje, bi se morala Komisija nemudoma posvetovati z državami članicami in zadevnim gospodarskim subjektom ali subjekti ter oceniti nacionalni ukrep. Na podlagi rezultatov te ocene bi se morala 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, lahko Komisija razmisli tudi o sprejetju predlogov za revizijo zadevne zakonodaje Unije.

(59) Komisija lahko 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 je tveganje za zdravje ali varnost oseb, temeljne pravice ali opravljanje storitev bistvenih subjektov iz [Priloge I k Direktivi XXX/XXXX (NIS2)], od agencije ENISA zahteva, naj opravi oceno. Na podlagi te ocene lahko Komisija z izvedbenimi akti sprejme popravne ali omejevalne ukrepe na ravni Unije, vključno z odreditvijo umika zadevnih izdelkov s trga ali njihovega odpoklica v razumnem roku, ki je sorazmeren z naravo tveganja. Komisija lahko uporabi take ukrepe samo v izjemnih okoliščinah, ki upravičujejo takojšnje ukrepanje za ohranitev dobrega delovanja notranjega trga, in samo, če organi za nadzor niso sprejeli učinkovitih ukrepov za odpravo težave. Take izjemne okoliščine so lahko izredne razmere, v katerih na primer proizvajalec zagotovi splošno dostopnost neskladnega izdelka v več državah članicah in navedeni izdelek v ključnih sektorjih uporabljajo tudi subjekti s področja uporabe [Direktive XXX/XXXX (NIS2)], pri čemer pa vključuje znane ranljivosti, ki jih izrabljajo zlonamerni akterji in za katere proizvajalec ne zagotovi razpoložljivih popravkov. Komisija lahko v takih izrednih razmerah posreduje samo med trajanjem izjemnih okoliščin in če se neskladnost s to uredbo ali pomembna tveganja ne odpravijo.

(60) 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.

(61) Sočasni usklajeni kontrolni ukrepi (usklajena preiskava) 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 pogosto predstavljajo tveganja za kibernetsko varnost. Agencija ENISA bi morala organom za nadzor trga predložiti predloge za kategorije izdelkov, za katere bi se lahko organizirale usklajene preiskave, med drugim na podlagi uradnih obvestil o ranljivostih izdelkov in incidentih, ki jih prejme.

(62) Za zagotovitev, da se lahko regulativni okvir po potrebi prilagodi, bi bilo treba na Komisijo v skladu s členom 290 Pogodbe prenesti pooblastilo za sprejemanje aktov v zvezi s posodobitvami seznama kritičnih izdelkov iz Priloge III ter določitvijo opredelitev teh kategorij izdelkov. 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 navedene 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 nekaterih zelo kritičnih izdelkov z digitalnimi elementi na podlagi meril kritičnosti iz te uredbe ter za določitev minimalne vsebine izjave EU 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[21]. 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.

(63) Za zagotovitev enotnih pogojev izvajanja te uredbe bi bilo treba na Komisijo prenesti izvedbena pooblastila za: določitev oblike in elementov kosovnice za programsko opremo, podrobnejšo določitev vrste informacij, oblike in postopka za uradna obvestila o aktivno izrabljenih ranljivostih in incidentih, ki jih agenciji ENISA predložijo proizvajalci, določitev evropskih certifikacijskih shem kibernetske varnosti, sprejetih v skladu z Uredbo (EU) 2019/881, ki se lahko uporabljajo za dokazovanje skladnosti z bistvenimi zahtevami iz Priloge I k tej uredbi ali njihovimi deli, sprejetje skupnih specifikacij v zvezi z bistvenimi zahtevami iz Priloge I, določitev tehničnih specifikacij za piktograme ali druge oznake v zvezi z varnostjo izdelkov z digitalnimi elementi in mehanizmov za spodbujanje njihove uporabe, sprejetje odločitve o popravnih ali omejevalnih ukrepih na ravni Unije v izjemnih okoliščinah, ki upravičujejo takojšnje ukrepanje za ohranitev dobrega delovanja notranjega trga. Navedena pooblastila bi bilo treba izvajati v skladu z Uredbo (EU) št. 182/2011 Evropskega parlamenta in Sveta[22].

(64) 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.

(65) 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 nacionalnih zakonih. 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, kakor so morebitne upravne globe, ki so jih istemu gospodarskemu subjektu za podobne kršitve že naložili drugi organi za nadzor trga. Take okoliščine so lahko oteževalne, 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.

(66) Kadar se upravne globe naložijo osebam, ki niso 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.

---

21 UL L 123, 12.5.2016, str. 1.

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

(67) EU si v odnosih s tretjimi državami prizadeva za spodbujanje mednarodne trgovine z reguliranimi proizvodi. 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 državami. Sporazumi so sklenjeni za več specifičnih sektorjev, ki se lahko od države do države razlikujejo. Za dodatno spodbujanje trgovine in ob upoštevanju, da so oskrbovalne 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 s to uredbo. Sodelovanje s partnerskimi državami je prav tako pomembno za okrepitev kibernetske odpornosti na svetovni ravni, saj bo to dolgoročno prispevalo k okrepljenemu okviru kibernetske varnosti v EU in zunaj nje.

(68) Komisija bi morala v posvetovanju z zainteresiranimi stranmi redno pregledovati to uredbo, zlasti da bi ugotovila, ali jo je treba prilagoditi spremenjenim družbenim, političnim, tehnološkim ali tržnim razmeram.

(69) Gospodarskim subjektom bi bilo treba zagotoviti dovolj časa za prilagoditev zahtevam iz te uredbe. Ta uredba bi se morala začeti uporabljati [24 mesecev] po začetku njene veljavnosti, razen obveznosti poročanja v zvezi z aktivno izkoriščenimi ranljivostmi in incidenti, ki bi se morale začeti uporabljati [12 mesecev] od začetka veljavnosti te uredbe.

(70) 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.

(71) V skladu s členom 42(1) Uredbe (EU) 2018/1725 Evropskega parlamenta in Sveta[23] je bilo opravljeno posvetovanje z Evropskim nadzornikom za varstvo podatkov, ki je mnenje podal […] –

SPREJELA NASLEDNJO UREDBO:

POGLAVJE I

SPLOŠNE DOLOČBE

Člen 1

Predmet urejanja

[23] 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).

Ta uredba določa:

(a) pravila za dajanje izdelkov z digitalnimi elementi na trg za zagotovitev njihove kibernetske varnosti;

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

(c) bistvene zahteve za postopke obravnavanja ranljivosti, ki jih vzpostavijo proizvajalci, za zagotovitev kibernetske varnosti izdelkov z digitalnimi elementi v celotnem življenjskem ciklu ter obveznosti gospodarskih subjektov v zvezi s temi postopki;

(d) pravila o nadzoru trga ter izvrševanju navedenih pravil in zahtev.

Člen 2

Področje uporabe

1. Ta uredba se uporablja za izdelke z digitalnimi elementi, katerih predvidena 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 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. 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 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 navedene izdelke, ter

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

   V skladu s členom 50 se na Komisijo prenese pooblastilo za sprejemanje delegiranih aktov za spremembo te uredbe, s katerimi se določi, ali je potrebna taka omejitev ali izključitev, ter navedejo zadevni izdelki in pravila ter obseg omejitve, če je ustrezno.

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

Člen 3

Opredelitev pojmov

V tej uredbi se uporabljajo naslednje opredelitve pojmov:

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

(2) „daljinska obdelava podatkov“ pomeni vsako 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) „kritični izdelek z digitalnimi elementi“ pomeni izdelek z digitalnimi elementi, ki predstavlja tveganje za kibernetsko varnost v skladu z merili iz člena 6(2) in katerega osnovna funkcija je navedena v Prilogi III;

(4) „zelo kritični izdelek z digitalnimi elementi“ pomeni izdelek z digitalnimi elementi, ki predstavlja tveganje za kibernetsko varnost v skladu z merili iz člena 6(5);

(5) „operativna tehnologija“ pomeni programirljive digitalne sisteme ali naprave, ki vzajemno delujejo s fizičnim okoljem ali upravljajo naprave, ki vzajemno delujejo s fizičnim okoljem;

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

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

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

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

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

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

(12) „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;

(13) „privilegij“ pomeni pravico dostopa, dodeljeno posameznim uporabnikom ali programom za izvajanje operacij, pomembnih za varnost, v elektronskem informacijskem sistemu;

(14) „razširjeni privilegij“ pomeni pravico dostopa, dodeljeno posameznim uporabnikom ali programom za izvajanje razširjenega nabora operacij, pomembnih za varnost, v elektronskem informacijskem sistemu, pri čemer lahko zloraba ali ogroženost te pravice zlonamernemu akterju omogoči, da pridobi širši dostop do virov sistema ali organizacije;

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

(16) „omrežni in računalniški viri“ pomeni podatkovno funkcijo ali funkcijo strojne ali programske opreme, ki je dostopna lokalno ali prek omrežja ali druge povezane naprave;

(17) „gospodarski subjekt“ pomeni proizvajalca, pooblaščenega predstavnika, uvoznika, distributerja ali katero koli drugo fizično ali pravno osebo, za katero veljajo obveznosti iz te uredbe;

(18) „proizvajalec“ pomeni vsako 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 blagovno znamko, bodisi za plačilo bodisi brezplačno;

(19) „pooblaščeni predstavnik“ pomeni vsako fizično ali pravno osebo s sedežem v Uniji, ki jo je proizvajalec pisno pooblastil, da v njegovem imenu izvaja določene naloge;

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

(21) „distributer“ pomeni vsako fizično ali pravno osebo v oskrbovalni verigi, razen proizvajalca ali uvoznika, ki omogoči dostopnost izdelka z digitalnimi elementi na trgu Unije, ne da bi vplivala na njegove lastnosti;

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

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

(24) „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;

(25) „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;

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

(27) „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;

(28) „ugotavljanje skladnosti“ pomeni postopek preverjanja, ali so bistvene zahteve iz Priloge I izpolnjene;

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

(30) „priglašeni organ“ pomeni organ za ugotavljanje skladnosti, imenovan v skladu s členom 33 te uredbe in drugo ustrezno harmonizacijsko zakonodajo Unije;

(31) „bistvena sprememba“ pomeni spremembo izdelka z digitalnimi elementi po tem, ko je bil dan na trg, ki vpliva na skladnost navedenega izdelka z bistvenimi zahtevami iz

oddelka 1 Priloge I ali povzroči spremembo predvidene uporabe, za katero je bil izdelek z digitalnimi elementi ocenjen;

(32) „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 iz Priloge I in druge zakonodaje Unije o harmonizaciji pogojev za trženje proizvodov (v nadaljnjem besedilu: harmonizacijska zakonodaja Unije), ki se uporablja in določa namestitev oznake;

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

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

(35) „tveganje za kibernetsko varnost“ pomeni tveganje, kakor je opredeljeno v členu [člen X] Direktive [Direktiva XXX/XXXX (NIS2)];

(36) „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;

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

(38) „ranljivost“ pomeni ranljivost, kakor je opredeljena v členu [člen X] Direktive [Direktiva XXX/XXXX (NIS2)];

(39) „aktivno izrabljena ranljivost“ pomeni ranljivost, za katero obstajajo zanesljivi dokazi, da je akter izvedel zlonamerno kodo v sistemu brez dovoljenja lastnika sistema;

(40) „osebni podatki“ pomeni podatke, kakor so opredeljeni v členu 4, točka 1, Uredbe (EU) 2016/679.

Člen 4

Prosti pretok

1. Države članice za zadeve, zajete v tej uredbi, ne ovirajo 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 in uporabe izdelka z digitalnimi elementi, ki ni skladen s to uredbo,

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

Člen 5

Zahteve za izdelke z digitalnimi elementi

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

(1) izpolnjujejo bistvene zahteve iz oddelka 1 Priloge I, če se ustrezno namestijo, vzdržujejo, uporabljajo za predvideni namen ali pod razumno predvidljivimi pogoji in po potrebi posodabljajo, ter

(2) so postopki, ki jih je vzpostavil proizvajalec, skladni z bistvenimi zahtevami iz oddelka 2 Priloge I.

Člen 6

Kritični izdelki z digitalnimi elementi

1. Izdelki z digitalnimi elementi, ki spadajo v kategorijo, navedeno v Prilogi III, se štejejo za kritične izdelke z digitalnimi elementi. Za izdelke, katerih osnovna funkcija spada v kategorijo, navedeno v Prilogi III k tej uredbi, se šteje, da spadajo v navedeno kategorijo. Kategorije kritičnih izdelkov z digitalnimi elementi so razdeljene v razred I in razred II, kot sta določena v Prilogi III, s katerima je izražena raven tveganja za kibernetsko varnost, povezana s temi izdelki.

2. V skladu s členom 50 se na Komisijo prenese pooblastilo za sprejemanje delegiranih aktov za spremembo Priloge III z vključitvijo nove kategorije kritičnih izdelkov z digitalnimi elementi na seznam kategorij takih izdelkov ali umikom obstoječe kategorije s seznama. Komisija pri ocenjevanju potrebe po spremembi seznama iz Priloge III upošteva raven tveganja za kibernetsko varnost, povezano s kategorijo izdelkov z digitalnimi elementi. Pri ugotavljanju ravni tveganja za kibernetsko varnost se upošteva eno ali več naslednjih meril:

   (a) funkcija izdelka z digitalnimi elementi, povezana s kibernetsko varnostjo, in to, ali ima izdelek z digitalnimi elementi vsaj eno od naslednjih lastnosti:

      (i) namenjen je uporabi z razširjenim privilegijem ali upravljanju privilegijev;

      (ii) ima neposreden ali privilegiran dostop do omrežnih in računalniških virov;

      (iii) namenjen je nadzoru dostopa do podatkov ali operativne tehnologije;

      (iv) opravlja funkcijo, ki je kritična za zaupanje, zlasti varnostne funkcije, kakor so nadzor omrežja, varnost končnih točk in zaščita omrežja;

   (b) predvidena uporaba v občutljivih okoljih, vključno z uporabo v industrijskih okoljih ali s strani bistvenih subjektov iz Priloge [Priloga I] k Direktivi [Direktiva XXX/XXXX (NIS2)];

   (c) predvidena uporaba za izvajanje kritičnih ali občutljivih funkcij, kakor je obdelava osebnih podatkov;

   (d) morebitni obseg škodljivega vpliva, zlasti v smislu njegove intenzivnosti in zmožnosti, da vpliva na številne različne osebe;

   (e) obseg, v katerem je uporaba izdelkov z digitalnimi elementi že povzročila materialno ali nematerialno izgubo ali motnjo ali resne pomisleke glede uresničitve škodljivega vpliva.

3. V skladu s členom 50 se na Komisijo prenese pooblastilo za sprejetje delegiranega akta za dopolnitev te uredbe z določitvijo opredelitev kategorij izdelkov iz razredov I in II, kot sta določena v Prilogi III. Delegirani akt se sprejme v [12 mesecih od začetka veljavnosti te uredbe].

4. V zvezi s kritičnimi izdelki z digitalnimi elementi se uporabljajo postopki ugotavljanja skladnosti iz člena 24(2) in (3).

5. V skladu s členom 50 se na Komisijo prenese pooblastilo za sprejemanje delegiranih aktov za dopolnitev te uredbe z določitvijo kategorij zelo kritičnih izdelkov z digitalnimi elementi, za katere morajo proizvajalci pridobiti evropski certifikat kibernetske varnosti v okviru evropske certifikacijske sheme kibernetske varnosti v skladu z Uredbo (EU) 2019/881, da dokažejo skladnost z bistvenimi zahtevami iz Priloge I ali njihovimi deli. Komisija pri določanju takih kategorij zelo kritičnih izdelkov z digitalnimi elementi upošteva raven tveganja za kibernetsko varnost, povezano s kategorijo izdelkov z digitalnimi elementi, glede na eno ali več meril iz odstavka 2 in glede na presojo, ali navedeno kategorijo izdelkov:

   (a) uporabljajo ali se nanjo zanašajo bistveni subjekti iz Priloge [Priloga I] k Direktivi [Direktiva XXX/XXXX (NIS2)] oziroma bo morda pomembna za dejavnosti navedenih subjektov v prihodnosti ali

   (b) je pomembna za odpornost celotne oskrbovalne verige izdelkov z digitalnimi elementi proti dogodkom, ki povzročajo motnje.

Člen 7

Splošna varnost izdelkov

Kadar za izdelke z digitalnimi elementi ne veljajo posebne zahteve, ki jih nalaga druga harmonizacijska zakonodaja Unije v smislu [člena 3, točka 25, uredbe o splošni varnosti proizvodov], se z odstopanjem od člena 2(1), tretji pododstavek, točka (b), Uredbe [uredba o splošni varnosti proizvodov] poglavje III, oddelek 1, poglavji V in VII ter poglavja IX do XI Uredbe [uredba o splošni varnosti proizvodov] uporabljajo za navedene izdelke v zvezi z varnostnimi tveganji, ki niso zajeta s to uredbo.

Člen 8

Umetnointeligenčni sistemi velikega tveganja

1. Za izdelke z digitalnimi elementi, opredeljene kot umetnointeligenčni sistemi velikega tveganja v skladu s členom [člen 6] Uredbe [uredba o umetni inteligenci], ki spadajo na področje uporabe te uredbe in izpolnjujejo bistvene zahteve iz oddelka 1 Priloge I k tej uredbi ter v zvezi s katerimi so postopki, ki jih je vzpostavil proizvajalec, skladni z bistvenimi zahtevami iz oddelka 2 Priloge I, se šteje, da so skladni z zahtevami v zvezi s kibernetsko varnostjo iz člena [člen 15] Uredbe [uredba o umetni inteligenci], brez poseganja v druge zahteve v zvezi s točnostjo in robustnostjo iz navedenega člena, če izjava EU o skladnosti, izdana v skladu s to uredbo, dokazuje doseganje ravni varstva, potrebne v skladu z navedenimi zahtevami.

2. Za izdelke in zahteve glede kibernetske varnosti iz odstavka 1 se uporablja ustrezni postopek ugotavljanja skladnosti, kot se zahteva v skladu s členom [člen 43] Uredbe [uredba o umetni inteligenci]. Za namene navedenega ugotavljanja imajo priglašeni organi, ki imajo pravico nadzorovati skladnost umetnointeligenčnih sistemov velikega tveganja na podlagi Uredbe [uredba o umetni inteligenci], tudi pravico nadzorovati skladnost navedenih sistemov, 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 29 te uredbe ocenjena v okviru postopka priglasitve na podlagi uredbe [uredba o umetni inteligenci].

3. Z odstopanjem od odstavka 2 se za kritične izdelke z digitalnimi elementi iz Priloge III k tej uredbi, za katere je treba uporabljati postopke ugotavljanja skladnosti iz člena 24(2), točki (a) in (b), ter člena 24(3), točki (a) in (b), te uredbe ter ki so opredeljeni tudi kot umetnointeligenčni sistemi velikega tveganja v skladu s členom [člen 6] Uredbe [uredba o umetni inteligenci], za katere se uporablja postopek ugotavljanja skladnosti na podlagi notranje kontrole iz Priloge [Priloga VI] k Uredbi [uredba o umetni inteligenci], v zvezi z bistvenimi zahtevami iz te uredbe uporabljajo postopki ugotavljanja skladnosti, kot se zahtevajo s to uredbo.

Člen 9

Stroji in strojna oprema

Za stroje in strojno opremo, ki spadajo na področje uporabe Uredbe [uredba o strojih in strojni opremi] in so izdelki z digitalnimi elementi v smislu te uredbe ter za katere je bila izdana izjava EU o skladnosti na podlagi te uredbe, se šteje, da so v skladu z bistvenimi zdravstvenimi in varnostnimi zahtevami iz Priloge [Priloga III, oddelka 1.1.9 in 1.2.1] k Uredbi [uredba o strojih in strojni opremi] v zvezi z zaščito pred zlorabo ter varnostjo in zanesljivostjo krmilnih sistemov, če izjava EU o skladnosti, izdana na podlagi te uredbe, dokazuje doseganje ravni varstva, potrebne v skladu z navedenimi zahtevami.

POGLAVJE II

OBVEZNOSTI GOSPODARSKIH SUBJEKTOV

Člen 10

Obveznosti proizvajalcev

1. Proizvajalci pri dajanju izdelka z digitalnimi elementi na trg zagotovijo, da je bil zasnovan, razvit in proizveden v skladu z bistvenimi zahtevami iz oddelka 1 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 varnostne incidente in čim bolj zmanjšajo vplive takih incidentov, tudi v zvezi z zdravjem in varnostjo uporabnikov.

3. Proizvajalec pri dajanju izdelka z digitalnimi elementi na trg vključi oceno tveganj za kibernetsko varnost v tehnično dokumentacijo iz člena 23 in Priloge V. Za izdelke z digitalnimi elementi iz člena 8 in člena 24(4), za katere se uporabljajo tudi drugi akti Unije, je lahko ocena tveganj za kibernetsko varnost del ocene tveganj, ki se zahteva v skladu z navedenimi akti Unije. Kadar se določene bistvene zahteve ne uporabljajo za izdelek z digitalnimi elementi, ki se trži, proizvajalec v navedeno dokumentacijo vključi jasno utemeljitev.

4. Za namene izpolnjevanja obveznosti iz odstavka 1 so proizvajalci pri vgradnji sestavnih delov, pridobljenih od tretjih oseb, v izdelke z digitalnimi elementi

ustrezno skrbni. Proizvajalci zagotovijo, da taki sestavni deli ne ogrozijo varnosti izdelka z digitalnimi elementi.

5. Proizvajalec sistematično in na način, ki je sorazmeren z naravo in tveganji za kibernetsko varnost, dokumentira ustrezne vidike kibernetske varnosti v zvezi z izdelkom z digitalnimi elementi, vključno z ranljivostmi, s katerimi se seznani, in morebitnimi ustreznimi informacijami, ki jih zagotovijo tretje osebe, ter po potrebi posodobi oceno tveganj za izdelek.

6. Proizvajalci pri dajanju izdelka z digitalnimi elementi na trg in v predvideni življenjski dobi izdelka ali v obdobju petih let od dajanja izdelka na trg – kar koli od tega je krajše – zagotovijo učinkovito obravnavanje ranljivosti navedenega izdelka v skladu z bistvenimi zahtevami iz oddelka 2 Priloge I.

   Proizvajalci imajo vzpostavljene ustrezne politike in postopke, vključno s politikami usklajenega razkrivanja ranljivosti iz oddelka 2, točka (5), Priloge I, za obravnavo in odpravo morebitnih ranljivosti izdelka z digitalnimi elementi, ki jih sporočijo notranji ali zunanji viri.

7. Proizvajalci pred dajanjem izdelka z digitalnimi elementi na trg pripravijo tehnično dokumentacijo iz člena 23.

   Proizvajalci izvedejo izbrane postopke ugotavljanja skladnosti iz člena 24 ali zagotovijo, da se taki postopki izvedejo.

   Kadar se pri navedenem postopku ugotavljanja skladnosti ugotovi, da je izdelek z digitalnimi elementi skladen z bistvenimi zahtevami iz oddelka 1 Priloge I, postopki, ki jih je vzpostavil proizvajalec, pa so skladni z bistvenimi zahtevami iz oddelka 2 Priloge I, proizvajalci pripravijo izjavo EU o skladnosti v skladu s členom 20 in namestijo oznako CE v skladu s členom 22.

8. Proizvajalci hranijo tehnično dokumentacijo in izjavo EU o skladnosti ter organom za nadzor trga po potrebi omogočijo dostop do njiju še deset let po tem, ko so izdelek z digitalnimi elementi dali na trg.

9. Proizvajalci zagotovijo, da so za izdelke z digitalnimi elementi v serijski proizvodnji vzpostavljeni postopki za ohranjanje njihove skladnosti. Proizvajalec ustrezno upošteva 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 19, na podlagi katerih se potrdi ali preverja skladnost izdelka z digitalnimi elementi.

10. Proizvajalci zagotovijo, da se izdelkom z digitalnimi elementi priložijo informacije in navodila iz Priloge II v elektronski ali fizični obliki. Take informacije in navodila so v jeziku, ki ga uporabniki zlahka razumejo. Take informacije in navodila so jasni, razumljivi in berljivi. Omogočajo varno namestitev, delovanje in uporabo izdelkov z digitalnimi elementi.

11. Proizvajalci izjavo EU o skladnosti priložijo izdelku z digitalnimi elementi ali pa v navodilih in informacijah iz Priloge II navedejo spletni naslov, na katerem je dostopna izjava EU o skladnosti.

12. Po dajanju izdelka z digitalnimi elementi na trg in v predvideni življenjski dobi izdelka ali v obdobju petih let od dajanja izdelka z digitalnimi elementi na trg – kar koli od tega je krajše – proizvajalci, ki ugotovijo ali upravičeno domnevajo, da izdelek z digitalnimi elementi ali postopki, ki jih je vzpostavil proizvajalec, ni v

skladu z bistvenimi zahtevami iz Priloge I, nemudoma sprejmejo potrebne popravne ukrepe, da zagotovijo skladnost navedenega izdelka z digitalnimi elementi ali postopki, ki jih je vzpostavil proizvajalec, ali po potrebi umaknejo izdelek s trga ali ga odpokličejo.

13. 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 iz Priloge I, in sicer v jeziku, ki ga navedeni organ zlahka razume. Na zahtevo navedenega 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.

14. Proizvajalec, ki preneha opravljati dejavnosti in zato ne more izpolniti obveznosti iz te uredbe, o tem 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.

15. Komisija lahko z izvedbenimi akti določi obliko in elemente kosovnice za programsko opremo iz oddelka 2, točka (1), Priloge I. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 51(2).

Člen 11

Obveznosti poročanja za proizvajalce

1. Proizvajalec brez nepotrebnega odlašanja, vsekakor pa v 24 urah po seznanitvi z aktivno izrabljeno ranljivostjo v izdelku z digitalnimi elementi o njej uradno obvesti agencijo ENISA. Uradno obvestilo vključuje podrobnosti v zvezi z zadevno ranljivostjo, po potrebi pa tudi morebitne sprejete popravne ali blažilne ukrepe. Agencija ENISA uradno obvestilo po njegovem prejemu brez nepotrebnega odlašanja, ki ni utemeljeno z razlogi, povezanimi s tveganji za kibernetsko varnost, posreduje skupinam CSIRT zadevnih držav članic, imenovanim za namene usklajenega razkrivanja ranljivosti v skladu s členom [člen X] Direktive [Direktiva XXX/XXXX (NIS2)], ter o sporočeni ranljivosti obvesti organ za nadzor trga.

2. Proizvajalec brez nepotrebnega odlašanja, vsekakor pa v 24 urah po seznanitvi z incidentom, ki vpliva na varnost izdelka z digitalnimi elementi, o njem uradno obvesti agencijo ENISA. Agencija ENISA uradna obvestila brez nepotrebnega odlašanja, ki ni utemeljeno z razlogi, povezanimi s tveganji za kibernetsko varnost, posreduje enotnim kontaktnim točkam zadevnih držav članic, imenovanim v skladu s členom [člen X] Direktive [Direktiva XXX/XXXX (NIS2)], ter o sporočenih incidentih obvesti organ za nadzor trga. Uradno obvestilo o incidentu vključuje informacije o resnosti in vplivu incidenta, po potrebi pa se v njem navede tudi, ali proizvajalec sumi, da je incident posledica nezakonitih ali zlonamernih dejanj, ali meni, da ima čezmejni vpliv.

3. Agencija ENISA informacije, sporočene v skladu z odstavkoma 1 in 2, predloži evropski organizacijski mreži za povezovanje v kibernetski krizi (EU-CyCLONe), ustanovljeni s členom [člen X] Direktive [Direktiva XXX/XXXX (NIS2)], če so take informacije pomembne za usklajeno upravljanje velikih kibernetskih incidentov in kriz na operativni ravni.

4. Proizvajalec po seznanitvi z incidentom brez nepotrebnega odlašanja obvesti uporabnike izdelka z digitalnimi elementi o incidentu, po potrebi pa tudi o popravnih ukrepih, ki jih lahko uporabnik sprejme za zmanjšanje vpliva incidenta.

5. Komisija lahko z izvedbenimi akti podrobneje določi vrsto informacij, obliko in postopek za uradna obvestila, predložena v skladu z odstavkoma 1 in 2. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 51(2).

6. Agencija ENISA na podlagi uradnih obvestil, ki jih prejme v skladu z odstavkoma 1 in 2, pripravi dvoletno tehnično poročilo o novih trendih glede tveganj za kibernetsko varnost pri izdelkih z digitalnimi elementi ter ga predloži skupini za sodelovanje iz člena [člen X] Direktive [Direktiva XXX/XXXX (NIS2)]. Prvo tako poročilo predloži v 24 mesecih po začetku uporabe obveznosti iz odstavkov 1 in 2.

7. Proizvajalec po ugotovitvi ranljivosti v sestavnem delu, vključno z odprtokodnim sestavnim delom, vgrajenim v izdelek z digitalnimi elementi, sporoči ranljivost osebi ali subjektu, ki vzdržuje sestavni del.

Člen 12

Pooblaščeni predstavniki

1. Proizvajalec lahko s pisnim pooblastilom imenuje pooblaščenega predstavnika.

2. Obveznosti iz člena 10(1) do (7), prva alinea, in (9) niso del pooblastila pooblaščenega predstavnika.

3. Pooblaščeni predstavnik izvaja naloge, določene v pooblastilu, ki ga prejme od proizvajalca. Pooblastilo pooblaščenemu predstavniku omogoča, da izvaja vsaj naslednje naloge:

   (a) hrani izjavo EU o skladnosti iz člena 20 in tehnično dokumentacijo iz člena 23 ter organom za nadzor trga omogoči dostop do njiju še deset let po tem, ko je bil izdelek z digitalnimi elementi dan na trg;

   (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 predstavnika.

Člen 13

Obveznosti uvoznikov

1. Uvozniki dajo na trg samo izdelke z digitalnimi elementi, ki so skladni z bistvenimi zahtevami iz oddelka 1 Priloge I, in če so postopki, ki jih je vzpostavil proizvajalec, skladni z bistvenimi zahtevami iz oddelka 2 Priloge I.

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

   (a) je proizvajalec izvedel ustrezne postopke ugotavljanja skladnosti iz člena 24;

   (b) je proizvajalec pripravil tehnično dokumentacijo;

   (c) je izdelek z digitalnimi elementi opremljen z oznako CE iz člena 22 ter so mu priloženi informacije in navodila za uporabo iz Priloge II.

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

4. Uvozniki navedejo svoje ime, registrirano trgovsko ime ali registrirano blagovno znamko, poštni naslov in e-poštni naslov, na katerem so dosegljivi, na izdelku z digitalnimi elementi, če to ni mogoče, 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 zagotovijo, da so izdelku z digitalnimi elementi priloženi navodila in informacije iz Priloge II v jeziku, ki ga uporabniki zlahka razumejo.

6. Uvozniki, ki ugotovijo ali upravičeno domnevajo, da izdelek z digitalnimi elementi, ki so ga dali na trg, ali postopki, ki jih je vzpostavil proizvajalec, niso skladni z bistvenimi zahtevami iz Priloge I, nemudoma sprejmejo potrebne popravne ukrepe, da zagotovijo skladnost navedenega izdelka z digitalnimi elementi ali postopkov, ki jih je vzpostavil proizvajalec, z bistvenimi zahtevami iz Priloge I ali po potrebi umaknejo izdelek s trga ali ga odpokličejo.

   Uvozniki po ugotovitvi ranljivosti 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.

7. Uvozniki še deset let po tem, ko je bil izdelek z digitalnimi elementi dan na trg, hranijo kopijo izjave EU o skladnosti in organom za nadzor trga omogočijo dostop do nje ter zagotovijo, da je tehnična dokumentacija na zahtevo na voljo navedenim organom.

8. 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 iz oddelka 1 Priloge I ter skladnosti postopkov, ki jih je vzpostavil proizvajalec, z bistvenimi zahtevami iz oddelka 2 Priloge I, in to v jeziku, ki ga navedeni organ zlahka razume. Na zahtevo navedenega 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.

9. 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, kolikor je mogoče in na kakršen koli možen način pa tudi uporabnike izdelkov z digitalnimi elementi, danih na trg.

Člen 14

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 10(10) in (11) oziroma člena 13(4).

3. Kadar distributer meni ali upravičeno domneva, da izdelek z digitalnimi elementi ali postopki, ki jih je vzpostavil proizvajalec, niso skladni z bistvenimi zahtevami 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. Kadar izdelek z digitalnimi elementi predstavlja povečano tveganje za kibernetsko varnost, distributer o tem obvesti proizvajalca in organe za nadzor trga.

4. Distributerji, ki 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 z bistvenimi zahtevami iz Priloge I, 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 ugotovitvi ranljivosti 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, z bistvenimi zahtevami iz Priloge I, in to v jeziku, ki ga navedeni organ zlahka razume. Na zahtevo navedenega 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 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, kolikor je mogoče in na kakršen koli možen način pa tudi uporabnike izdelkov z digitalnimi elementi, danih na trg.

Člen 15

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

Uvoznik ali distributer se šteje za proizvajalca za namene te uredbe in zanj veljajo obveznosti proizvajalca iz člena 10 ter člena 11(1), (2), (4) in (7), kadar navedeni uvoznik ali distributer da izdelek z digitalnimi elementi na trg pod svojim imenom ali blagovno znamko ali bistveno spremeni izdelek z digitalnimi elementi, ki je že bil dan na trg.

Člen 16

Drugi primeri, v katerih se uporabljajo obveznosti izdelovalcev

Fizična ali pravna oseba, ki ni proizvajalec, uvoznik ali distributer in ki bistveno spremeni izdelek z digitalnimi elementi, se šteje za proizvajalca za namene te uredbe.

Za navedeno osebo veljajo obveznosti proizvajalca iz člena 10 ter člena 11(1), (2), (4) in (7) za del izdelka, na katerega vpliva bistvena sprememba, ali za celotni izdelek, če bistvena sprememba vpliva na kibernetsko varnost izdelka z digitalnimi elementi kot celoto.

Člen 17

Identifikacija gospodarskih subjektov

1. Gospodarski subjekti organom za nadzor trga na zahtevo predložijo naslednje informacije, če so na voljo:

   (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.

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.

POGLAVJE III

SKLADNOST IZDELKA Z DIGITALNIMI ELEMENTI

Člen 18

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 iz teh standardov ali njihovih delov, določenimi v Prilogi I.

2. Za izdelke z digitalnimi elementi in postopke, ki jih je vzpostavil proizvajalec in ki so v skladu s skupnimi specifikacijami iz člena 19, se domneva, da so skladni z bistvenimi zahtevami iz Priloge I, kolikor te skupne specifikacije vključujejo navedene zahteve.

3. Za izdelke z digitalnimi elementi in postopke, ki jih je vzpostavil proizvajalec, za katere sta bila izjava EU o skladnosti ali certifikat izdana na podlagi evropske certifikacijske sheme kibernetske varnosti, sprejete na podlagi Uredbe (EU) 2019/881 in določene v skladu z odstavkom 4, se domneva, da so skladni z bistvenimi zahtevami iz Priloge I, kolikor se izjava EU o skladnosti ali certifikat kibernetske varnosti ali njuni deli nanašajo na navedene zahteve.

4. Na Komisijo se prenese pooblastilo, da z izvedbenimi akti določi evropske certifikacijske sheme kibernetske varnosti, sprejete v skladu z Uredbo (EU) 2019/881, ki jih je mogoče uporabiti za dokazovanje skladnosti z bistvenimi zahtevami ali njihovimi deli, kot je določeno v Prilogi I. Nadalje, če je ustrezno,

Komisija navede, ali certifikat kibernetske varnosti, izdan na podlagi takih shem, oprosti proizvajalca obveznosti zagotoviti ugotavljanje skladnosti z ustreznimi zahtevami, ki ga opravi tretja oseba, kakor je določeno v členu 24(2), točki (a) in (b), ter členu 24(3), točki (a) in (b). Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 51(2).

Člen 19

Skupne specifikacije

Če harmonizirani standardi iz člena 18 ne obstajajo ali če Komisija meni, da ustrezni harmonizirani standardi ne izpolnjujejo zahtev iz te uredbe ali niso skladni z zahtevo Komisije za standardizacijo, ali če prihaja do neupravičenih zamud pri postopku standardizacije, ali če evropske organizacije za standardizacijo niso sprejele zahteve Komisije glede harmoniziranih standardov, se na Komisijo prenese pooblastilo, da z izvedbenimi akti sprejme skupne specifikacije glede bistvenih zahtev iz Priloge I. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 51(2).

Člen 20

Izjava EU o skladnosti

1. Proizvajalci pripravijo izjavo EU o skladnosti v skladu s členom 10(7) in navedejo, da je bilo dokazano izpolnjevanje veljavnih bistvenih zahtev iz Priloge I.

2. Izjava EU o skladnosti ima vzorčno strukturo, navedeno v Prilogi IV, in vsebuje elemente, opredeljene v ustreznih postopkih ugotavljanja skladnosti iz Priloge VI. Taka izjava se stalno posodablja. Na voljo je v jeziku ali jezikih, ki ga/jih zahteva država članica, v kateri se izdelek z digitalnimi elementi da na trg ali na voljo.

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

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

5. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov v skladu s členom 50, s katerimi se zaradi upoštevanja tehnološkega napredka ta uredba dopolni z dodajanjem elementov minimalni vsebini izjave EU o skladnosti, kakor je določena v Prilogi IV.

Člen 21

Splošna načela oznake CE

Za oznako CE, kakor je opredeljena v členu 3, točka 32, se uporabljajo splošna načela iz člena 30 Uredbe (ES) št. 765/2008.

Člen 22

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 izjavo EU o skladnosti iz člena 20, priloženo izdelku z digitalnimi elementi. Pri izdelkih z digitalnimi elementi v obliki programske opreme se oznaka CE namesti na izjavo EU o skladnosti iz člena 20 ali na spletišče, povezano z izdelkom programske opreme.

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 ali uporabo, določeno v izvedbenih aktih iz odstavka 6.

4. Oznaki CE sledi identifikacijska številka priglašenega organa, če je ta vključen v postopek ugotavljanja skladnosti na podlagi popolnega zagotavljanja kakovosti (na podlagi modula H) iz člena 24.

   Identifikacijsko številko priglašenega organa namesti organ sam ali jo v skladu z njegovimi navodili namesti proizvajalec ali njegov pooblaščeni predstavnik.

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. Če izdelek z digitalnimi elementi ureja druga zakonodaja Unije, ki prav tako določa namestitev oznake CE, taka oznaka kaže, da izdelek izpolnjuje tudi zahteve navedene druge zakonodaje.

6. Komisija lahko z izvedbenimi akti določi tehnične specifikacije glede piktogramov ali katerih koli drugih oznak, ki se nanašajo na varnost izdelkov z digitalnimi elementi, in mehanizme za spodbujanje njihove uporabe. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 51(2).

Člen 23

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 iz Priloge I. Vsebuje vsaj elemente iz Priloge V.

2. Tehnična dokumentacija se pripravi, preden se izdelek z digitalnimi elementi da na trg, in se stalno posodablja, če je ustrezno, in sicer v pričakovani življenjski dobi izdelka ali v obdobju petih let po tem, ko se izdelek z digitalnimi elementi da na trg, pri čemer se upošteva krajše obdobje.

3. Za izdelke z digitalnimi elementi iz člena 8 in člena 24(4), za katere se uporabljajo tudi drugi akti Unije, se pripravi enotna tehnična dokumentacija, ki vsebuje informacije iz Priloge V k tej uredbi in informacije, ki jih zahtevajo navedeni ustrezni 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 50, 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 V.

Člen 24

Postopki ugotavljanja skladnosti izdelkov z digitalnimi elementi

1. Proizvajalec opravi ugotavljanje skladnosti izdelka z digitalnimi elementi in postopkov, ki jih je vzpostavil, da se preveri izpolnjevanje bistvenih zahtev iz Priloge I. Proizvajalec ali njegov pooblaščeni predstavnik dokazujeta skladnost z bistvenimi zahtevami z uporabo enega od naslednjih postopkov:

   (a) postopka notranje kontrole (na podlagi modula A) iz Priloge VI, ali

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

   (c) ugotavljanja skladnosti na podlagi popolnega zagotavljanja kakovosti (na podlagi modula H) iz Priloge VI.

2. Če proizvajalec ali njegov pooblaščeni predstavnik pri ugotavljanju skladnosti kritičnega izdelka z digitalnimi elementi razreda I, kot je določen v Prilogi III, in postopkov, ki jih je vzpostavil proizvajalec, z bistvenimi zahtevami iz Priloge I ne uporabi ali le delno uporabi harmonizirane standarde, skupne specifikacije ali evropske certifikacijske sheme kibernetske varnosti iz člena 18 ali če 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 navedenih bistvenih zahtev uporabi eden od naslednjih dveh postopkov:

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

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

3. Če je izdelek kritični izdelek z digitalnimi elementi razreda II, kakor je določen v Prilogi III, proizvajalec ali njegov pooblaščeni predstavnik dokazuje skladnost z bistvenimi zahtevami iz Priloge I z uporabo enega od naslednjih postopkov:

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

   (b) ugotavljanja skladnosti na podlagi popolnega zagotavljanja kakovosti (na podlagi modula H) iz Priloge VI.

4. Proizvajalci izdelkov z digitalnimi elementi, ki so v Uredbi [uredba o evropskem zdravstvenem podatkovnem prostoru] opredeljeni kot sistemi za vodenje elektronskih zdravstvenih zapisov, dokazujejo skladnost z bistvenimi zahtevami iz Priloge I te uredbe z uporabo ustreznega postopka ugotavljanja skladnosti, kot to zahteva uredba [poglavje III uredbe o evropskem zdravstvenem podatkovnem prostoru].

5. Priglašeni organi pri določanju pristojbin za izvajanje postopkov ugotavljanja skladnosti upoštevajo posebne interese in potrebe malih in srednjih podjetij (MSP)

ter navedene pristojbine zmanjšajo sorazmerno s temi posebnimi interesi in potrebami.

POGLAVJE IV

PRIGLASITEV ORGANOV ZA UGOTAVLJANJE SKLADNOSTI

Člen 25

Priglasitev

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

Člen 26

Priglasitveni organi

1. Države članice določijo priglasitveni organ, ki je odgovoren za vzpostavitev in izvajanje potrebnih postopkov za ocenjevanje in priglasitev organov za ugotavljanje skladnosti ter za spremljanje priglašenih organov, vključno s skladnostjo s členom 31.
2. Države članice lahko določijo, da ocenjevanje in spremljanje iz odstavka 1 izvaja nacionalni akreditacijski organ v smislu Uredbe (ES) št. 765/2008 in v skladu z njo.

Člen 27

Zahteve v zvezi s priglasitvenimi organi

1. Priglasitveni organ se ustanovi tako, da ne pride do navzkrižja 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 28

Obveznost 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 navedene informacije javno dostopne.

Člen 29

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 v skladu z nacionalnim pravom in je pravna oseba.

3. Organ za ugotavljanje skladnosti je organ tretje strani, neodvisen od organizacije ali izdelka, 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, če se dokažeta njegova samostojnost in neobstoj navzkrižja interesov.

4. Organ za ugotavljanje skladnosti, njegovo najvišje vodstvo in osebje, odgovorno za izvajanje nalog ugotavljanja skladnosti, ne smejo biti oblikovalci, razvijalci, proizvajalci, dobavitelji, monterji, kupci, lastniki, uporabniki ali vzdrževalci izdelkov z digitalnimi elementi, ki jih ocenjujejo, niti pooblaščeni predstavniki katere koli izmed navedenih 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, trženju, vgradnji, uporabi ali vzdrževanju navedenih izdelkov in ne 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 VI, 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 se izvaja ugotavljanje skladnosti, da se zagotovita preglednost in zmožnost ponovitve navedenih 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.

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, veljavnih harmoniziranih standardov 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 država 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 VI 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 40, ali zagotovijo, da je njihovo osebje za ugotavljanje skladnosti obveščeno o teh dejavnostih, ter kot splošne smernice uporabljajo upravne odločbe in dokumente, ki so rezultat dela navedene skupine.

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

Člen 30

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 29, kolikor se veljavni harmonizirani standardi nanašajo na navedene zahteve.

Člen 31

Odvisne družbe in podizvajalci priglašenih organov

1. Kadar priglašeni organ za določene naloge, povezane z ugotavljanjem skladnosti, sklene pogodbo s podizvajalcem ali jih prenese na odvisno družbo, zagotovi, da podizvajalec ali odvisna družba izpolnjuje zahteve iz člena 29, ter o tem obvesti priglasitveni organ.
2. Priglašeni organi so v celoti odgovorni za naloge, ki jih izvajajo podizvajalci ali odvisne družbe, ne glede na to, kje imajo ti podizvajalci ali te odvisne družbe sedež.
3. Dejavnosti se lahko prenesejo na podizvajalca ali odvisno družbo le, če proizvajalec s tem soglaša.
4. Priglašeni organi hranijo zadevne dokumente v zvezi z ocenjevanjem usposobljenosti podizvajalca ali odvisne družbe ter nalogami, ki jih izvajajo na podlagi te uredbe, ter omogočajo priglasitvenemu organu dostop do njih.

Člen 32

Vloga za priglasitev

1. Organ za ugotavljanje skladnosti predloži vlogo za priglasitev priglasitvenemu organu države članice, v kateri ima sedež.
2. Vlogi za priglasitev se priloži opis dejavnosti ugotavljanja skladnosti, postopka ali postopkov ugotavljanja skladnosti ter izdelka ali izdelkov, za katere je navedeni organ po lastnih trditvah pristojen, priloži pa se tudi morebitno potrdilo o akreditaciji, ki ga izda nacionalni akreditacijski organ in ki potrjuje, da organ za ugotavljanje skladnosti izpolnjuje zahteve iz člena 29.
3. Če zadevni organ za ugotavljanje skladnosti ne more zagotoviti potrdila o akreditaciji, priglasitvenemu organu predloži vse listinske dokaze, potrebne za preverjanje, priznavanje in redno spremljanje njegove skladnosti z zahtevami iz člena 29.

Člen 33

Postopek priglasitve

1. Priglasitveni organi lahko priglasijo samo tiste organe za ugotavljanje skladnosti, ki izpolnjujejo zahteve iz člena 29.
2. Priglasitveni organ obvesti Komisijo in druge države članice prek informacijskega sistema o priglašenih in imenovanih organih po Novem pristopu (NANDO), 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 ter ustrezno potrdilo o usposobljenosti.

4. Kadar priglasitev ne temelji na potrdilu o akreditaciji iz člena 32(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 29.

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

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

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

Člen 34

Identifikacijske številke in seznami priglašenih organov

1. Komisija priglašenemu organu dodeli identifikacijsko številko.

   Dodeli mu samo eno tako številko, tudi če je organ priglašen na podlagi več 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 navedeni seznam posodablja.

Člen 35

Spremembe priglasitev

1. Če priglasitveni organ ugotovi ali je obveščen, da priglašeni organ ne izpolnjuje več zahtev iz člena 29 ali ne izpolnjuje svojih obveznosti, omeji, začasno prekliče ali prekliče priglasitev, kot je ustrezno glede na resnost neizpolnjevanja navedenih zahtev ali nespoštovanja navedenih obveznosti. O tem takoj obvesti Komisijo in druge države članice.

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

Člen 36

Izpodbijanje usposobljenosti priglašenih organov

1. Komisija razišče vse primere, v katerih dvomi oziroma 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. Če 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 37

Obveznosti priglašenih organov glede njihovega dela

1. Priglašeni organi izvajajo ugotavljanje skladnosti v skladu s postopki ugotavljanja skladnosti iz člena 24 in Priloge VI.

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, sektor, v katerem deluje, njegovo strukturo, stopnjo zahtevnosti tehnologije zadevnega izdelka in masovno ali serijsko naravo proizvodnega postopka.

3. Vendar priglašeni organi upoštevajo stopnjo strogosti in raven zaščite, ki sta potrebni za skladnost izdelka z določbami Uredbe.

4. Če priglašeni organ ugotovi, da proizvajalec ni izpolnil zahtev iz Priloge I ali ustreznih harmoniziranih standardov ali skupnih specifikacij iz člena 19, od njega zahteva, naj sprejme ustrezne popravne ukrepe, in ne izda potrdila o skladnosti.

5. Če priglašeni organ med postopkom spremljanja skladnosti po izdaji potrdila o skladnosti ugotovi, da izdelek 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. Če popravni ukrepi niso sprejeti ali nimajo zahtevanega učinka, priglašeni organ omeji, začasno prekliče ali prekliče katera koli potrdila, kakor je ustrezno.

Člen 38

Obveznost priglašenih organov glede obveščanja

1. Priglašeni organi obvestijo priglasitveni organ o:

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

   (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,

zagotavljajo ustrezne informacije o vprašanjih v zvezi z negativnimi in, na zahtevo, pozitivnimi rezultati ugotavljanja skladnosti.

Člen 39

Izmenjava izkušenj

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

Člen 40

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 navedene skupine.

POGLAVJE V

NADZOR TRGA IN IZVRŠEVANJE

Člen 41

Nadzor trga in nadzor izdelkov z digitalnimi elementi na trgu Unije

1. Uredba (EU) 2019/1020 se uporablja za izdelke z digitalnimi elementi v okviru področja 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. Če 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 v skladu s členom 11 te uredbe imenovani organi za nadzor trga sodelujejo z agencijo ENISA.

4. Če je ustrezno, organi za nadzor trga sodelujejo z drugimi organi za nadzor trga, imenovanimi na podlagi druge harmonizacijske zakonodaje Unije za druge izdelke, in si z njimi redno izmenjujejo informacije.

5. Organi za nadzor trga sodelujejo, kakor je ustrezno, z organi za nadzor zakonodaje Unije o varstvu podatkov. Tako sodelovanje vključuje obveščanje navedenih organov o vseh ugotovitvah, pomembnih za izpolnjevanje njihovih pristojnosti, tudi ko izdajajo smernice in nasvete v skladu z odstavkom 8 tega člena, če se take smernice in nasveti nanašajo na obdelavo osebnih podatkov.

   Organi za nadzor zakonodaje 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.

6. Države članice zagotovijo, da imajo imenovani organi za nadzor trga na voljo ustrezne finančne in človeške vire za izpolnjevanje svojih nalog na podlagi te uredbe.

7. Komisija olajša izmenjavo izkušenj med imenovanimi organi za nadzor trga.

8. Organi za nadzor trga lahko zagotavljajo smernice in nasvete gospodarskim subjektom glede izvajanja te uredbe, ob podpori Komisije.

9. 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 zakonodaje Unije s področja konkurence.

10. Glede izdelkov z digitalnimi elementi na področju uporabe te uredbe, ki so v skladu s členom [člen 6] Uredbe [uredba o umetni inteligenci] opredeljeni kot umetnointeligenčni sistemi velikega tveganja, so organi za nadzor trga, imenovani za namene Uredbe [uredba o umetni inteligenci], organi, ki so odgovorni za dejavnosti nadzora trga, ki se zahtevajo na podlagi te uredbe. Organi za nadzor trga, imenovani v skladu z Uredbo [uredba o umetni inteligenci], sodelujejo, kakor je ustrezno, z organi za nadzor trga, imenovanimi v skladu s to uredbo, v zvezi z nadzorom izvajanja obveznosti poročanja na podlagi člena 11 pa tudi z agencijo ENISA. Organi za nadzor trga, imenovani na podlagi Uredbe [uredba o umetni inteligenci], 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.

11. V skladu s členom 30(2) Uredbe (EU) 2019/1020 se ustanovi namenska skupina za upravno sodelovanje (ADCO) za enotno uporabo te uredbe. Skupino ADCO sestavljajo predstavniki imenovanih organov za nadzor trga in, če je ustrezno, predstavniki enotnih povezovalnih organov.

Člen 42

Dostop do podatkov in dokumentacije

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

Člen 43

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

1. Če 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, 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.

   Če med navedenim ocenjevanjem organ za nadzor trga ugotovi, da izdelek z digitalnimi elementi ne izpolnjuje zahtev iz te uredbe, od zadevnega gospodarskega subjekta nemudoma zahteva, naj sprejme vse ustrezne popravne ukrepe za

zagotovitev, da izdelek izpolnjuje navedene zahteve, ali pa naj izdelek umakne s trga oziroma ga odpokliče v razumnem roku, ki je sorazmeren z naravo tveganja.

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

2. Če 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.

3. Proizvajalec zagotovi izvedbo vseh ustreznih popravnih ukrepov glede vseh zadevnih izdelkov z digitalnimi elementi, katerih dostopnost na trgu je omogočil kjer koli Uniji.

4. Če proizvajalec izdelka z digitalnimi elementi 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 na svojem nacionalnem trgu oziroma za njegov umik ali odpoklic s trga.

Navedeni organ o navedenih ukrepih brez odlašanja obvesti Komisijo in druge države članice.

5. Informacije iz odstavka 4 vsebujejo vse razpoložljive podrobnosti, zlasti podatke, potrebne za identifikacijo neskladnih izdelkov z digitalnimi elementi, poreklo 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 ali postopki, ki jih je vzpostavil proizvajalec, ne izpolnjujejo bistvenih zahtev iz Priloge I;

(b) obstajajo pomanjkljivosti v harmoniziranih standardih, certifikacijskih shemah kibernetske varnosti ali skupnih specifikacijah, navedenih v členu 18.

6. 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, ter o svojih ugovorih v primeru nestrinjanja s priglašenim nacionalnim ukrepom.

7. Če države članice ali Komisija v treh mesecih po prejemu informacij iz odstavka 4 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.

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

Člen 44

Zaščitni postopek Unije

1. Če država članica v treh mesecih od prejema obvestila iz člena 43(4) poda ugovor proti ukrepu, ki ga je sprejela druga država članica, ali če Komisija meni, da je ukrep v nasprotju z zakonodajo Unije, se Komisija brez odlašanja posvetuje z zadevno državo članico in gospodarskim subjektom ali gospodarskimi subjekti ter oceni nacionalni ukrep. Komisija na podlagi rezultatov navedenega ocenjevanja v devetih

mesecih od obvestila iz člena 43(4) odloči, ali je nacionalni ukrep upravičen ali ne, in o taki odločitvi 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 nacionalni ukrep šteje za neupravičenega, ga zadevna država članica odpravi.

3. Če se nacionalni ukrep šteje za upravičenega, vzrok za neskladnost izdelka z digitalnimi elementi pa so pomanjkljivosti v harmoniziranih standardih, Komisija uporabi postopek iz člena 10 Uredbe (EU) št. 1025/2012.

4. Če 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 18, Komisija prouči, ali naj spremeni ali razveljavi izvedbeni akt, kakor je naveden v členu 18(4), ki določa domnevo o skladnosti v zvezi s tako certifikacijsko shemo.

5. Če se nacionalni ukrep šteje za upravičenega, vzrok za neskladnost izdelka z digitalnimi elementi pa so pomanjkljivosti v skupnih specifikacijah iz člena 19, Komisija prouči, ali naj spremeni ali razveljavi izvedbeni akt iz člena 19, v katerem so določene navedene skupne specifikacije.

Člen 45

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

1. Če ima Komisija zadostne razloge za domnevo, 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, lahko od zadevnih organov za nadzor trga zahteva, naj ocenijo skladnost in izvedejo postopke iz člena 43.

2. V izjemnih okoliščinah, ki zahtevajo takojšnje ukrepanje za ohranitev dobrega delovanja notranjega trga, in če ima Komisija zadostne razloge za mnenje, da izdelek iz odstavka 1 še vedno ni skladen z zahtevami iz te uredbe, zadevni organi za nadzor trga pa niso sprejeli učinkovitih ukrepov, lahko Komisija od agencije ENISA zahteva, naj opravi oceno skladnosti. Komisija o tem obvesti zadevne organe za nadzor trga. Zadevni gospodarski subjekti sodelujejo z agencijo ENISA, kakor je potrebno.

3. Komisija se lahko na podlagi ocene agencije ENISA odloči, 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.

4. Na podlagi posvetovanja iz odstavka 3 lahko Komisija sprejme izvedbene akte, s katerimi odloči o popravnih ali omejevalnih ukrepih na ravni Unije, vključno z odreditvijo umika s trga ali odpoklica v razumnem roku, ki je sorazmeren z naravo tveganja. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 51(2).

5. Komisija odločitev iz odstavka 4 takoj sporoči zadevnemu gospodarskemu subjektu ali subjektom. Države članice brez odlašanja izvedejo akte iz odstavka 4 in o tem obvestijo Komisijo.

6. Odstavki 2 do 5 se uporabljajo, dokler trajajo izredne razmere, ki upravičujejo poseg Komisije, in dokler se ne zagotovi skladnost zadevnega izdelka s to uredbo.

Člen 46

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

1. Če organ za nadzor trga države članice po izvedbi ocene iz člena 43 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 varnost ali zdravje oseb, tveganje za skladnost z obveznostmi na podlagi zakonodaje Unije ali nacionalne zakonodaje, namenjene varstvu temeljnih pravic, tveganje za razpoložljivost, avtentičnost, celovitost ali zaupnost storitev, ki jih z uporabo elektronskega informacijskega sistema zagotavljajo bistveni subjekti iz [Priloge I k Direktivi XXX/XXXX (NIS2)], ali tveganje za druge vidike zaščite javnega interesa, od zadevnega gospodarskega subjekta zahteva, naj sprejme vse ustrezne ukrepe za zagotovitev, da zadevni izdelek z digitalnimi elementi in postopki, ki jih je vzpostavil proizvajalec, ko so dani na trg, ne pomenijo več navedenega tveganja, oziroma naj izdelek z digitalnimi elementi umakne s trga ali ga odpokliče v razumnem roku, ki je sorazmeren z naravo tveganja.

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 v skladu z odstavkom 1. Navedene informacije vsebujejo vse razpoložljive podrobnosti, zlasti podatke, potrebne za identifikacijo zadevnih izdelkov z digitalnimi elementi, poreklo in oskrbovalno 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 svojo odločitev naslovi na države članice.

6. Če ima Komisija zadostne razloge za domnevo, 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, lahko od zadevnega organa ali organov za nadzor trga zahteva, naj opravijo oceno skladnosti in izvedejo postopke iz člena 43 ter iz odstavkov 1, 2 in 3 tega člena.

7. V izjemnih okoliščinah, ki zahtevajo takojšnje ukrepanje za ohranitev dobrega delovanja notranjega trga, in če ima Komisija zadostne razloge za mnenje, da izdelek iz odstavka 6 še vedno pomeni tveganja iz odstavka 1, zadevni nacionalni organi za nadzor trga pa niso sprejeli učinkovitih ukrepov, lahko od agencije ENISA zahteva, naj opravi oceno tveganj navedenega izdelka, 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 agencije ENISA 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 lahko Komisija sprejme izvedbene akte, s katerimi odloči o popravnih ali omejevalnih ukrepih na ravni Unije, vključno z odreditvijo umika s trga ali odpoklica v razumnem roku, ki je sorazmeren z naravo tveganja. Navedeni izvedbeni akti se sprejmejo v skladu s postopkom pregleda iz člena 51(2).

10. Komisija odločitev iz odstavka 9 takoj sporoči zadevnemu gospodarskemu subjektu ali subjektom. Države članice takšne 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 še pomeni tveganja iz odstavka 1.

Člen 47

Formalna neskladnost

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

   (a) oznaka skladnosti ni nameščena v skladu s členoma 21 in 22;

   (b) oznaka skladnosti ni nameščena;

   (c) izjava EU o skladnosti ni pripravljena;

   (d) izjava EU o skladnosti ni pravilno pripravljena;

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

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

2. Če 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 48

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, pri katerih se pogosto ugotovi, da pomenijo tveganje za kibernetsko varnost.

2. Komisija ali agencija ENISA lahko 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, ki spadajo na področje uporabe te uredbe, z zahtevami iz te uredbe v več državah članicah.

3. Organi za nadzor trga in Komisija, če 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, če je ustrezno, omogočita dostop javnosti do sporazuma o skupnih dejavnostih, vključno z imeni strank.

Člen 49

Usklajene preiskave

1. Organi za nadzor trga se lahko odločijo za izvajanje sočasnih usklajenih kontrolnih ukrepov (usklajenih preiskav) posameznih izdelkov z digitalnimi elementi ali njihovih kategorij, da se preveri njihova skladnost s to uredbo ali da se odkrijejo kršitve te uredbe.

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

3. Agencija ENISA lahko pri izvajanju svojih nalog, tudi na podlagi obvestil, prejetih v skladu s členom 11(1) in (2), opredeli kategorije izdelkov, glede katerih je mogoče organizirati usklajene preiskave. Predlog za usklajene preiskave se predloži potencialnemu koordinatorju iz odstavka 2 v obravnavo organom za nadzor trga.

4. Pri izvajanju usklajenih preiskav lahko vključeni organi za nadzor trga uporabijo preiskovalna pooblastila iz členov 41 do 47 in vsa druga pooblastila, ki so jim podeljena z nacionalno zakonodajo.

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 50

Izvajanje prenosa pooblastil

1. Pooblastilo za sprejemanje delegiranih aktov se prenese na Komisijo pod pogoji iz tega člena.

2. Na Komisijo se prenese pooblastilo za sprejemanje delegiranih aktov iz člena 2(4), člena 6(2), (3) in (5), člena 20(5) ter člena 23(5).

3. Evropski parlament ali Svet lahko kadar koli prekliče prenos pooblastila iz člena 2(4), člena 6(2), (3) in (5), člena 20(5) ter člena 23(5). S sklepom o preklicu preneha veljati prenos pooblastila, navedenega v njem. Sklep začne veljati dan po njegovi objavi v *Uradnem listu Evropske unije* ali na poznejši datum, kakor 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 imenuje vsaka država članica, v skladu z načeli iz Medinstitucionalnega sporazuma 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 v skladu s členom 2(4), členom 6(2), (3) in (5), členom 20(5) ter členom 23(5), začne veljati le, če mu v dveh mesecih od uradnega obvestila Evropskemu parlamentu in Svetu o navedenem aktu ne nasprotuje nobeden od navedenih dveh organov ali če pred iztekom tega roka Evropski parlament in Svet obvestita Komisijo, da mu ne bosta nasprotovala. Na pobudo Evropskega parlamenta ali Sveta se ta rok podaljša za dva meseca.

Člen 51

Postopek v odboru

1. Komisiji pomaga odbor. Navedeni 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, če se v roku za izdajo mnenja za to odloči predsednik odbora ali tako zahteva član odbora.

POGLAVJE VII

ZAUPNOST IN KAZNI

Člen 52

Zaupnost

1. Vse stranke, 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[24];

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

   (c) javne interese in interese nacionalne varnosti;

   (d) celovitost kazenskih ali upravnih postopkov.

[24] 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).

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 v skladu s kazenskim pravom držav članic.

4. Komisija in države članice lahko izmenjajo, če 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 53

Kazni

1. Države članice določijo pravila o kaznih, ki se uporabljajo za kršitve te uredbe s strani gospodarskih subjektov, in sprejmejo vse potrebne ukrepe za zagotovitev, da se te kazni izvršujejo. Kazni so učinkovite, sorazmerne in odvračilne.

2. Države članice o teh pravilih in ukrepih uradno obvestijo Komisijo brez odlašanja in jo brez odlašanja uradno obvestijo o vsakršni naknadni spremembi, ki nanje vpliva.

3. Neskladnost z bistvenimi zahtevami glede kibernetske varnosti iz Priloge I ter neizpolnjevanje obveznosti iz členov 10 in 11 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.

4. Neizpolnjevanje katere koli druge obveznosti iz te uredbe 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.

5. 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.

6. 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 drugi organi za nadzor trga istemu gospodarskemu subjektu za podobno kršitev že naložili upravne globe;

   (c) velikost in tržni delež gospodarskega subjekta, ki je storil kršitev.

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

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

9. 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 zadevnih državah članicah. Uporaba takih pravil v navedenih državah članicah ima enakovreden učinek.

10. 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.

POGLAVJE VIII

PREHODNE IN KONČNE DOLOČBE

Člen 54

Spremembe Uredbe (EU) 2019/1020

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

„71. [Uredba XXX][akt o kibernetski odpornosti]“.

Člen 55

Prehodne določbe

1. Potrdila o EU-pregledu tipa in sklepi o odobritvi, izdani glede zahtev v zvezi s kibernetsko varnostjo za izdelke z digitalnimi elementi, za katere se uporablja druga harmonizacijska zakonodaja Unije, ostanejo veljavni do [42 mesecev po datumu začetka veljavnosti te uredbe], razen če potečejo pred tem datumom ali če je drugače določeno v drugi zakonodaji Unije, pri čemer v takem primeru ostanejo veljavni, kakor je določeno v navedeni zakonodaji Unije.

2. Za izdelke z digitalnimi elementi, ki so bili dani na trg pred [datum začetka uporabe te uredbe, naveden v členu 57], se zahteve iz te uredbe uporabljajo le, če se navedenim izdelkom po navedenem datumu bistveno spremeni zasnova ali predvideni namen.

3. Z odstopanjem od odstavka 2 se obveznosti iz člena 11 uporabljajo za vse izdelke z digitalnimi elementi na področju uporabe te uredbe, ki so bili dani na trg pred [datum začetka uporabe te uredbe, naveden v členu 57].

Člen 56

Ocena in pregled

Komisija v [36 mesecih po datumu začetka uporabe te uredbe] ter nato vsaka štiri leta Evropskemu parlamentu in Svetu predloži poročilo o oceni in pregledu te uredbe. Poročila se objavijo.

Člen 57

Začetek veljavnosti in uporaba

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

Uporablja se od [24 mesecev od datuma začetka veljavnosti te uredbe]. Člen 11 pa se uporablja od [12 mesecev od datuma začetka veljavnosti te uredbe].

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

V Bruslju,

Za Evropski parlament	*Za Svet*
predsednica	*predsednik*

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

1.2. Zadevna področja

1.3. Ukrep, na katerega se predlog/pobuda nanaša

1.4. Cilji

1.4.1. Splošni cilji

1.4.2. Specifični cilji

1.4.3. Pričakovani rezultati in posledice

1.4.4. Kazalniki smotrnosti

1.5. Utemeljitev predloga/pobude

1.5.1. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno, vključno s podrobno časovnico za uvajanje ustreznih ukrepov za izvajanje pobude

1.5.2. Dodana vrednost ukrepanja Unije (ki je lahko posledica različnih dejavnikov, npr. boljšega usklajevanja, pravne varnosti, večje učinkovitosti ali dopolnjevanja). Za namene te točke je „dodana vrednost ukrepanja Unije“ vrednost, ki izhaja iz ukrepanja Unije in predstavlja dodatno vrednost poleg tiste, ki bi jo sicer ustvarile države članice same.

1.5.3. Spoznanja iz podobnih izkušenj v preteklosti

1.5.4. Skladnost z večletnim finančnim okvirom in možne sinergije z drugimi ustreznimi instrumenti

1.5.5. Ocena različnih razpoložljivih možnosti financiranja, vključno z možnostmi za prerazporeditev

1.6. Trajanje predloga/pobude in finančnih posledic

1.7. Načrtovani načini upravljanja

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

2.2. Upravljavski in kontrolni sistemi

2.2.1. Utemeljitev načinov upravljanja, mehanizmov financiranja, načinov plačevanja in predlagane strategije kontrol

2.2.2. Podatki o ugotovljenih tveganjih in vzpostavljenih sistemih notranjih kontrol za njihovo zmanjševanje

2.2.3. Ocena in utemeljitev stroškovne učinkovitosti kontrol (razmerje „stroški kontrol ÷ vrednost z njimi povezanih upravljanih sredstev“) ter ocena pričakovane stopnje tveganja napake (ob plačilu in ob zaključku)

2.3. Ukrepi za preprečevanje goljufij in nepravilnosti

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

3.2. Ocenjene finančne posledice predloga za odobritve

3.2.1. Povzetek ocenjenih posledic za odobritve za poslovanje

3.2.2. Ocenjene realizacije, financirane z odobritvami za poslovanje

3.2.3. Povzetek ocenjenih posledic za upravne odobritve

3.2.4. Skladnost z veljavnim večletnim finančnim okvirom

3.2.5. Udeležba tretjih oseb pri financiranju

3.3. Ocenjene posledice za prihodke

OCENA FINANČNIH POSLEDIC ZAKONODAJNEGA PREDLOGA

1. OKVIR PREDLOGA/POBUDE

1.1. Naslov predloga/pobude

Predlog uredbe o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi (akt o kibernetski odpornosti)

1.2. Zadevna področja

Komunikacijska omrežja, vsebine in tehnologija

1.3. Ukrep, na katerega se predlog/pobuda nanaša

× **Nov ukrep**

☐ **Nov ukrep na podlagi pilotnega projekta / pripravljalnega ukrepa**[37]

☐ **Podaljšanje obstoječega ukrepa**

☐ **Združitev ali preusmeritev enega ali več ukrepov v drug/nov ukrep**

1.4. Cilji

1.4.1. Splošni cilji

Predlog ima dva glavna cilja, katerih namen je zagotoviti pravilno delovanje notranjega trga: (1) **ustvariti pogoje za razvoj varnih izdelkov z digitalnimi elementi** z zagotavljanjem, da se izdelki strojne in programske opreme dajejo na trg z manj ranljivostmi in da proizvajalci v celotnem življenjskem ciklu izdelka resno obravnavajo vprašanje varnosti, ter (2) **ustvariti pogoje, ki uporabnikom omogočajo upoštevanje kibernetske varnosti pri izbiri in uporabi izdelkov z digitalnimi elementi.**

1.4.2. Specifični cilji

Za predlog so bili oblikovani **štirje specifični cilji:** (i) zagotoviti, da proizvajalci izboljšujejo varnost izdelkov z digitalnimi elementi že od faze zasnove in razvoja ter v celotnem življenjskem ciklu izdelka; (ii) zagotoviti skladen okvir kibernetske varnosti, s čimer se olajša zagotavljanje skladnosti za proizvajalce strojne in programske opreme; (iii) izboljšati preglednost varnostnih lastnosti izdelkov z digitalnimi elementi ter (iv) podjetjem in potrošnikom omogočiti varno uporabo izdelkov z digitalnimi elementi.

Pričakovani rezultati in posledice

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

Predlog bi imel pomembne koristi za različne deležnike. Za podjetja bi preprečil različna varnostna pravila glede izdelkov z digitalnimi elementi in znižal stroške zagotavljanja skladnosti z zadevno zakonodajo o kibernetski varnosti. Zmanjšal bi število kibernetskih incidentov, znižal stroške obvladovanja incidentov in zmanjšal škodo za ugled. Za celotno EU se ocenjuje, da bi se lahko zaradi pobude stroški zaradi incidentov, ki prizadenejo podjetja, znižali za približno 180 do 290

[37] Po členu 58(2)(a) oz. (b) finančne uredbe.

milijard EUR na leto[38]. S pobudo bi se povečal promet zaradi povečanja povpraševanja po izdelkih z digitalnimi elementi. Izboljšal bi se globalni ugled podjetij, zaradi česar bi se povečalo povpraševanje tudi zunaj EU. Za uporabnike bi prednostna možnost izboljšala preglednost varnostnih lastnosti in olajšala uporabo izdelkov z digitalnimi elementi. Potrošniki in državljani bi imeli tudi koristi zaradi boljše zaščite svojih temeljnih pravic, kot sta zasebnost in varstvo podatkov.

Hkrati bi predlog pomenil višje stroške zagotavljanja skladnosti in izvrševanja za podjetja, priglašene organe in javne organe, vključno z akreditacijskimi organi in organi za nadzor trga. Za razvijalce programske opreme in proizvajalce strojne opreme bo pomenil višje neposredne stroške zagotavljanja skladnosti zaradi novih varnostnih zahtev, ugotavljanja skladnosti, zagotavljanja dokumentacije in obveznosti poročanja, zaradi česar bodo skupni stroški zagotavljanja skladnosti dosegli približno 29 milijard EUR glede na ocenjeno tržno vrednost 1 485 milijard EUR prometa[39]. Za uporabnike, vključno s poslovnimi uporabniki, potrošniki in državljani, bo to morda pomenilo višje cene izdelkov z digitalnimi elementi. Vendar pa bi jih bilo treba presojati glede na pomembne koristi, opisane zgoraj.

1.4.3. Kazalniki smotrnosti

Navedite, s katerimi kazalniki se bodo spremljali napredek in dosežki.

Za preverjanje, ali proizvajalci izboljšujejo varnost svojih izdelkov z digitalnimi elementi od faze zasnove in razvoja naprej in v celotnem življenjskem ciklu navedenih izdelkov, bi bilo mogoče upoštevati več kazalnikov. Ti bi lahko bili število pomembnih incidentov v Uniji zaradi ranljivosti, delež izdelovalcev strojne in programske opreme, ki upoštevajo življenjski cikel sistematičnega varnega razvoja, kvalitativna analiza varnosti izdelkov z digitalnimi elementi, kvantitativna in kvalitativna ocena zbirk podatkov o ranljivosti, pogostost varnostnih popravkov, ki jih dajo na voljo proizvajalci, ali povprečno število dni, ki pretečejo od odkritja ranljivosti do zagotovitve varnostnih popravkov.

Kazalnik skladnega okvira kibernetske varnosti bi lahko bil neobstoj ciljne nacionalne zakonodaje na področju kibernetske varnosti za posamezne izdelke.

Kazalnik izboljšanja preglednosti glede varnostnih lastnosti izdelkov z digitalnimi elementi bi lahko bil delež izdelkov z digitalnimi elementi, ki se pošiljajo z informacijami o varnostnih lastnostih. Nadalje, delež izdelkov z digitalnimi elementi, ki se pošiljajo z navodili za uporabnika o varni uporabi, bi bilo mogoče uporabiti kot kazalnik, ali je organizacijam in potrošnikom omogočena varna uporaba izdelkov z digitalnimi elementi.

Za spremljanje učinka uredbe bi bilo mogoče predvideti nekatere kazalnike, ki bi jih ocenjevala Komisija, če je ustrezno ob podpori agencije ENISA. Glede na operativni cilj, ki ga je treba doseči, so v nadaljevanju navedeni nekateri kazalniki spremljanja, na podlagi katerih bi se lahko ocenila uspešnost horizontalnih zahtev glede kibernetske varnosti.

Za oceno ravni kibernetske varnosti izdelkov z digitalnimi elementi:

[38] Glej [Delovni dokument služb Komisije o poročilu o oceni učinka, priložen uredbi o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi].

[39] Glej [Delovni dokument služb Komisije o poročilu o oceni učinka, priložen uredbi o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi].

– statistični podatki in kvalitativne analize incidentov, ki prizadenejo izdelke z digitalnimi elementi, ter kako so bili ti obravnavani. Zbirala in ocenjevala bi jih lahko Komisija ob podpori agencije ENISA;

– evidence znanih ranljivosti in analize njihove obravnave. Take analize bi lahko izvajala agencija ENISA na podlagi evropske zbirke podatkov o ranljivosti, vzpostavljene na podlagi [Direktive XXX/XXXX (NIS2)];

– ankete med proizvajalci strojne in programske opreme z namenom spremljanja napredka.

Za oceno ravni informacij o varnostnih lastnostih, varnostni podpori, izrabljenosti in dolžnosti skrbnega ravnanja: rezultati anket med uporabniki in podjetji, ki jih izvede Komisija ob podpori agencije ENISA.

Za oceno izvajanja bi si lahko Komisija zadala cilj zagotoviti učinkovito izvajanje ugotavljanja skladnosti. V ta namen bo izdana zahteva za standardizacijo, nato pa se bo spremljalo njeno izvajanje. Komisija bo preverjala tudi zmogljivosti priglašenih organov in, če je ustrezno, certifikacijskih organov.

Glede uporabe bo Komisija na podlagi poročil držav članic preverila, ali se nacionalne pobude ne nanašajo na vidike, ki jih ureja uredba.

1.5. Utemeljitev predloga/pobude

1.5.1. Potrebe, ki jih je treba zadovoljiti kratkoročno ali dolgoročno, vključno s podrobno časovnico za uvajanje ustreznih ukrepov za izvajanje pobude

Uredba bi se morala začeti v celoti uporabljati 24 mesecev po začetku njene veljavnosti. Vendar bi morali biti elementi strukture upravljanja vzpostavljeni že pred tem. Zlasti velja, da države članice do takrat imenujejo obstoječe organe in/ali ustanovijo nove organe za opravljanje nalog iz zakonodaje.

1.5.2. Dodana vrednost ukrepanja Unije (ki je lahko posledica različnih dejavnikov, npr. boljšega usklajevanja, pravne varnosti, večje učinkovitosti ali dopolnjevanja). Za namene te točke je „dodana vrednost ukrepanja Unije“ vrednost, ki izhaja iz ukrepanja Unije in predstavlja dodatno vrednost poleg tiste, ki bi jo sicer ustvarile države članice same.

Očitno čezmejna narava kibernetske varnosti in vse večje število incidentov, katerih učinki segajo čez meje, v razne sektorje in izdelke, pomeni, da države članice ne morejo same učinkovito doseči navedenih ciljev. Glede na globalno naravo trga izdelkov z digitalnimi elementi se države članice na svojih ozemljih spoprijemajo z istimi tveganji glede istih izdelkov z digitalnimi elementi. Nastajajoči neenotni okvir potencialno različnih nacionalnih pravil lahko tudi ogrozi odprt in konkurenčen enotni trg izdelkov z digitalnimi elementi. Zato je potrebno skupno ukrepanje na ravni EU, da se povečata zaupanje med uporabniki in privlačnost izdelkov z digitalnimi elementi iz EU. To bi tudi koristilo notranjemu trgu, saj bi zagotavljalo pravno varnost in enake konkurenčne pogoje za prodajalce izdelkov z digitalnimi elementi.

1.5.3. Spoznanja iz podobnih izkušenj v preteklosti

Akt o kibernetski odpornosti je prvi tovrstni predpis, ki uvaja zahteve glede kibernetske varnosti za dajanje izdelkov z digitalnimi elementi na trg. Temelji na

vzpostavitvi novega zakonodajnega okvira in spoznanjih iz postopkov izvajanja obstoječe harmonizacijske zakonodaje Unije, ki se nanaša na številne različne izdelke, predvsem glede priprave za izvajanje, vključno z vidiki, kot je priprava harmoniziranih standardov.

1.5.4. Skladnost z večletnim finančnim okvirom in možne sinergije z drugimi ustreznimi instrumenti

Uredba o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi opredeljuje nove zahteve glede kibernetske varnosti za vse izdelke z digitalnimi elementi, ki se dajo na trg EU, ter presega zahteve iz obstoječe zakonodaje. Hkrati pa predlog temelji na obstoječi strukturi zakonodaje novega zakonodajnega okvira. Zato bi gradil na obstoječih strukturah in postopkih novega zakonodajnega okvira, kakor so sodelovanje priglašenih organov in organov za nadzor trga, moduli ugotavljanja skladnosti ter razvoj harmoniziranih standardov. Nov predlog bi se opiral tudi na nekatere strukture, razvite v skladu z drugo zakonodajo o kibernetski varnosti, kot sta Direktiva (EU) 2016/1148 (direktiva o varnosti omrežij in informacijskih sistemov) oziroma [Direktiva XXX/XXXX (NIS2)] ali Uredba (EU) 2019/881 (Akt o kibernetski varnosti).

1.5.5. Ocena različnih razpoložljivih možnosti financiranja, vključno z možnostmi za prerazporeditev

Upravljanje področij ukrepanja, dodeljenih agenciji ENISA, ustreza njenim sedanjim pristojnostim in splošnim nalogam. Ta področja ukrepanja lahko zahtevajo posebne profile ali nove naloge, vendar ne v pomembnejšem obsegu, saj jih je mogoče izvesti tudi z obstoječimi viri agencije ENISA ter s premestitvami ali povezovanjem različnih nalog. Eno od glavnih področij ukrepanja, dodeljenih agenciji ENISA, se na primer nanaša na zbiranje in obdelavo uradnih obvestil izdelovalcev glede izrabljenih ranljivosti izdelkov. Z [Direktivo XXX/XXXX (NIS2)] je agenciji ENISA že dodeljena naloga vzpostavitve evropske zbirke podatkov o ranljivosti, v kateri je mogoče prostovoljno razkriti in evidentirati javno znane ranljivosti, da se uporabnikom omogoči, da lahko sprejmejo ustrezne blažilne ukrepe. Viri, namenjeni temu, bi se lahko uporabili tudi za nove zgoraj navedene naloge, ki se nanašajo na obveščanje o ranljivosti izdelkov. To bi lahko zagotovilo učinkovito uporabo obstoječih virov, hkrati pa bi ustvarilo potrebne sinergije med nalogami, ki lahko bolje prispevajo k analizam tveganj in groženj za kibernetsko varnost, ki jih izvaja agencija ENISA.

1.6. Trajanje predloga/pobude in finančnih posledic

☐ **Časovno omejeno**

– ☐ od [D. MMMM] LLLL do [D. MMMM] LLLL,

– ☐ finančne posledice med letoma LLLL in LLLL za odobritve za prevzem obveznosti ter med letoma LLLL in LLLL za odobritve plačil.

× **Časovno neomejeno**

– Izvajanje z obdobjem uvajanja od leta 2025.

– ki mu sledi izvajanje v celoti.

1.7. Načrtovani načini upravljanja[40]

☐ **Neposredno upravljanje** – Komisija:

– × z lastnimi službami, vključno s svojim osebjem v delegacijah Unije,

– ☐ prek izvajalskih agencij.

☐ **Deljeno upravljanje** z državami članicami.

☐ **Posredno upravljanje**, tako da se naloge izvrševanja proračuna poverijo:

– ☐ tretjim državam ali organom, ki jih te imenujejo,

– ☐ mednarodnim organizacijam in njihovim agencijam (navedite),

– ☐ EIB in Evropskemu investicijskemu skladu,

– ☐ organom iz členov 70 in 71 finančne uredbe,

– ☐ subjektom javnega prava,

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

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

– ☐ osebam, pooblaščenim za izvajanje določenih ukrepov SZVP na podlagi naslova V PEU in opredeljenim v zadevnem temeljnem aktu.

– *Pri navedbi več kot enega načina upravljanja je treba to natančneje obrazložiti v oddelku „opombe“.*

Opombe

S to uredbo je izvajanje nekaterih ukrepov dodeljeno agenciji ENISA v skladu z njenimi obstoječimi pristojnostmi ter zlasti s členom 3(2) Uredbe (EU) 2019/881, ki določa, da agencija ENISA izvaja naloge, ki so ji dodeljene s pravnimi akti Unije, ki določajo ukrepe za približevanje zakonov in drugih predpisov držav članic, ki se nanašajo na kibernetsko varnost. Agenciji ENISA je zlasti dodeljena naloga prejemanja uradnih obvestil izdelovalcev o aktivno izrabljenih ranljivostih v izdelkih z digitalnimi elementi in incidentih, ki vplivajo na varnost navedenih izdelkov. Agencija ENISA bi morala taka uradna obvestila tudi posredovati zadevnim skupinam CSIRT oziroma zadevnim enotnim kontaktnim točkam držav članic, imenovanim v skladu s členom [člen X] Direktive [Direktiva XXX/XXXX (NIS2)], ter o njih obvestiti organe za nadzor trga. Agencija ENISA bi morala na podlagi informacij, ki jih zbere,

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

pripraviti dvoletno tehnično poročilo o novih trendih glede tveganj za kibernetsko varnost pri izdelkih z digitalnimi elementi ter ga predložiti skupini za sodelovanje na področju varnosti omrežij in informacijskih sistemov. Nadalje, agencija ENISA lahko glede na svoje strokovno znanje izkušnje, zbrane informacije in analize groženj podpre postopek izvajanja te uredbe tako, da predlaga skupne dejavnosti nacionalnih organov za nadzor trga na podlagi znakov ali informacij o morebitni neskladnosti izdelkov z digitalnimi elementi s to uredbo v več državah članicah ali opredeli kategorije izdelkov, za katere je mogoče organizirati sočasne usklajene kontrolne ukrepe. Komisija lahko v izjemnih okoliščinah od agencije ENISA zahteva izvedbo ocen posameznih izdelkov, in sicer v zvezi z izdelki z digitalnimi elementi, ki pomenijo povečano tveganje za kibernetsko varnost, če je potrebno takojšnje ukrepanje, da se ohrani dobro delovanje notranjega trga.

Ocenjuje se, da bodo vse te naloge zahtevale približno 4,5 ekvivalenta polnega delovnega časa iz obstoječih virov agencije ENISA, pri čemer se bodo lahko uporabili strokovno znanje in izkušnje agencije ENISA ter pripravljalno delo, ki ga agencija ENISA že opravlja, med drugim v podporo prihodnjemu izvajanju [Direktive XXX/XXXX (NIS2)], za namene katerega so bili viri agencije ENISA dopolnjeni.

2. UKREPI UPRAVLJANJA

2.1. Pravila o spremljanju in poročanju

Navedite pogostost in pogoje.

Komisija bo v 36 mesecih po datumu začetka uporabe te uredbe ter nato vsaka štiri leta Evropskemu parlamentu in Svetu predložila poročilo o oceni in pregledu te uredbe. Poročila se objavijo.

2.2. Upravljavski in kontrolni sistemi

2.2.1. Utemeljitev načinov upravljanja, mehanizmov financiranja, načinov plačevanja in predlagane strategije kontrol

S to uredbo se vzpostavlja nova politika v zvezi s harmoniziranimi zahtevami glede kibernetske varnosti izdelkov z digitalnimi elementi, ki se dajo na notranji trg, v njihovem celotnem življenjskem ciklu. Po sprejetju pravnega akta bo Komisija pri evropskih organih za standardizacijo vložila zahteve za razvoj standardov.

Za izpolnjevanje teh novih nalog je treba službam Komisije zagotoviti ustrezna sredstva. Predvideva se, da bo za izvrševanje nove uredbe potrebnih sedem ekvivalentov polnega delovnega časa (od tega en napoteni nacionalni strokovnjak) za izvajanje naslednjih nalog:

- priprava zahtev za standardizacijo in/ali skupnih specifikacij z izvedbenimi akti, če postopek standardizacije ne bo uspešen;
- priprava delegiranega akta [v 12 mesecih od začetka veljavnosti Uredbe] z opredelitvami kritičnih izdelkov z digitalnimi elementi;
- morebitna priprava delegiranih aktov za posodobitev seznama kritičnih izdelkov razredov I in II; določitev, ali je za izdelke z digitalnimi elementi, zajete z drugimi pravili Unije, ki določajo zahteve, s katerimi se doseže enaka raven varstva kot s to uredbo, potrebna omejitev ali izključitev; določitev obveznosti certificiranja nekaterih zelo kritičnih izdelkov z digitalnimi elementi na podlagi meril iz te uredbe; določitev minimalne vsebine izjave EU o skladnosti in dopolnitev elementov, ki jih je treba vključiti v tehnično dokumentacijo;
- morebitna priprava izvedbenih aktov, ki se nanašajo na obliko ali elemente obveznosti poročanja, kosovnico za programsko opremo, skupne specifikacije ali namestitev oznake CE;
- morebitna priprava takojšnjega ukrepanja za naložitev popravnih ali omejevalnih ukrepov v izjemnih okoliščinah, da se ohrani dobro delovanje notranjega trga, vključno s pripravo izvedbenega akta;
- organizacija in usklajevanje priglasitev držav članic v zvezi s priglašenimi organi ter usklajevanje priglašenih organov;
- podpora usklajevanju organov držav članic za nadzor trga.

2.2.2. Podatki o ugotovljenih tveganjih in vzpostavljenih sistemih notranjih kontrol za njihovo zmanjševanje

Komisija je pristojna za usklajevanje priglašenih organov in organov za nadzor trga, da se zagotovi izmenjava informacij med njimi in njihovo dobro sodelovanje. Za

tehnično strokovno znanje in strokovno znanje o trgu bo ustanovljena strokovna skupina.

2.2.3. Ocena in utemeljitev stroškovne učinkovitosti kontrol (razmerje „stroški kontrol ÷ vrednost z njimi povezanih upravljanih sredstev“) ter ocena pričakovane stopnje tveganja napake (ob plačilu in ob zaključku)

2.3. Pri odhodkih za sestanke se glede na nizko vrednost posameznih transakcij (npr. povračilo potnih stroškov za delegata na sestanku) zdijo standardni kontrolni postopki zadostni. Ukrepi za preprečevanje goljufij in nepravilnosti

Navedite obstoječe ali načrtovane preprečevalne in zaščitne ukrepe, npr. iz strategije za boj proti goljufijam.

Obstoječi ukrepi za preprečevanje goljufij, ki se uporabljajo za Komisijo, bodo vključevali dodatne odobritve, potrebne za to uredbo.

3. OCENA FINANČNIH POSLEDIC PREDLOGA/POBUDE

3.1. Zadevni razdelki večletnega finančnega okvira in odhodkovne proračunske vrstice

- Obstoječe proračunske vrstice

Shema

- Zahtevane nove proračunske vrstice

n. r.

3.2. Ocenjene finančne posledice predloga za odobritve

3.2.1. Povzetek ocenjenih posledic za odobritve za poslovanje

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

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

v mio. EUR (na tri decimalna mesta natančno)

Razdelek večletnega finančnega okvira	Številka	

GD <…….>			Leto **N**[41]	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)			**SKUPAJ**
• Odobritve za poslovanje										
Proračunska vrstica[42]	obveznosti	(1a)								
	plačila	(2a)								
Proračunska vrstica	obveznosti	(1b)								
	plačila	(2b)								
Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov[43]										
Proračunska vrstica		(3)								
Odobritve za GD <…….> SKUPAJ	obveznosti	= 1a + 1b + 3								
	plačila	= 2a								

41 Leto N je leto začetka izvajanja predloga/pobude. Nadomestite „N“ s pričakovanim prvim letom izvajanja (na primer: 2021). Naredite isto za naslednja leta.

42 Po uradni proračunski nomenklaturi.

43 Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanja programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

		+ 2b + 3								

• Odobritve za poslovanje SKUPAJ	obveznosti	(4)								
	plačila	(5)								
• Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov, SKUPAJ		(6)								
Odobritve iz RAZDELKA <….> večletnega finančnega okvira **SKUPAJ**	obveznosti	= 4 + 6								
	plačila	= 5 + 6								

<u>Če ima predlog/pobuda posledice za več razdelkov za poslovanje, ponovite zgornji odsek:</u>

• Odobritve za poslovanje SKUPAJ (vsi razdelki za poslovanje)	obveznosti	(4)								
	plačila	(5)								
Odobritve za upravne zadeve, ki se financirajo iz sredstev določenih programov, SKUPAJ (vsi razdelki za poslovanje)		(6)								
Odobritve iz RAZDELKOV od 1 do 6 večletnega finančnega okvira **SKUPAJ** (referenčni znesek)	obveznosti	= 4 + 6								
	plačila	= 5 + 6								

Razdelek večletnega finančnega okvira	**7**	„Upravni odhodki“

Ta oddelek se izpolni s „proračunskimi podatki upravne narave“, ki jih je treba najprej vnesti v Prilogo k oceni finančnih posledic zakonodajnega predloga (Priloga V k notranjim pravilom), ki se prenese v sistem DECIDE za namene posvetovanj med službami.

v mio. EUR (na tri decimalna mesta natančno)

		Leto **2024**	Leto **2025**	Leto **2026**	Leto **2027**	**SKUPAJ**
GD CNECT						
• Človeški viri		1,030	1,030	1,030	1,030	**4,120**
• Drugi upravni odhodki		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
GD CNECT, **SKUPAJ**	odobritve	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

Odobritve iz RAZDELKA 7 večletnega finančnega okvira **SKUPAJ**	(obveznosti skupaj = plačila skupaj)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

v mio. EUR (na tri decimalna mesta natančno)

		Leto **2024**	Leto **2025**	Leto **2026**	Leto **2027**	**SKUPAJ**
Odobritve iz RAZDELKOV od 1 do 7 večletnega finančnega okvira **SKUPAJ**	obveznosti	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	plačila	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Ocenjene realizacije, financirane z odobritvami za poslovanje

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

Cilji in realizacije ⇩			Leto **N**		Leto **N+1**		Leto **N+2**		Leto **N+3**		Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)						**SKUPAJ**	
	REALIZACIJE																	
	vrsta 44	povprečni stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število	stroški	število realizacij skupaj	stroški realizacij skupaj
SPECIFIČNI CILJ št. 1[45] …																		
– realizacija																		
– realizacija																		
– realizacija																		
Seštevek za specifični cilj št. 1																		
SPECIFIČNI CILJ št. 2 …																		
– realizacija																		
Seštevek za specifični cilj št. 2																		
SKUPAJ																		

[44] Realizacije so dobavljeni proizvodi in opravljene storitve (npr. število financiranih izmenjav študentov, število kilometrov novozgrajenih cest …).

[45] Kakor je opisan v točki 1.4.2 „Specifični cilji …“.

3.2.3. Povzetek ocenjenih posledic za upravne odobritve

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

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

v mio. EUR (na tri decimalna mesta natančno)

	Leto **2024**	Leto **2025**	Leto **2026**	Leto **2027**	
RAZDELEK 7 večletnega finančnega okvira					
Človeški viri	1,030	1,030	1,030	1,030	**4,120**
Drugi upravni odhodki	0,222	0,222	0,222	0,222	**0,888**
Seštevek za RAZDELEK 7 večletnega finančnega okvira	1,252	1,252	1,252	1,252	**5,008**

Odobritve zunaj RAZDELKA 7[46] večletnega finančnega okvira					
Človeški viri					
Drugi upravni odhodki					
Seštevek za odobritve zunaj RAZDELKA 7 večletnega finančnega okvira					

SKUPAJ	1,252	1,252	1,252	1,252	**5,008**

Potrebe po odobritvah za človeške vire in druge upravne odhodke se krijejo z odobritvami GD, ki so že dodeljene za upravljanje ukrepa in/ali so bile prerazporejene znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na proračunske omejitve.

[46] Tehnična in/ali upravna pomoč ter odhodki za podporo izvajanja programov in/ali ukrepov EU (prej vrstice BA), posredne raziskave, neposredne raziskave.

3.2.3.1. Ocenjene potrebe po človeških virih

– ☐ Za predlog/pobudo niso potrebni človeški viri.

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

ocena, izražena v ekvivalentu polnega delovnega časa

		Leto **2024**	Leto **2025**	Leto **2026**	Leto **2027**
20 01 02 01 (sedež in predstavništva Komisije)		6	6	6	6
20 01 02 03 (delegacije)					
01 01 01 01 (posredne raziskave)					
01 01 01 11 (neposredne raziskave)					
Druge proračunske vrstice (navedite)					
• Zunanji sodelavci (v ekvivalentu polnega delovnega časa: EPDČ)[47]					
20 02 01 (PU, NNS, ZU iz splošnih sredstev)		1	1	1	1
20 02 03 (PU, LU, NNS, ZU in MSD na delegacijah)					
XX 01 xx **yy zz** [48]	– na sedežu				
	– na delegacijah				
01 01 01 02 (PU, NNS, ZU za posredne raziskave)					
01 01 01 12 (PU, NNS, ZU za neposredne raziskave)					
Druge proračunske vrstice (navedite)					
SKUPAJ		**7**	**7**	**7**	**7**

XX je zadevno področje ali naslov v proračunu.

Potrebe po človeških virih se krijejo z osebjem GD, ki je že dodeljeno za upravljanje ukrepa in/ali je bilo prerazporejeno znotraj GD, po potrebi skupaj z dodatnimi viri, ki se lahko pristojnemu GD dodelijo v postopku letne dodelitve virov glede na proračunske omejitve.

Opis nalog:

Uradniki in začasni uslužbenci 6 EPDČ x 157 000 EUR/leto = 942 000 EUR	Kot je opisano v točki 2.2.1.: – priprava zahtev za standardizacijo in/ali skupnih specifikacij z izvedbenimi akti, če postopek standardizacije ne bo uspešen; – priprava delegiranega akta [v 12 mesecih od začetka veljavnosti Uredbe] z opredelitvami kritičnih izdelkov z digitalnimi elementi; – morebitna priprava delegiranih aktov za posodobitev seznama kritičnih izdelkov razredov I in II; določitev, ali je za izdelke z digitalnimi elementi, zajete z drugimi pravili Unije, ki določajo zahteve, s katerimi se doseže enaka raven varstva kot s to uredbo, potrebna omejitev ali izključitev; določitev obveznosti certificiranja nekaterih zelo kritičnih izdelkov z digitalnimi elementi na podlagi meril iz te uredbe; določitev minimalne vsebine izjave EU o skladnosti in dopolnitev elementov, ki jih je treba vključiti v tehnično dokumentacijo; – morebitna priprava izvedbenih aktov, ki se nanašajo na obliko ali elemente obveznosti poročanja, kosovnico za programsko opremo, skupne specifikacije ali namestitev oznake CE;

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

[48] Dodatna zgornja meja za zunanje sodelavce v okviru odobritev za poslovanje (prej vrstice BA).

	– morebitna priprava takojšnjega ukrepanja za naložitev popravnih ali omejevalnih ukrepov v izjemnih okoliščinah, da se ohrani dobro delovanje notranjega trga, vključno s pripravo izvedbenega akta; – organizacija in usklajevanje priglasitev držav članic v zvezi s priglašenimi organi ter usklajevanje priglašenih organov; – podpora usklajevanju organov držav članic za nadzor trga.
Zunanji sodelavci 1 NNS x 88 000 EUR/leto	Kot je opisano v točki 2.2.1.: – priprava zahtev za standardizacijo in/ali skupnih specifikacij z izvedbenimi akti, če postopek standardizacije ne bo uspešen; – priprava delegiranega akta [v 12 mesecih od začetka veljavnosti Uredbe] z opredelitvami kritičnih izdelkov z digitalnimi elementi; – morebitna priprava delegiranih aktov za posodobitev seznama kritičnih izdelkov razredov I in II; določitev, ali je za izdelke z digitalnimi elementi, zajete z drugimi pravili Unije, ki določajo zahteve, s katerimi se doseže enaka raven varstva kot s to uredbo, potrebna omejitev ali izključitev; določitev obveznosti certificiranja nekaterih zelo kritičnih izdelkov z digitalnimi elementi na podlagi meril iz te uredbe; določitev minimalne vsebine izjave EU o skladnosti in dopolnitev elementov, ki jih je treba vključiti v tehnično dokumentacijo; – morebitna priprava izvedbenih aktov, ki se nanašajo na obliko ali elemente obveznosti poročanja, kosovnico za programsko opremo, skupne specifikacije ali namestitev oznake CE; – morebitna priprava takojšnjega ukrepanja za naložitev popravnih ali omejevalnih ukrepov v izjemnih okoliščinah, da se ohrani dobro delovanje notranjega trga, vključno s pripravo izvedbenega akta; – organizacija in usklajevanje priglasitev držav članic v zvezi s priglašenimi organi ter usklajevanje priglašenih organov; – podpora usklajevanju organov držav članic za nadzor trga.

3.2.4. Skladnost z veljavnim večletnim finančnim okvirom

Predlog/pobuda:

– x se lahko v celoti financira s prerazporeditvijo znotraj zadevnega razdelka večletnega finančnega okvira.

Spremembe niso potrebne.

– ☐ zahteva uporabo nedodeljene razlike do zgornje meje v zadevnem razdelku večletnega finančnega okvira in/ali uporabo posebnih instrumentov, kot so opredeljeni v uredbi o večletnem finančnem okviru;

-

– ☐ zahteva spremembo večletnega finančnega okvira.

-

3.2.5. Udeležba tretjih oseb pri financiranju

V predlogu/pobudi:

– x ni načrtovano sofinanciranje tretjih oseb

– ☐ je načrtovano sofinanciranje, kot je ocenjeno v nadaljevanju:

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

	Leto **N**[49]	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)			Skupaj
Navedite organ, ki bo sofinanciral predlog/pobudo								
Sofinancirane odobritve SKUPAJ								

[49] Leto N je leto začetka izvajanja predloga/pobude. Nadomestite „N“ s pričakovanim prvim letom izvajanja (na primer: 2021). Naredite isto za naslednja leta.

3.3. Ocenjene posledice za prihodke

– ☐ Predlog/pobuda nima finančnih posledic za prihodke.

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

  – ☐ za lastna sredstva,

  – ☐ za druge prihodke.

  – navedite, ali so prihodki dodeljeni za odhodkovne vrstice ☐

v mio. EUR (na tri decimalna mesta natančno)

Prihodkovna proračunska vrstica	Odobritve na voljo za tekoče proračunsko leto	Posledice predloga/pobude[50]						
		Leto **N**	Leto **N+1**	Leto **N+2**	Leto **N+3**	Vstavite ustrezno število let glede na trajanje posledic (gl. točko 1.6)		
Člen …….								

Za namenske prejemke navedite zadevne odhodkovne proračunske vrstice.

Druge opombe (npr. metoda/formula za izračun posledic za prihodke ali druge informacije).

[50] Pri tradicionalnih lastnih sredstvih (carine, prelevmani na sladkor) se navedejo neto zneski, tj. bruto zneski po odbitku 20 % stroškov pobiranja.