Vijeće
Europske unije

Bruxelles, 16. rujna 2022.
(OR. en)

12429/22

Međuinstitucijski predmet:
2022/0272(COD)

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

PRIJEDLOG

Od:	Glavna tajnica Europske komisije, potpisala direktorica Martine DEPREZ
Datum primitka:	15. rujna 2022.
Za:	Glavno tajništvo Vijeća
Br. dok. Kom.:	COM(2022) 454 final
Predmet:	Prijedlog UREDBE EUROPSKOG PARLAMENTA I VIJEĆA o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020

Za delegacije se u prilogu nalazi dokument COM(2022) 454 final.

Priloženo: COM(2022) 454 final

EUROPSKA
KOMISIJA

Bruxelles, 15.9.2022.
COM(2022) 454 final

2022/0272 (COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020

(Tekst značajan za EGP)

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

OBRAZLOŽENJE

1. KONTEKST PRIJEDLOGA

• Razlozi i ciljevi prijedloga

Hardverski i softverski proizvodi sve su izloženiji uspješnim kibernapadima te se procjenjuje da je do 2021. godišnja šteta od kiberkriminaliteta bila 5,5 bilijuna EUR. Dva su glavna problema zbog kojih ti proizvodi stvaraju troškove korisnicima i društvu: 1. imaju nisku razinu kibersigurnosti, čemu su dokaz raširene ranjivosti te nedovoljna i neredovita sigurnosna ažuriranja za njihovo otklanjanje, i 2. korisnici nemaju dovoljno znanja ni informacija, pa ne mogu odabrati proizvode s odgovarajućim kibersigurnosnim svojstvima ili ih rabiti na siguran način. U povezanom okruženju kiberincident u jednom proizvodu može utjecati na cijelu organizaciju ili cjelokupni lanac opskrbe jer se često vrlo brzo proširi preko granica unutarnjeg tržišta. To može uzrokovati ozbiljan poremećaj gospodarskih i društvenih aktivnosti ili čak ugroziti ljudske živote.

Kibersigurnost proizvoda s digitalnim elementima ima izrazitu prekograničnu dimenziju jer se proizvodi proizvedeni u jednoj zemlji često rabe na cijelom unutarnjem tržištu. Usto, incidenti isprva zahvate jedan subjekt ili jednu državu članicu često se veoma brzo prošire na cijelo unutarnje tržište.

Premda se postojeće zakonodavstvo o unutarnjem tržištu primjenjuje na određene proizvode s digitalnim elementima, većina hardverskih i softverskih proizvoda trenutačno nije obuhvaćena nijednim propisom EU-a koji se odnosi na njihovu kibersigurnost. Točnije, postojećim se pravnim okvirom EU-a ne uređuje pitanje kibersigurnosti neugrađenog softvera iako su kibernapadi sve češće usmjereni na ranjivosti tih proizvoda, što uzrokuje znatne društvene i gospodarske troškove. Mnogobrojni su primjeri važnih kibernapada koji su posljedica neoptimalne sigurnosti proizvoda: primjerice napad ucjenjivačkog crva WannaCry, koji je 2017. iskoristio ranjivost Windowsa i zahvatio 200 000 računala u 150 zemalja te prouzročio štetu koja se mjeri u milijardama dolara, zatim napad putem Kaseyinog softvera za mrežnu administraciju VSA na više od 1 000 poduzeća u lancu opskrbe zbog kojeg je jedan lanac supermarketa morao zatvoriti svih 500 trgovina u Švedskoj ili mnogi incidenti u kojima se bankovne aplikacije hakiraju kako bi se ukrao novac od lakovjernih potrošača.

Utvrđena su dva glavna cilja kako bi se osiguralo pravilno funkcioniranje unutarnjeg tržišta: 1. stvoriti uvjete za razvoj sigurnih proizvoda s digitalnim elementima tako što će se urediti da se hardverski i softverski proizvodi stavljaju na tržište s manje ranjivosti i da proizvođači ozbiljno shvaćaju sigurnost tijekom cijelog životnog ciklusa proizvoda; i 2. stvoriti uvjete koji korisnicima omogućuju da proizvode s digitalnim elementima odabiru i rabe vodeći računa o kibersigurnosti. Utvrđena su četiri posebna cilja: i. osigurati da proizvođači povećavaju sigurnost proizvoda s digitalnim elementima od faze projektiranja i razvoja te tijekom cijelog životnog ciklusa; ii. stvoriti usklađen okvir za kibersigurnost kako bi ga se proizvođači hardvera i softvera lakše pridržavali; iii. povećati transparentnost sigurnosnih svojstava proizvoda s digitalnim elementima i iv. poduzećima i potrošačima omogućiti sigurnu upotrebu proizvoda s digitalnim elementima.

Zbog izrazite prekogranične prirode kibersigurnosti i sve češćih incidenata čiji se učinci prelijevaju preko granica te na druge sektore i proizvode države članice ne mogu same učinkovito postići te ciljeve. Zbog globalne prirode tržišta proizvoda s digitalnim elementima isti proizvod s digitalnim elementima ima iste sigurnosne rizike na državnim područjima različitih država članica. Rascjepkan okvir od potencijalno različitih nacionalnih pravila

kakav se počeo pojavljivati mogao bi ugroziti otvoreno i konkurentno jedinstveno tržište proizvoda s digitalnim elementima. Dakle, zajedničko djelovanje na razini EU-a potrebno je radi povećanja povjerenja korisnika i privlačnosti proizvoda s digitalnim elementima iz EU-a. To bi pogodovalo i unutarnjem tržištu zbog stvaranja pravne sigurnosti i jednakih uvjeta za dobavljače proizvoda s digitalnim elementima, kako je istaknuto i u završnom izvješću Konferencije o budućnosti Europe, u kojem građani pozivaju na veću ulogu EU-a u borbi protiv prijetnji kibersigurnosti.

- **Međudjelovanje s postojećim odredbama politike u tom području**

Okvir EU-a sastoji se od nekoliko horizontalnih akata kojima su obuhvaćeni određeni aspekti povezani s kibersigurnošću iz različitih kutova (proizvodi, usluge, upravljanje krizama i kaznena djela). U 2013. na snagu je stupila Direktiva o napadima na informacijske sustave[1], kojom su usklađeni kriminalizacija i sankcije za niz kaznenih djela protiv informacijskih sustava. U kolovozu 2016. na snagu je stupila Direktiva (EU) 2016/1148 o sigurnosti mrežnih i informacijskih sustava (Direktiva NIS)[2] kao prvi zakonodavni akt o kibersigurnosti na razini EU-a. Njezinom revizijom, iz koje je proizišla Direktiva [Direktiva XXX/XXXX (NIS2)], povećane su zajedničke ambicije na razini EU-a. U 2019. na snagu je stupio Akt EU-a o kibersigurnosti[3], kojem je cilj povećati sigurnost IKT proizvoda, usluga i postupaka uvođenjem dobrovoljnog europskog okvira za kibersigurnosnu certifikaciju[4].

Lanac opskrbe je kibersiguran samo ako su kibersigurni svi njegovi dijelovi. Međutim, spomenuto zakonodavstvo EU-a ima znatnih nedostataka u tom pogledu jer ne obuhvaća obvezne zahtjeve u pogledu sigurnosti proizvoda s digitalnim elementima.

Iako predloženi Akt o kiberotpornosti obuhvaća proizvode s digitalnim elementima koji se stavljaju na tržište, Direktivom [Direktiva XXX/XXX (NIS2)] nastoji se postići visoka razina kibersigurnosti usluga koje pružaju ključni i važni subjekti. Direktivom [Direktiva XXX/XXXX (NIS2)] od država članica zahtijeva se da osiguraju da ključni i važni subjekti obuhvaćeni područjem primjene, kao što su pružatelji zdravstvene zaštite ili usluga u oblaku i tijela javne uprave, poduzmu odgovarajuće i proporcionalne tehničke, operativne i organizacijske kibersigurnosne mjere. To uključuje, među ostalim, zahtjev u pogledu sigurnosti u nabavi, razvoju i održavanju mrežnih i informacijskih sustava, uključujući upravljanje ranjivostima i njihovo otkrivanje. Prema Direktivi [Direktiva XXX/XXXX (NIS2)] Komisija je dužna, u roku od 21 mjeseca nakon datuma stupanja te direktive na snagu, donijeti provedbene akte kojima se utvrđuju tehnički i metodološki zahtjevi u pogledu tih mjera za određene vrste subjekata, kao što su pružatelji usluga računalstva u oblaku. Za sve ostale subjekte Komisija može donijeti provedbeni akt kojim se utvrđuju tehnički i metodološki zahtjevi te sektorski zahtjevi. Tim će se okvirom postići da se tehničke specifikacije i mjere slične bitnim kibersigurnosnim zahtjevima iz Akta o kiberotpornosti

---

1 Direktiva 2013/40/EU Europskog parlamenta i Vijeća od 12. kolovoza 2013. o napadima na informacijske sustave i o zamjeni Okvirne odluke Vijeća 2005/222/PUP, SL L 218, 14.8.2013., str. 8.–14.

2 Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije (SL L 194/1, 19.7.2016., str. 1.).

3 Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

4 Akt o kibersigurnosti omogućuje razvoj posebnih programa certifikacije. Svaki program uključuje upućivanja na relevantne norme, tehničke specifikacije ili druge kibersigurnosne zahtjeve definirane u programu. Odluka o razvoju kibersigurnosne certifikacije temelji se na riziku.

provode i za projektiranje, razvoj i upravljanje ranjivostima softvera koji se pruža kao usluga (softver kao usluga). Na primjer, to bi moglo biti sredstvo za postizanje visoke razine kibersigurnosti u sustavima elektroničkih zdravstvenih zapisa, uključujući slučajeve kad se isporučuju u obliku softvera kao usluge (SaaS) i kad se razvijaju unutar zdravstvenih ustanova (interno), u skladu s predloženom [Uredbom o europskom prostoru za zdravstvene podatke].

- **Međudjelovanje s drugim politikama Unije**

Kako je navedeno u Komunikaciji „Izgradnja digitalne budućnosti Europe”[5], od ključne je važnosti da EU iskoristi sve prednosti digitalnog doba te poveća industrijske i inovacijske kapacitete unutar sigurnog i etičkog okvira. U europskoj strategiji za podatke utvrđeno je da su četiri stupa – zaštita podataka, temeljna prava, sigurnost i kibersigurnost – ključni preduvjeti za društvo koje koristi moć podataka.

Trenutačni okvir EU-a[6] primjenjiv na proizvode koji mogu sadržavati digitalne elemente sastoji se od nekoliko zakonodavnih akata, uključujući akte EU-a o određenim proizvodima koje se odnosi na sigurnosne aspekte i opće zakonodavstvo o odgovornosti za proizvode. Prijedlog je usklađen s trenutačnim regulatornim okvirom EU-a za proizvode te s najnovijim zakonodavnim prijedlozima kao što je Komisijin Prijedlog uredbe [Uredba o umjetnoj inteligenciji (UI)][7].

Predložena uredba primjenjivala bi se na svu radijsku opremu obuhvaćenu područjem primjene Delegirane uredbe Komisije (EU) 2022/30. Nadalje, zahtjevi utvrđeni ovom Uredbom uključuju sve elemente bitnih zahtjeva iz članka 3. stavka 3. točaka (d), (e) i (f) Direktive 2014/53/EU, uključujući glavne elemente utvrđene u [Provedbena odluka Komisije XXX/2022 o zahtjevu za normizaciju upućenom europskim organizacijama za normizaciju] izdanoj na temelju te delegirane uredbe. Kako bi se izbjeglo regulatorno preklapanje, predviđeno je da Komisija ukine ili izmijeni delegiranu uredbu u pogledu radijske opreme obuhvaćene predloženom uredbom tako da se predložena uredba, nakon što se počne primjenjivati, primjenjuje na tu opremu.

Nadalje, kako bi se izbjeglo udvostručavanje rada, predviđeno je da Komisija i europske organizacije za normizaciju u okviru pripreme i izrade usklađenih normi radi lakše provedbe Uredbe uzmu u obzir rad na normizaciji u kontekstu Provedbene odluke Komisije C(2022)5637 o zahtjevu za normizaciju za potrebe Direktive o radijskoj opremi i Delegirane uredbe (EU) 2022/30.

2. PRAVNA OSNOVA, SUPSIDIJARNOST I PROPORCIONALNOST

- **Pravna osnova**

Pravna je osnova ovog Prijedloga članak 114. Ugovora o funkcioniranju Europske unije (UFEU), kojim se predviđa donošenje mjera za osiguravanje uspostave i funkcioniranja unutarnjeg tržišta. Svrha je Prijedloga uskladiti kibersigurnosne zahtjeve za proizvode s

[5] Komunikacija Komisije Europskom parlamentu, Vijeću, Europskom gospodarskom i socijalnom odboru i Odboru regija „Izgradnja digitalne budućnosti Europe” od 19. veljače 2020., COM(2020) 67 final.

[6] Uglavnom propisi novog zakonodavnog okvira.

[7] Prijedlog uredbe Europskog parlamenta i Vijeća o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (Akt o umjetnoj inteligenciji) i izmjeni određenih zakonodavnih akata Unije od 21. travnja 2021., COM(2021) 206 final.

digitalnim elementima u svim državama članicama i ukloniti prepreke slobodnom kretanju robe.

Članak 114. UFEU-a može se primijeniti kao pravna osnova za sprečavanje tih prepreka koje proizlaze iz različitih nacionalnih zakona i pristupa otklanjanju pravnih nesigurnosti i nedostataka u postojećim pravnim okvirima[8]. Nadalje, Sud je priznao da bi primjena heterogenih tehničkih zahtjeva mogla biti valjana osnova za primjenu članka 114. UFEU-a[9].

Trenutačni okvir EU-a primjenjiv na proizvode s digitalnim elementima temelji se na članku 114. UFEU-a i sastoji se od nekoliko zakonodavnih akata, uključujući akte o određenim proizvodima i sigurnosnim aspektima te opće zakonodavstvo o odgovornosti za proizvode. Međutim, njime su obuhvaćeni samo određeni aspekti povezani s kibersigurnošću materijalnih digitalnih proizvoda i, ako je primjenjivo, softvera ugrađenog u te proizvode. Na nacionalnoj razini države članice počinju poduzimati nacionalne mjere kojima se od dobavljača digitalnih proizvoda zahtijeva da povećaju svoju kibersigurnost[10]. S druge strane, kibersigurnost digitalnih proizvoda ima izrazitu prekograničnu dimenziju jer proizvode proizvedene u jednoj zemlji često rabe organizacije i potrošači na cjelokupnom unutarnjem tržištu. Incidenti koji isprva pogode jedan subjekt ili jednu državu članicu često se vrlo brzo prošire na druge organizacije, sektore i nekoliko država članica.

Raznim dosad donesenim aktima i inicijativama na razini EU-a i na nacionalnoj razini samo se djelomično rješavaju utvrđeni problemi i rizici, pa na unutarnjem tržištu nastaje pravna neujednačenost, dobavljačima i korisnicima tih proizvoda povećava se pravna nesigurnost a poduzećima se nameće nepotrebno opterećenje jer moraju ispunjavati niz zahtjeva za slične vrste proizvoda.

Predloženom uredbom uskladio bi se i pojednostavnio regulatorni okvir EU-a uvođenjem kibersigurnosnih zahtjeva za proizvode s digitalnim elementima te bi se izbjeglo preklapanje zahtjeva koji proizlaze iz različitih zakonodavnih akata. Time bi se stvorila veća pravna sigurnost za gospodarske subjekte i korisnike u Uniji te bi se bolje uskladilo jedinstveno europsko tržište, čime bi se stvorili održiviji uvjeti za subjekte koji žele ući na tržište EU-a.

- **Supsidijarnost (za neisključivu nadležnost)**

Zbog općenito izrazito prekogranične prirode kibersigurnosti te sve učestalijih rizika i incidenata čiji se učinci prelijevaju preko granica te na druge sektore i proizvode države članice ne mogu same učinkovito postići ciljeve ove intervencije. Nacionalni pristupi rješavanju tih problema, posebice pristupi kojima se uvode obvezni zahtjevi, prouzročit će dodatnu pravnu nesigurnost i pravne zapreke. Poduzećima bi moglo biti onemogućeno neometano širenje u druge države članice, pa bi korisnici bili uskraćeni za pogodnosti njihovih proizvoda.

Dakle, zajedničko djelovanje na razini EU-a potrebno je kako bi se postiglo veliko povjerenje korisnika i povećala privlačnost proizvoda s digitalnim elementima iz EU-a. To bi

---

8 Presuda Suda (veliko vijeće) od 3. prosinca 2019., Češka Republika protiv Europskog parlamenta i Vijeća Europske unije, predmet C-482/17, točka 35.

9 Presuda Suda (veliko vijeće) od 2. svibnja 2006., Ujedinjena Kraljevina Velike Britanije i Sjeverne Irske protiv Europskog parlamenta i Vijeća Europske unije, predmet C-217/04, točke 62. i 63.

10 Na primjer, Finska je 2019. uspostavila program označivanja uređaja interneta stvari, kao što su pametni televizori, pametni telefoni i igračke, na temelju normi ETSI-ja. Njemačka je nedavno uvela potrošačku oznaku sigurnosti za širokopojasne rutere, pametne televizore, kamere, zvučnike, igračke te robote za čišćenje i vrtlarenje.

pogodovalo i jedinstvenom digitalnom tržištu te unutarnjem tržištu općenito zbog stvaranja pravne sigurnosti i jednakih uvjeta za proizvođače proizvoda s digitalnim elementima.

Naposljetku, u Zaključcima Vijeća od 23. svibnja 2022. o razvoju položaja Europske unije u pogledu kiberprostora Komisiju se poziva da do kraja 2022. predloži zajedničke kibersigurnosne zahtjeve za povezane uređaje.

- **Proporcionalnost**

Kad je riječ o proporcionalnosti predložene uredbe, mjere u okviru razmatranih opcija politike ne bi prelazile ono što je potrebno za postizanje općih i posebnih ciljeva te se njima ne bi nametnuli neproporcionalni troškovi. Točnije, razmatranom bi se intervencijom proizvodi s digitalnim elementima zaštitili tijekom cijelog životnog ciklusa proporcionalno rizicima kojima su izloženi primjenom tehnološki neutralnih zahtjeva koji su orijentirani na ciljeve, razumni i općenito u skladu s interesima uključenih subjekata.

Bitni kibersigurnosni zahtjevi u Prijedlogu temelje se na normama koje se uobičajeno primjenjuju, a u naknadnom postupku normizacije uzele bi se u obzir tehničke specifičnosti proizvoda. To znači da bi se sigurnosne kontrole prema potrebi prilagodile ovisno o razini rizika. Nadalje, predviđenim horizontalnim pravilima ocjenjivanje koje provodi treća strana propisalo bi se samo za rizične proizvode. To bi uključivalo samo mali udio tržišta za proizvode s digitalnim elementima. Učinak na MSP-ove ovisio bi o njihovoj prisutnosti na tržištu unutar tih specifičnih kategorija proizvoda.

Kad je riječ o proporcionalnosti troškova ocjenjivanja sukladnosti, prijavljena tijela koja provode ocjenjivanje kao treće strane naknade bi određivala s obzirom na veličinu poduzeća. Kako bi odgovarajuća tržišta imala dovoljno vremena za pripremu uz jasan smjer za ulaganja u istraživanje i razvoj, propisalo bi se i razumno prijelazno razdoblje od 24 mjeseca za pripremu provedbe. Koristi koje donosi veća sigurnost proizvoda s digitalnim elementima i, naposljetku, porast povjerenja korisnika u te proizvode, nadmašili bi sve troškove usklađivanja za poduzeća.

- **Odabir instrumenta**

Regulatorna intervencija podrazumijevala bi donošenje uredbe, a ne direktive. To je zato što bi se, za ovu vrstu zakonodavstva o proizvodima, uredbom djelotvornije riješili utvrđeni problemi i ispunili definirani ciljevi jer je riječ o intervenciji kojom se uvjetuje stavljanje na unutarnje tržište vrlo široke kategorije proizvoda. Postupak prijenosa u slučaju donošenja direktive za takvu intervenciju mogao bi ostaviti previše prostora za diskrecijske odluke na nacionalnoj razini, što bi moglo uzrokovati neujednačenost određenih bitnih kibersigurnosnih zahtjeva, pravnu nesigurnost, dodatnu rascjepkanost ili čak diskriminatorne prekogranične situacije, tim više ako se uzme u obzir to da obuhvaćeni proizvodi mogu imati višestruku namjenu ili uporabu te da proizvođači mogu proizvesti više kategorija takvih proizvoda.

3. REZULTATI EX POST EVALUACIJA, SAVJETOVANJA S DIONICIMA I PROCJENA UČINKA

- **Savjetovanja s dionicima**

Komisija se savjetovala sa širokim krugom dionika. Države članice i dionici pozvani su da sudjeluju u otvorenom javnom savjetovanju te u anketama i radionicama organiziranima u okviru studije koju je kao pomoć Komisiji u pripremama za procjenu učinka proveo konzorcij Wavestone, Centar za studije europskih politika (CEPS) i ICF. Sudjelovala su nacionalna tijela za nadzor tržišta, tijela Unije koja se bave kibersigurnošću, proizvođači hardvera i softvera, uvoznici i distributeri hardvera i softvera, trgovinska udruženja, organizacije

potrošača, korisnici proizvoda s digitalnim elementima, građani, istraživači i akademska zajednica, prijavljena tijela i akreditacijska tijela te stručnjaci iz sektora kibersigurnosti.

Aktivnosti savjetovanja obuhvaćale su:

- prvu studiju koju je proveo konzorcij organizacija ICF, Wavestone, Carsa i CEPS te koja je objavljena u prosincu 2021.[11] U toj studiji utvrđeno je nekoliko tržišnih nedostataka te su ocijenjene moguće regulatorne intervencije;
- otvoreno javno savjetovanje za građane, dionike i stručnjake za kibersigurnost. Dostavljeno je 176 odgovora. Ti su odgovori pomogli da se prikupe različita mišljenja i iskustva iz svih skupina dionika;
- radionice organizirane u okviru studije za potporu pripremnom radu Komisije za Akt o kiberotpornosti koje su okupile oko100 predstavnika iz svih 27 država članica koji su zastupali različite dionike;
- razgovore sa stručnjacima radi dobivanja podrobnijeg uvida u trenutačne kibersigurnosne probleme povezane s proizvodima s digitalnim elementima i razmatranja opcija politike za potencijalnu regulatornu intervenciju;
- bilateralne razgovore s nacionalnim tijelima za kibersigurnost, privatnim sektorom i organizacijama potrošača;
- ciljano savjetovanje s ključnim dionicima iz kruga MSP-ova.

- **Prikupljanje i primjena stručnog znanja**

Aktivnostima savjetovanja htjelo se prikupiti informacije o pet glavnih evaluacijskih kriterija na temelju Smjernica EU-a za bolju regulativu (djelotvornost, učinkovitost, relevantnost, usklađenost, dodana vrijednost za EU) te potencijalnim učincima mogućih opcija u budućnosti. Naručitelj se obratio ne samo dionicima na koje bi predložena uredba izravno utjecala nego se savjetovao i s nizom različitih stručnjaka za kibersigurnost.

- **Procjena učinka**

Komisija je provela procjenu učinka ovog Prijedloga, koju je ispitao Komisijin Odbor za nadzor regulative. Sastanak s Odborom za nadzor regulative održan je 6. srpnja 2022. te je taj odbor dao pozitivno mišljenje. Procjena učinka prilagođena je tako da se uzmu u obzir preporuke i primjedbe Odbora za nadzor regulative.

Komisija je ispitala različite opcije politike za postizanje općeg cilja Prijedloga:

- pravno neobvezujuće i dobrovoljne mjere (1. opcija): U okviru te opcije ne bi se provela obvezna regulatorna intervencija. Umjesto toga, Komisija bi izdala priopćenja, smjernice, preporuke i eventualno kodekse ponašanja kako bi potaknula dobrovoljne mjere. I dalje bi se razvijali nacionalni programi, dobrovoljni ili obvezni, kako bi se nadoknadio nedostatak horizontalnih pravila EU-a;

[11] Studija o potrebi za kibersigurnosnim zahtjevima za IKT proizvode – br. 2020-0715, Završno izvješće o studiji, dostupno na: https://digital-strategy.ec.europa.eu/hr/library/study-need-cybersecurity-requirements-ict-products.

- *ad hoc* regulatorna intervencija radi kibersigurnosti materijalnih proizvoda s digitalnim elementima i odgovarajućeg ugrađenog softvera (2. opcija): Ta bi opcija podrazumijevala *ad hoc* regulatornu intervenciju za pojedine proizvode koja bi bila ograničena na dodavanje i/ili izmjenu kibersigurnosnih zahtjeva u postojećim propisima ili uvođenje novih propisa ovisno o pojavi novih rizika, potencijalno i za neugrađeni softver;

Treća i četvrta opcija podrazumijevaju horizontalnu regulatornu intervenciju različitog područja primjene, uglavnom na temelju novog zakonodavnog okvira. Tim okvirom utvrđeni su bitni zahtjevi koji su uvjet za stavljanje određenih proizvoda na unutarnje tržište. U novom zakonodavnom okviru u pravilu je propisano i ocjenjivanje sukladnosti, postupak koji provodi proizvođač kako bi dokazao jesu li ispunjeni određeni zahtjevi koji se odnose na proizvod.

- mješoviti pristup, uključujući horizontalna obvezna pravila za kibersigurnost materijalnih proizvoda s digitalnim elementima i odgovarajućim ugrađenim softverom te postupni pristup za neugrađeni softver (3. opcija). Ta bi opcija podrazumijevala uredbu kojom bi se, kao uvjet za stavljanje na tržište, uveli horizontalni kibersigurnosni zahtjevi za sve materijalne proizvode s digitalnim elementima i softver ugrađen u njih te bi uključivala dvije podopcije s obveznim ocjenjivanjem koje provodi treća strana ili bez njega (3.i i 3.ii). Neugrađeni softver ne bi bio reguliran;
- horizontalna regulatorna intervencija kojom bi se uveli kibersigurnosni zahtjevi za širok raspon materijalnih i nematerijalnih digitalnih proizvoda, uključujući neugrađeni softver (4. opcija): Ta je opcija slična 3. opciji, osim u pogledu područja primjene. Prema 4. opciji područje primjene potencijalne uredbe obuhvaćalo bi neugrađeni softver (s dvjema podopcijama koje bi uključivale samo rizičan softver (4.a) ili sav softver (4.b)). Za svaku podopciju razmatrale bi se iste podopcije za ocjenjivanje sukladnosti kao i za 3. opciju.

Na temelju procjene djelotvornosti za ostvarenje posebnih ciljeva i procjene učinkovitosti troškova u odnosu na koristi prednost je dana 4. opciji (s podopcijama koje obuhvaćaju sav softver i uključuju obvezno ocjenjivanje rizičnih proizvoda koje provodi treća strana). Tom bi se opcijom osiguralo utvrđivanje posebnih horizontalnih kibersigurnosnih zahtjeva za sve proizvode s digitalnim elementima koji se stavljaju na unutarnje tržište ili na raspolaganje na unutarnjem tržištu te bi ona bila jedina opcija koja bi obuhvatila cjelokupni digitalni lanac opskrbe. Takvom regulatornom intervencijom obuhvatio bi se i neugrađeni softver, koji je često podložan ranjivostima, te tako postigao usklađen pristup prema svim proizvodima s digitalnim elementima, s jasnom podjelom odgovornosti raznih gospodarskih subjekata.

Ta opcija politike donosi i dodanu vrijednost jer obuhvaća obvezu postupanja s dužnom pažnjom i aspekte cijelog životnog ciklusa nakon stavljanja na tržište proizvoda s digitalnim elementima s ciljem da se, među ostalim, osigura pružanje odgovarajućih informacija o sigurnosnoj potpori i sigurnosnih ažuriranja. Njome bi se usto na najdjelotvorniji način dopunila nedavna revizija okvira za sigurnost mrežnih i informacijskih sustava jer bi se njome uredili preduvjeti za veću sigurnost lanaca opskrbe.

Najpoželjnija opcija donijela bi znatne koristi različitim dionicima. Kad je riječ o poduzećima, spriječila bi pojavu različitih sigurnosnih pravila za proizvode s digitalnim elementima i smanjila troškove usklađivanja s povezanim zakonodavstvom o kibersigurnosti. Smanjila bi broj kiberincidenata, troškove rješavanja incidenata i štetu za ugled. Procjenjuje se da bi inicijativa cijelom EU-u mogla smanjiti troškove od incidenata koji pogađaju poduzeća za otprilike 180 do 290 milijardi EUR godišnje. Dovela bi do povećanja prometa zbog veće prihvaćenosti proizvoda s digitalnim elementima. Poduzećima bi povećala globalni

ugled, pa bi potražnja porasla i izvan EU-a. Korisnicima bi najpoželjnija opcija povećala transparentnost sigurnosnih svojstava i olakšala uporabu proizvoda s digitalnim elementima. Potrošači i građani koristi bi imali i od bolje zaštite temeljnih prava kao što su pravo na privatnost i zaštitu podataka.

Upitani da ocijene djelotvornost intervencija politike, sudionici javnog savjetovanja složili su se da bi četvrta opcija bila najdjelotvornija mjera (4,08 na ljestvici od 1 do 5). Među njima su organizacije potrošača (5,00), sudionici koji su se identificirali kao korisnici (4,22), prijavljena tijela (4,17), tijela za nadzor tržišta (5,00) i proizvođači proizvoda s digitalnim elementima (3,85), uključujući male i srednje proizvođače (4,05).

- **Primjerenost i pojednostavnjenje propisa**

Ovim Prijedlogom utvrđuju se zahtjevi koji će se primjenjivati na proizvođače softvera i hardvera. Postoji potreba za pravnom sigurnošću i prestankom daljnjeg tržišnog cjepkanja zahtjeva koji se odnose na kibersigurnost proizvoda na unutarnjem tržištu, što je potvrdila široka potpora različitih dionika horizontalnoj intervenciji. Prijedlogom će se smanjiti regulatorno opterećenje proizvođača koje je posljedica postojanja više propisa o sigurnosti proizvoda. Usklađivanje s novim zakonodavnim okvirom omogućit će bolje funkcioniranje intervencije i njezine provedbe. Prijedlogom se pojednostavnjuje proces zaštitnih postupaka uključivanjem proizvođača i država članica prije obavješćivanja Komisije. Velik dio proizvođača obuhvaćenih područjem primjene Prijedloga već je upoznat s novim zakonodavnim okvirom, što će doprinijeti njegovu razumijevanju i provedbi. Kad je riječ o potrošačima i poduzećima, Prijedlogom će se promicati povjerenje u proizvode s digitalnim elementima.

- **Temeljna prava**

Prema procjenama, svim bi se opcijama politike u određenoj mjeri povećala zaštita temeljnih prava i sloboda kao što su privatnost, zaštita osobnih podataka, sloboda poslovanja i zaštita imovine ili osobnog dostojanstva i integriteta. U tom bi smislu najdjelotvornija bila najpoželjnija, 4. opcija politike, koja se sastoji od horizontalnih regulatornih intervencija i širokog područja primjene, jer je vjerojatnije da će doprinijeti smanjenju broja i težine incidenata, uključujući povrede osobnih podataka. Njome bi se i povećala pravna sigurnost i izjednačili uvjeti za gospodarske subjekte te povećali povjerenje među korisnicima i privlačnost proizvoda s digitalnim elementima iz EU-a u cjelini, a time bi se pak zaštitila imovina i poboljšali uvjeti za poslovanje gospodarskih subjekata.

Horizontalni kibersigurnosni zahtjevi doprinijeli bi sigurnosti osobnih podataka zaštitom povjerljivosti, cjelovitosti i dostupnosti informacija u proizvodima s digitalnim elementima. Sukladnost s tim zahtjevima olakšat će sukladnost sa zahtjevom za sigurnu obradu osobnih podataka prema Uredbi (EU) 2016/679 (Opća uredba o zaštiti podataka)[12]. Prijedlogom bi se poboljšala transparentnost i informiranost korisnika, uključujući korisnike koji možda nemaju dovoljno razvijene vještine u području kibersigurnosti. Korisnici bi bili bolje informirani i o rizicima, mogućnostima i ograničenjima proizvoda s digitalnim elementima, čime bi ih se stavilo u bolju poziciju jer bi mogli poduzeti potrebne preventivne mjere i mjere za ublažavanje radi smanjenja preostalih rizika.

[12] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka), SL L 119, 4.5.2016., str. 1.

4. UTJECAJ NA PRORAČUN

Kako bi se ispunile zadaće dodijeljene Agenciji Europske unije za kibersigurnost (ENISA) na temelju ove Uredbe, ENISA će morati preraspodijeliti približno 4,5 EPRV-a. Komisija bi trebala alocirati 7 EPRV-a kako bi ispunila odgovornosti povezane s provedbom prema ovoj Uredbi.

Detaljan pregled uključenih troškova nalazi se u „financijskom izvještaju" povezanom s ovim Prijedlogom.

5. DRUGI ELEMENTI

- **Planovi provedbe i mehanizmi praćenja, evaluacije i izvješćivanja**

Komisija će pratiti provedbu, primjenu i sukladnost s tim novim odredbama kako bi procijenila njihovu djelotvornost. Komisija će prema Uredbi biti dužna provesti evaluaciju i preispitivanje te Europskom parlamentu i Vijeću podnijeti javno izvješće o njima najkasnije 36 mjeseci od datuma početka njezine primjene i nakon toga svake četiri godine.

- **Detaljno obrazloženje posebnih odredaba prijedloga**

Opće odredbe (poglavlje I.)

Predloženom uredbom utvrđuju se (a) pravila za stavljanje na tržište proizvoda s digitalnim elementima kako bi se zajamčila kibersigurnost takvih proizvoda; (b) bitni zahtjevi za projektiranje, razvoj i proizvodnju proizvoda s digitalnim elementima te obveze gospodarskih subjekata u vezi s tim proizvodima koje se odnose na kibersigurnost; (c) bitni zahtjevi za postupke upravljanje ranjivostima koje proizvođači uspostave kako bi zajamčili kibersigurnost proizvoda s digitalnim elementima tijekom cijelog životnog ciklusa i obveze gospodarskih subjekata u pogledu tih postupaka; (d) pravila o nadzoru tržišta i provedbi prethodno navedenih pravila i zahtjeva.

Predložena uredba primjenjivat će se na proizvode s digitalnim elementima čija namjena i razumno predvidljiva uporaba uključuje izravnu ili neizravnu logičku ili fizičku podatkovnu vezu s uređajem ili mrežom.

Predložena uredba neće se primjenjivati na proizvode s digitalnim elementima obuhvaćene područjem primjene Uredbe (EU) 2017/745 [medicinski proizvodi za ljudsku uporabu te pribor za takve proizvode] i Uredbe (EU) 2017/746 [*in vitro* dijagnostički medicinski proizvodi za ljudsku uporabu i pribor za takve proizvode] jer obje te uredbe sadržavaju zahtjeve za proizvode, uključujući softver i opće obveze proizvođača, koji se odnose na cijeli životni ciklus proizvoda te postupke ocjenjivanja sukladnosti. Ova se Uredba neće primjenjivati na proizvode s digitalnim elementima koji su certificirani u skladu s Uredbom 2018/1139 [visoka i ujednačena razina sigurnosti civilnog zrakoplovstva] ni na proizvode na koje se primjenjuje Uredba (EU) 2019/2144 [o zahtjevima za homologaciju tipa za motorna vozila i njihove prikolice te za sustave, sastavne dijelove i zasebne tehničke jedinice namijenjene za takva vozila].

Rizični proizvodi s digitalnim elementima podlijegat će posebnim postupcima ocjenjivanja sukladnosti te će biti podijeljeni u I. i II. razred, kako je utvrđeno u Prilogu III., prema razini kibersigurnosnog rizika, pri čemu II. razred znači veći rizik. Rizičnost i uvrštavanje proizvoda s digitalnim elementima u Prilog III. određuje se s obzirom na utjecaj potencijalnih kibersigurnosnih ranjivosti proizvoda s digitalnim elementima. Pri određivanju kibersigurnosnog rizika u obzir se, među ostalim, uzimaju povezanost funkcionalnosti

proizvoda s digitalnim elementima s kibersigurnošću i je li mu namjena rad u osjetljivim okruženjima, primjerice industrijskom.

Komisija ima i ovlast za donošenje delegiranih akata za dopunu ove Uredbe određivanjem kategorija visokorizičnih proizvoda s digitalnim elementima za koje će proizvođači biti dužni ishoditi europski kibersigurnosni certifikat u okviru europskog programa kibersigurnosne certifikacije kako bi dokazali sukladnost s bitnim zahtjevima iz Priloga I. ili njihovim dijelovima. Pri određivanju takvih kategorija visokorizičnih proizvoda s digitalnim elementima Komisija će u obzir uzimati razinu kibersigurnosnog rizika povezanog s kategorijom proizvoda s digitalnim elementima prema jednom ili više kriterija za uvrštavanje rizičnih proizvoda s digitalnim elementima na popis u Prilogu III. te na temelju procjene je li to kategorija proizvoda koju rabe ili o kojoj ovise ključni subjekti koji pripadaju vrsti iz Priloga [Prilog I.] Direktivi [Direktiva XXX/XXXX (NIS2)] ili koja bi mogla biti važna za aktivnosti tih subjekata u budućnosti; ili je li ta kategorija proizvoda relevantna za otpornost cjelokupnog lanca opskrbe proizvoda s digitalnim elementima na remetilačke događaje.

Obveze gospodarskih subjekata (poglavlje II.)

Prijedlog uključuje obveze za proizvođače, uvoznike i distributere na temelju referentnih odredbi predviđenih Odlukom 768/2008/EZ. Svi proizvodi s digitalnim elementima smjeli bi se staviti na raspolaganje na tržištu samo ako ispunjavaju bitne kibersigurnosne zahtjeve utvrđene ovom Uredbom kad su ispravno isporučeni, instalirani i održavani te kad se upotrebljavaju u skladu s namjenom ili u uvjetima koji se mogu razumno predvidjeti.

Prema bitnim zahtjevima i obvezama proizvođači bi bili dužni uzimati u obzir kibersigurnost pri projektiranju, razvoju i proizvodnji proizvoda s digitalnim elementima, postupati s dužnom pažnjom u vezi sa sigurnosnim aspektima pri projektiranju i razvoju proizvoda, biti transparentni u vezi s aspektima kibersigurnosti s kojima kupcima trebaju biti upoznati, pružati sigurnosnu podršku (ažuriranja) na proporcionalan način i poštovati zahtjeve za upravljanje ranjivostima.

Utvrdile bi se obveze gospodarskih subjekata, od proizvođača do distributera i uvoznika, povezane sa stavljanjem na tržište proizvoda s digitalnim elementima, primjereno njihovoj ulozi i odgovornostima u lancu opskrbe.

Sukladnost proizvoda s digitalnim elementima (poglavlje III.)

Za proizvod s digitalnim elementima koji je sukladan s usklađenim normama ili dijelom usklađenih normi na koje su objavljena upućivanja u *Službenom listu Europske unije* pretpostavlja se da je sukladan s bitnim zahtjevima iz predložene Uredbe. Ako usklađene norme ne postoje ili su nedovoljne ili ako postoje neopravdana kašnjenja u postupku normizacije ili ako europske organizacije za normizaciju nisu prihvatile zahtjev Komisije, Komisija može provedbenim aktima donijeti zajedničke specifikacije.

Usto, za proizvode s digitalnim elementima koji su certificirani ili za koje su izdani EU izjava o sukladnosti ili certifikat u okviru europskog programa kibersigurnosne certifikacije na temelju Uredbe (EU) 2019/881 za koji je Komisija provedbenim aktom odredila da može stvoriti pretpostavku sukladnosti za potrebe ove Uredbe pretpostavlja se da su sukladni s bitnim zahtjevima iz ove Uredbe ili njihovim dijelovima u mjeri u kojoj EU izjava o sukladnosti ili kibersigurnosni certifikat, ili njihovi dijelovi, obuhvaćaju te zahtjeve.

Nadalje, kako bi se izbjeglo neopravdano administrativno opterećenje proizvođača kad je to moguće, Komisija bi trebala odrediti oslobađa li kibersigurnosni certifikat izdan u okviru takvog europskog programa kibersigurnosne certifikacije proizvođače obveze ocjenjivanja sukladnosti koje provodi treća strana kako je propisano ovom Uredbom za odgovarajuće zahtjeve.

Proizvođač provedbom jednog od postupaka iz Priloga VI. ocjenjuje sukladnost proizvoda s digitalnim elementima i postupaka upravljanja ranjivostima koje je uspostavio kako bi dokazao sukladnost s bitnim zahtjevima iz Priloga I. Proizvođači rizičnih proizvoda I. i II. razreda primjenjuju odgovarajuće module potrebne za sukladnost. Proizvođači rizičnih proizvoda II. razreda u ocjenjivanje sukladnosti moraju uključiti treću stranu.

Prijavljivanje tijela za ocjenjivanje sukladnosti (poglavlje IV.)

Pravilno funkcioniranje prijavljenih tijela ključno je za postizanje visoke razine kibersigurnosti i stjecanje povjerenja svih zainteresiranih strana u sustav novog pristupa. Stoga su Prijedlogom, u skladu s Odlukom 768/2008/EZ, utvrđeni zahtjevi za nacionalna tijela koja su nadležna za tijela za ocjenjivanje sukladnosti (prijavljena tijela). Krajnja odgovornost za određivanje i praćenje prijavljenih tijela ostavljena je državama članicama. Države članice određuju tijelo koje provodi prijavljivanje koje je nadležno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje i prijavljivanje tijelâ za ocjenjivanje sukladnosti te za praćenje prijavljenih tijela.

Nadzor tržišta i provedba (poglavlje V.)

U skladu s Uredbom (EU) 2019/1020 nacionalna tijela za nadzor tržišta provode nadzor tržišta na državnom području te države članice. Države članice mogu odrediti da bilo koje postojeće ili novo tijelo djeluje kao tijelo za nadzor tržišta, uključujući nacionalna nadležna tijela iz članka [članak X.] Direktive [Direktiva XXX/XXXX (NIS2)] ili imenovana nacionalna tijela za kibersigurnosnu certifikaciju iz članka 58. Uredbe (EU) 2019/881. Od gospodarskih subjekata traži se da u potpunosti surađuju s tijelima za nadzor tržišta i drugim nadležnim tijelima.

Delegiranje ovlasti i postupci odbora (poglavlje VI.)

Kako bi se regulatorni okvir mogao prema potrebi prilagođavati, Komisiji je delegirana ovlast za donošenje akata u skladu s člankom 290. UFEU-a radi ažuriranja popisa rizičnih proizvoda I. i II. razreda i određivanja definicija tih proizvoda, utvrđivanja je li potrebno ograničenje ili izuzeće za proizvode s digitalnim elementima obuhvaćene drugim pravilima Unije kojima se utvrđuju zahtjevi za postizanje iste razine zaštite kao i ovom Uredbom, uvođenje obveze certifikacije određenih visokorizičnih proizvoda s digitalnim elementima na temelju kriterija utvrđenih ovom Uredbom, određivanja minimalnog sadržaja EU izjave o sukladnosti i dodatnih elemenata koje treba uključiti u tehničku dokumentaciju.

Komisija je ovlaštena i za donošenje provedbenih akata kako bi: odredila format ili elementi obveza izvješćivanja i popisa softverskog materijala, odredila europske programe kibersigurnosne certifikacije koji se mogu primijeniti za dokazivanje sukladnosti s bitnim zahtjevima ili njihovim dijelovima iz ove Uredbe, donijela zajedničke specifikacije, utvrdila tehničke specifikacije za postavljanje oznake CE, donijela korektivne ili restriktivne mjere na razini Unije u iznimnim okolnostima koje opravdavaju brzu intervenciju radi očuvanja dobrog funkcioniranja unutarnjeg tržišta.

Povjerljivost i sankcije (poglavlje VII.)

Sve strane koje primjenjuju ovu Uredbu moraju poštovati povjerljivost informacija i podataka koje dobiju pri obavljanju svojih zadaća i aktivnosti.

Kako bi se osiguralo učinkovito izvršavanje obveza utvrđenih u ovoj Uredbi, svako tijelo za nadzor tržišta trebalo bi imati ovlast izricati ili zahtijevati izricanje upravnih novčanih kazni. U istom smislu ovom se Uredbom utvrđuju najviše upravne novčane kazne koje bi trebale biti uređene nacionalnim propisima za nepoštovanje obveza utvrđenih ovom Uredbom.

Prijelazne i završne odredbe (poglavlje VIII.)

Kako bi se proizvođačima, prijavljenim tijelima i državama članicama dalo dovoljno vremena za prilagodbu novim zahtjevima, predložena uredba postaje primjenjiva [24 mjeseca] nakon stupanja na snagu, osim obveze izvješćivanja za proizvođače, koja bi se primjenjivala od [12 mjeseci] nakon datuma stupanja na snagu.

2022/0272 (COD)

Prijedlog

UREDBE EUROPSKOG PARLAMENTA I VIJEĆA

o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima i o izmjeni Uredbe (EU) 2019/1020

(Tekst značajan za EGP)

EUROPSKI PARLAMENT I VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o funkcioniranju Europske unije, a posebno njegov članak 114.,

uzimajući u obzir prijedlog Europske komisije,

nakon prosljeđivanja nacrta zakonodavnog akta nacionalnim parlamentima,

uzimajući u obzir mišljenje Europskoga gospodarskog i socijalnog odbora[1],

uzimajući u obzir mišljenje Odbora regija[2],

u skladu s redovnim zakonodavnim postupkom,

budući da:

(1) Potrebno je poboljšati funkcioniranje unutarnjeg tržišta utvrđivanjem jedinstvenog pravnog okvira za bitne kibersigurnosne zahtjeve za stavljanje na tržište Unije proizvoda s digitalnim elementima. Trebalo bi riješiti dva glavna problema koji povećavaju troškove korisnicima i društvu: nisku razinu kibersigurnosti proizvoda s digitalnim elementima, čemu su dokaz raširene ranjivosti te nedovoljna i neredovita sigurnosna ažuriranja za njihovo otklanjanje, te to što korisnici nemaju dovoljno znanja ni informacija, pa ne mogu odabrati proizvode s odgovarajućim kibersigurnosnim obilježjima ili ih rabiti na siguran način.

(2) Ovom se Uredbom nastoje utvrditi okvirni uvjeti za razvoj sigurnih proizvoda s digitalnim elementima tako što će se urediti da se na tržište stavljaju hardverski i softverski proizvodi s manje ranjivosti i da proizvođači ozbiljno shvaćaju sigurnost tijekom cijelog životnog ciklusa proizvoda. Njome se ujedno nastoje stvoriti uvjeti koji bi korisnicima omogućili da proizvode s digitalnim elementima odabiru i rabe vodeći računa o kibersigurnosti.

(3) Relevantno zakonodavstvo Unije koje je trenutačno na snazi sastoji se od nekoliko skupova horizontalnih pravila kojima se iz različitih kutova uređuju određeni aspekti povezani s kibersigurnošću, uključujući mjere za povećanje sigurnosti digitalnog lanca opskrbe. Međutim, postojećim zakonodavstvom Unije koje se odnosi na kibersigurnost, uključujući [Direktivu XXX/XXXX (NIS2)] i Uredbu (EU) 2019/881

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

Europskog parlamenta i Vijeća[3] ne uređuju se izravno obvezni zahtjevi u pogledu sigurnosti proizvoda s digitalnim elementima.

(4) Iako se postojeće zakonodavstvo Unije primjenjuje na određene proizvode s digitalnim elementima, ne postoji horizontalni regulatorni okvir Unije kojim bi bili utvrđeni sveobuhvatni kibersigurnosni zahtjevi za sve proizvode s digitalnim elementima. Raznim dosad donesenim aktima i inicijativama na razini EU-a i na nacionalnoj razini samo se djelomično rješavaju utvrđeni problemi i rizici povezani s kibersigurnošću, pa na unutarnjem tržištu nastaje pravna neujednačenost, dobavljačima i korisnicima tih proizvoda povećava se pravna nesigurnost a poduzećima se nameće nepotrebno opterećenje jer moraju ispunjavati niz zahtjeva za slične vrste proizvoda.. Kibersigurnost tih proizvoda ima izrazitu prekograničnu dimenziju jer proizvode proizvedene u jednoj zemlji često rabe organizacije i potrošači na cjelokupnom unutarnjem tržištu. Stoga je to područje potrebno urediti na razini Unije. Regulatorni okvir Unije trebalo bi uskladiti uvođenjem kibersigurnosnih zahtjeva za proizvode s digitalnim elementima. Usto, trebalo bi stvoriti pravnu sigurnost za subjekte i korisnike u cijeloj Uniji te bolje uskladiti jedinstveno tržište, čime bi se stvorili održiviji uvjeti za subjekte koji žele ući na tržište Unije.

(5) U raznim programskim i političkim dokumentima na razini Unije, kao što su Strategija EU-a za kibersigurnost za digitalno desetljeće[4], zaključci Vijeća od 2. prosinca 2020. i 23. svibnja 2022. ili Rezolucija Europskog parlamenta od 10. lipnja 2021.[5], pozivalo se na donošenje posebnih kibersigurnosnih zahtjeva Unije za digitalne ili povezane proizvode, a nekoliko zemalja u svijetu na vlastitu je inicijativu uvelo mjere za uređenje tog pitanja. U završnom izvješću Konferencije o budućnosti Europe[6] građani su pozvali na „veću ulogu EU-a u borbi protiv prijetnji kibersigurnosti”.

(6) Kako bi se povećala ukupna razina kibersigurnosti svih proizvoda s digitalnim elementima koji se stavljaju na unutarnje tržište, za te je proizvode potrebno uvesti tehnološki neutralne bitne kibersigurnosne zahtjeve koji su orijentirani na ciljeve i primjenuju se horizontalno.

(7) Pod određenim uvjetima svi proizvodi s digitalnim elementima koji su integrirani u veći elektronički informacijski sustav ili povezani s njim mogu poslužiti kao vektor napada za zlonamjerne aktere. Zbog toga čak i hardver i softver koji se smatraju manje rizičnima mogu olakšati početno ugrožavanje uređaja ili mreže i zlonamjernim akterima omogućiti povlašteni pristup sustavu ili lateralno kretanje sustavima. Stoga bi proizvođači trebali osigurati da su svi povezivi proizvodi s digitalnim elementima projektirani i razvijeni u skladu s bitnim zahtjevima iz ove Uredbe. To uključuje i proizvode koji se mogu fizički povezati hardverskim sučeljima i proizvode koji su logički povezani, na primjer mrežnim utičnicama, cjevovodima, datotekama, aplikacijskim programskim sučeljima ili bilo kojom drugom vrstom softverskog

---

3 Uredba (EU) 2019/881 Europskog parlamenta i Vijeća od 17. travnja 2019. o ENISA-i (Agencija Europske unije za kibersigurnost) te o kibersigurnosnoj certifikaciji u području informacijske i komunikacijske tehnologije i stavljanju izvan snage Uredbe (EU) br. 526/2013 (Akt o kibersigurnosti) (SL L 151, 7.6.2019., str. 15.).

4 JOIN(2020) 18 final, https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=JOIN:2020:18:FIN.

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

6 Konferencija o budućnosti Europe – izvješće o konačnom ishodu, svibanj 2022.; prijedlog 28, točka 2. Konferencija je održana od travnja 2021. do svibnja 2022. To je bila jedinstvena, građanski vođena primjena deliberativne demokracije na paneuropskoj razini u kojoj su sudjelovale tisuće europskih građana te politički akteri, socijalni partneri, predstavnici civilnog društva i ključni dionici.

sučelja. Budući da se kibersigurnosne prijetnje mogu širiti preko raznih proizvoda s digitalnim elementima prije nego što ispune određeni cilj, primjerice ulančavanjem više kodova za iskorištavanje ranjivosti, proizvođači bi također trebali osigurati kibersigurnost proizvoda koji su samo neizravno povezani s drugim uređajima ili mrežama.

(8) Utvrđivanjem kibersigurnosnih zahtjeva za stavljanje na tržište proizvoda s digitalnim elementima povećat će se kibersigurnost tih proizvoda i za potrošače i za poduzeća. To uključuje i zahtjeve za stavljanje na tržište potrošačkih proizvoda s digitalnim elementima namijenjenih za ranjive potrošače, kao što su igračke i uređaji za nadzor male djece.

(9) Ovom se Uredbom osigurava visoka razina kibersigurnosti proizvoda s digitalnim elementima. Njome se ne uređuju usluge, kao što je softver kao usluga, osim rješenja za daljinsku obradu podataka koja su povezana s proizvodom s digitalnim elementima kojima se smatra svaka obrada podataka na daljinu za koju je softver projektirao i razvio proizvođač tog proizvoda ili je projektiran i razvijen pod njegovom odgovornošću, a čiji bi nedostatak onemogućio obavljanje jedne od funkcija takvog proizvoda s digitalnim elementima. [Direktivom XXX/XXXX (NIS2)] utvrđuju se kibersigurnosni zahtjevi i zahtjevi za izvješćivanje o incidentima za ključne i važne subjekte, kao što je ključna infrastruktura, radi povećanja otpornosti usluga koje pružaju. [Direktiva XXX/XXXX (NIS2)] primjenjuje se na usluge računalstva u oblaku i modele usluga u oblaku, kao što je softver kao usluga. Područjem primjene te direktive obuhvaćeni su svi subjekti koji u Uniji pružaju usluge računalstva u oblaku i ispunjavaju ili premašuju prag za srednja poduzeća.

(10) Kako se ne bi ometale inovacije ili istraživanja, besplatni softver otvorenog koda razvijen ili isporučen izvan komercijalne djelatnosti ne bi trebao biti obuhvaćen ovom Uredbom. To se posebice odnosi na softver, uključujući njegov izvorni kod i izmijenjene verzije, koji se otvoreno dijeli i besplatno je dostupan te se besplatno može rabiti, mijenjati i dalje distribuirati. U kontekstu softvera komercijalna djelatnost ne mora podrazumijevati samo naplaćivanje proizvoda nego i naplaćivanje usluga tehničke podrške, pružanje softverske platforme putem koje proizvođač unovčuje druge usluge ili uporaba osobnih podataka u svrhe koje nisu isključivo povećanje sigurnosti, kompatibilnosti ili interoperabilnosti softvera.

(11) Ključne infrastrukture i društvo u cjelini ne mogu funkcionirati bez interneta. [Direktivom XXX/XXXX (NIS2)] nastoji se osigurati visoka razina kibersigurnosti usluga ključnih i važnih subjekata, uključujući pružatelje digitalne infrastrukture koji podupiru osnovne funkcije otvorenog interneta te omogućuju pristup internetu i internetske usluge. Stoga je važno da se proizvodi s digitalnim elementima koji su pružateljima digitalne infrastrukture nužni za osiguravanje funkcioniranja interneta razvijaju na siguran način i da su u skladu s uvriježenim standardima u području internetske sigurnosti. Ovom Uredbom, koja se primjenjuje na sve povezive hardverske i softverske proizvode, nastoji se i pružateljima digitalne infrastrukture olakšati poštovanje zahtjeva koji se odnose na lance opskrbe prema [Direktivi XXX/XXXX (NIS2)] tako što se propisuju siguran razvoj i dostupnost pravodobnih sigurnosnih ažuriranja proizvoda s digitalnim elementima koje pružatelji digitalne infrastrukture rabe za pružanje usluga.

(12) Uredbom (EU) 2017/745 Europskog parlamenta i Vijeća[7] utvrđuju se pravila za medicinske proizvode, a Uredbom (EU) 2017/746 Europskog parlamenta i Vijeća[8] za *in vitro* dijagnostičke medicinske proizvode. U obje se uređuje pitanje kibersigurnosnih rizika i temelje se na posebnim pristupima kao i ova Uredba. Točnije, uredbama (EU) 2017/745 i (EU) 2017/746 utvrđuju se bitni zahtjevi za medicinske proizvode koji funkcioniraju putem elektroničkog sustava ili koji su sami softver. Njima su obuhvaćeni i određeni neugrađeni softver te pristup koji se temelji na cijelom životnom ciklusu. Prema tim zahtjevima proizvođači su dužni primjenjivati načelâ upravljanja rizikom pri razvoju i izradi proizvoda te utvrditi zahtjeve koji se odnose na mjere IT sigurnosti te odgovarajuće postupke ocjenjivanja sukladnosti. Nadalje, od prosinca 2019. na snazi su posebne smjernice za kibersigurnost medicinskih proizvoda kojima se proizvođačima medicinskih proizvoda, što uključuje *in vitro* dijagnostičke proizvode, razjašnjava kako ispuniti sve relevantne bitne zahtjeve iz Priloga I. tim uredbama u pogledu kibersigurnosti[9]. Stoga se ova Uredba ne bi trebala primjenjivati na proizvode s digitalnim elementima na koje se primjenjuje bilo koja od tih uredbi.

(13) Uredbom (EU) 2019/2144 Europskog parlamenta i Vijeća[10] utvrđeni su zahtjevi za homologaciju vozila i njihovih sustava i sastavnih dijelova te su pritom uvedeni određeni kibersigurnosni zahtjevi, među ostalim u pogledu rada certificiranog sustava upravljanja kibersigurnošću i ažuriranja softvera, koji se odnose na politike i postupke organizacijâ za upravljanje kiberrizicima tijekom cijelog životnog ciklusa vozila, opreme i usluga u skladu s primjenjivim pravilnicima Ujedinjenih naroda o tehničkim specifikacijama i kibersigurnosti[11]te na posebne postupke ocjenjivanja sukladnosti. U području zrakoplovstva, glavni je cilj Uredbe (EU) 2018/1139 Europskog parlamenta i Vijeća[12] uspostaviti i održavati visoku i ujednačenu razinu sigurnosti civilnog zrakoplovstva u Uniji. Tom je uredbom uspostavljen okvir za bitne zahtjeve u pogledu

---

7 Uredba (EU) 2017/745 Europskog parlamenta i Vijeća od 5. travnja 2017. o medicinskim proizvodima, o izmjeni Direktive 2001/83/EZ, Uredbe (EZ) br. 178/2002 i Uredbe (EZ) br. 1223/2009 te o stavljanju izvan snage direktiva Vijeća 90/385/EEZ i 93/42/EEZ (SL L 117, 5.5.2017., str. 1.).

8 Uredba (EU) 2017/746 Europskog parlamenta i Vijeća od 5. travnja 2017. o *in vitro* dijagnostičkim medicinskim proizvodima te o stavljanju izvan snage Direktive 98/79/EZ i Odluke Komisije 2010/227/EU (SL L 117, 5.5.2017., str. 176.).

9 Smjernice MDCG 2019-16, koje je odobrila Koordinacijska skupina za medicinske proizvode (MDCG) osnovana člankom 103. Uredbe (EU) 2017/745.

10 Uredba (EU) 2019/2144 Europskog parlamenta i Vijeća od 27. studenoga 2019. o zahtjevima za homologaciju tipa za motorna vozila i njihove prikolice te za sustave, sastavne dijelove i zasebne tehničke jedinice namijenjene za takva vozila, u pogledu njihove opće sigurnosti te zaštite osoba u vozilima i nezaštićenih sudionika u cestovnom prometu, o izmjeni Uredbe (EU) 2018/858 Europskog parlamenta i Vijeća i stavljanju izvan snage uredbi (EZ) br. 78/2009, (EZ) br. 79/2009 i (EZ) br. 661/2009 Europskog parlamenta i Vijeća i uredbi Komisije (EZ) br. 631/2009, (EU) br. 406/2010, (EU) br. 672/2010, (EU) br. 1003/2010, (EU) br. 1005/2010, (EU) br. 1008/2010, (EU) br. 1009/2010, (EU) br. 19/2011, (EU) br. 109/2011, (EU) br. 458/2011, (EU) br. 65/2012, (EU) br. 130/2012, (EU) br. 347/2012, (EU) br. 351/2012, (EU) br. 1230/2012 i (EU) 2015/166 (SL L 325, 16.12.2019., str. 1.).

11 Pravilnik UN-a br. 155 – Jedinstvene odredbe o homologaciji vozila s obzirom na kibersigurnost i sustav za upravljanje kibersigurnošću [2021/387].

12 Uredba (EU) 2018/1139 Europskog parlamenta i Vijeća od 4. srpnja 2018. o zajedničkim pravilima u području civilnog zrakoplovstva i osnivanju Agencije Europske unije za sigurnost zračnog prometa i izmjeni uredbi (EZ) br. 2111/2005, (EZ) br. 1008/2008, (EU) br. 996/2010, (EU) br. 376/2014 i direktiva 2014/30/EU i 2014/53/EU Europskog parlamenta i Vijeća te stavljanju izvan snage uredbi (EZ) br. 552/2004 i (EZ) br. 216/2008 Europskog parlamenta i Vijeća i Uredbe Vijeća (EEZ) br. 3922/91 (SL L 212, 22.8.2018., str. 1.).

plovidbenosti za aeronautičke proizvode, dijelove i opremu, uključujući softver, kojim su uzete u obzir obveze zaštite od prijetnji informacijskoj sigurnosti. Stoga proizvodi s digitalnim elementima na koje se primjenjuje Uredba (EU) 2019/2144 i proizvodi certificirani u skladu s Uredbom (EU) 2018/1139 ne podliježu bitnim zahtjevima i postupcima ocjenjivanja sukladnosti utvrđenima u ovoj Uredbi. Postupkom certifikacije na temelju Uredbe (EU) 2018/1139 postiže se razina jamstva koja se nastoji postići ovom Uredbom.

(14) Ovom se Uredbom utvrđuju horizontalna pravila o kibersigurnosti koja nisu specifična za sektore ili određene proizvode s digitalnim elementima. Međutim, mogla bi se uvesti Unijina sektorska pravila ili pravila za pojedine proizvode kojima bi se utvrdili zahtjevi koji se odnose na sve ili neke rizike obuhvaćene bitnim zahtjevima utvrđenima ovom Uredbom. U takvim se slučajevima ova Uredba na proizvode s digitalnim elementima obuhvaćene drugim pravilima Unije kojima se utvrđuju zahtjevi koji se odnose na sve ili neke rizike obuhvaćene bitnim zahtjevima iz Priloga I. ovoj Uredbi može primjenjivati ograničeno ili ne primjenjivati ako je takvo ograničenje, odnosno neprimjena, u skladu s općim regulatornim okvirom koji se primjenjuje na te proizvode i ako se sektorskim pravilima postiže razina zaštite jednaka onoj propisanoj ovom Uredbom. Komisija je ovlaštena donositi delegirane akte radi izmjene ove Uredbe utvrđivanjem takvih proizvoda i pravila. Za postojeće zakonodavstvo Unije u odnosu na koje bi se trebala primjenjivati takva ograničenja, odnosno neprimjena, ova Uredba sadržava posebne odredbe kojima se pojašnjava njezin odnos s tim zakonodavstvom Unije.

(15) Delegiranom uredbom (EU) 2022/30 utvrđeno je da se bitni zahtjevi iz članka 3. stavka 3. točke (d) (šteta za mrežu i zlouporaba mrežnih resursa), točke (e) (osobni podaci i privatnost) i točke (f) (prijevara) Direktive 2014/53/EU primjenjuju na određenu radijsku opremu. [Provedbenom odlukom Komisije XXX/2022 o zahtjevu za normizaciju upućenom europskim organizacijama za normizaciju] utvrđeni su zahtjevi za izradu posebnih normi kojima se pobliže određuje kako bi trebalo ispuniti ta tri bitna zahtjeva. Bitni zahtjevi utvrđeni ovom Uredbom uključuju sve elemente bitnih zahtjeva iz članka 3. stavka 3. točaka (d), (e) i (f) Direktive 2014/53/EU. Nadalje, bitni zahtjevi utvrđeni ovom Uredbom usklađeni su s ciljevima zahtjevâ za posebne norme uključene u taj zahtjev za normizaciju. Dakle, ako Komisija Delegiranu uredbu (EU) 2022/30 stavi izvan snage ili je izmijeni tako da se ona prestane primjenjivati na određene proizvode koji podliježu ovoj Uredbi, Komisija i europske organizacije za normizaciju trebale bi u okviru pripreme i izrade usklađenih normi radi lakše provedbe ove Uredbe uzeti u obzir rad na normizaciji proveden u kontekstu Provedbene odluke Komisije C(2022)5637 o zahtjevu za normizaciju za potrebe Direktive o radijskoj opremi i Delegirane uredbe (EU) 2022/30.

(16) Direktiva 85/374/EEZ[13] dopunjava ovu Uredbu. Tom direktivom utvrđena su pravila o odgovornosti za neispravne proizvode kako bi oštećene osobe mogle zatražiti naknadu ako su štetu prouzročili neispravni proizvodi. Njome je uspostavljeno načelo da je proizvođač proizvoda odgovoran za štetu prouzročenu pomanjkanjem sigurnosti njegova proizvoda neovisno o krivnji („objektivna odgovornost”). Ako takvo pomanjkanje sigurnosti čini nedostatak sigurnosnih ažuriranja nakon stavljanja proizvoda na tržište i to prouzroči štetu, proizvođač može snositi odgovornost. Obveze

[13] Direktiva Vijeća 85/374/EEZ od 25. srpnja 1985. o približavanju zakona i drugih propisa država članica u vezi s odgovornošću za neispravne proizvode (SL L 210, 7.8.1985.).

proizvođača koje se odnose na pružanje takvih sigurnosnih ažuriranja trebalo bi utvrditi ovom Uredbom.

(17) Ovom se Uredbom ne bi trebalo dovesti u pitanje Uredbu (EU) 2016/679 Europskog parlamenta i Vijeća[14], uključujući odredbe o uspostavi mehanizama certificiranja zaštite podataka te pečata i oznaka za zaštitu podataka za potrebe dokazivanja usklađenosti postupaka obrade koje obavljaju voditelji ili izvršitelji obrade s tom uredbom. Takvi bi se postupci mogli ugraditi u proizvod s digitalnim elementima. Tehnička i integrirana zaštita podataka te općenito kibersigurnost ključni su elementi Uredbe (EU) 2016/679. Štiteći potrošače i organizacije od kibersigurnosnih rizika, bitni kibersigurnosni zahtjevi iz ove Uredbe trebali bi doprinijeti i poboljšanju zaštite osobnih podataka i privatnosti pojedinaca. Trebalo bi razmotriti moguće sinergije u području normizaciji i certifikaciji s obzirom na kibersigurnosne aspekte u okviru suradnje između Komisije, europskih organizacija za normizaciju, Agencije Europske unije za kibersigurnost (ENISA), Europskog odbora za zaštitu podataka uspostavljenog Uredbom (EU) 2016/679 i nacionalnih nadzornih tijela za zaštitu podataka. Sinergije između ove Uredbe i prava Unije o zaštiti podataka trebalo bi stvoriti i u području nadzora tržišta i provedbe. U tu bi svrhu nacionalna tijela za nadzor tržišta imenovana na temelju ove Uredbe trebala surađivati s tijelima koja nadziru pravo Unije o zaštiti podataka. Tijela koja nadziru pravo Unije o zaštiti podataka trebala bi ujedno imati pristup informacijama važnima za obavljanje svojih zadaća.

(18) U mjeri u kojoj su njihovi proizvodi obuhvaćeni područjem primjene ove Uredbe, izdavatelji europske lisnice za digitalni identitet iz članka [članak 6.a stavak 2. Uredbe (EU) br. 910/2014, kako je izmijenjena Prijedlogom uredbe o izmjeni Uredbe (EU) br. 910/2014 u pogledu uspostavljanja europskog okvira za digitalni identitet] trebali bi poštovati horizontalne bitne zahtjeve iz ove Uredbe i posebne sigurnosne zahtjeve iz članka [članak 6.a Uredbe (EU) br. 910/2014., kako je izmijenjena Prijedlogom uredbe o izmjeni Uredbe (EU) br. 910/2014 u pogledu uspostavljanja europskog okvira za digitalni identitet]. Kako bi se to olakšalo, izdavatelji lisnica trebali bi moći certificiranjem svojih proizvoda u okviru europskog programa kibersigurnosne certifikacije koji je uspostavljen na temelju Uredbe (EU) 2019/881 i za koji je Komisija provedbenim aktom utvrdila da stvara pretpostavku sukladnosti s ovom Uredbom dokazati sukladnost europskih lisnica za digitalni identitet s odgovarajućim zahtjevima iz oba ta akta u mjeri u kojoj certifikat, ili njegovi dijelovi, obuhvaća te zahtjeve.

(19) Određene zadaće propisane ovom Uredbom trebala bi obavljati ENISA, u skladu s člankom 3. stavkom 2. Uredbe (EU) 2019/881. Točnije, ENISA bi od proizvođača trebala primati obavijesti o iskorištenim ranjivostima proizvodâ s digitalnim elementima te o incidentima koji utječu na sigurnost tih proizvoda. ENISA bi ujedno te obavijesti trebala prosljeđivati relevantnim timovima za odgovor na računalne sigurnosne incidente (CSIRT-ovi) ili relevantnim jedinstvenim kontaktnim točkama država članica imenovanima u skladu s člankom [članak X.] Direktive [Direktiva XXX/XXXX (NIS2)] te bi o prijavljenoj ranjivosti trebala obavijestiti nadležna tijela za nadzor tržišta. Na temelju informacija koje prikupi ENISA bi trebala izraditi dvogodišnje tehničko izvješće o novim trendovima u području kibersigurnosnih rizika

[14] Uredba (EU) 2016/679 Europskog parlamenta i Vijeća od 27. travnja 2016. o zaštiti pojedinaca u vezi s obradom osobnih podataka i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Direktive 95/46/EZ (Opća uredba o zaštiti podataka) (SL L 119, 4.5.2016., str. 1.).

proizvoda s digitalnim elementima i dostaviti ga skupini za suradnju iz Direktive [Direktiva XXX/XXXX (NIS2)]. Nadalje, s obzirom na svoju stručnost i ovlasti, ENISA bi trebala moći pružati potporu procesu provedbe ove Uredbe. Točnije, trebala bi moći predlagati zajedničke aktivnosti koje bi provodila tijela za nadzor tržišta na temelju naznaka ili informacija povezanih s potencijalnom nesukladnošću proizvodâ s digitalnim elementima s ovom Uredbom u nekoliko država članica ili utvrditi kategorije proizvoda za koje bi trebalo organizirati istodobne koordinirane kontrolne mjere. U iznimnim okolnostima, kad je potrebna brza intervencija radi očuvanja dobrog funkcioniranja unutarnjeg tržišta, ENISA bi, na zahtjev Komisije, trebala moći provesti evaluacije povezane sa specifičnim proizvodima s digitalnim elementima koji predstavljaju znatan kibersigurnosni rizik.

(20) Proizvodi s digitalnim elementima trebali bi imati oznaku CE kao znak sukladnosti s ovom Uredbom kako bi se mogli slobodno kretati na unutarnjem tržištu. Države članice ne bi trebale stvarati neopravdane zapreke stavljanju na tržište proizvoda s digitalnim elementima koji su sukladni sa zahtjevima iz ove Uredbom i imaju oznaku CE.

(21) Kako bi proizvođači mogli izdavati softver u svrhu testiranja prije ocjenjivanja sukladnosti svojih proizvoda, države članice ne bi trebale sprečavati stavljanje na raspolaganje nedovršenog softvera, kao što su alfa verzije, beta verzije ili potencijalne verzije za objavu, pod uvjetom da je verzija stavljena na raspolaganje samo na razdoblje potrebno za testiranje i prikupljanje povratnih informacija. Proizvođači bi se trebali pobrinuti da se softver koji se stavi na raspolaganje pod tim uvjetima objavi tek nakon procjene rizika i da je u najvećoj mogućoj mjeri sukladan sa sigurnosnim zahtjevima iz ove Uredbe koji se odnose na svojstva proizvoda s digitalnim elementima. Proizvođači bi u najvećoj mogućoj mjeri trebali ispuniti i zahtjeve koji se odnose na upravljanje ranjivostima. Proizvođači ne bi trebali korisnike primoravati na nadogradnje na verzije objavljene samo radi testiranja.

(22) Kako proizvodi s digitalnim elementima koji su stavljeni na tržište ne bi predstavljali kibersigurnosne rizike za osobe i organizacije, trebalo bi utvrditi bitne zahtjeve za takve proizvode. Kad se takvi proizvodi naknadno mijenjaju, fizičkim ili digitalnim sredstvima, na način koji proizvođač nije predvidio i koji može ukazivati na to da više ne ispunjavaju relevantne bitne zahtjeve, takva izmjena trebala bi se smatrati bitnom. Na primjer, ažuriranja ili popravci softvera mogu se izjednačiti s održavanjem pod uvjetom da se njima proizvod koji je već stavljen na tržište ne preinačuje na takav način da to može utjecati na sukladnost s primjenjivim zahtjevima ili promijeniti namjenu za koju je proizvod ocijenjen. Kao i u slučaju fizičkih popravaka ili preinaka, proizvod s digitalnim elementima trebao bi se smatrati bitno izmijenjenim softverskom promjenom ako se ažuriranjem softvera izmijene izvorne predviđene funkcije, vrsta ili radne karakteristike proizvoda, a te promjene nisu bile predviđene u prvotnoj procjeni rizika ili ako se zbog ažuriranja softvera promijenila vrsta rizika ili povećala razina rizika.

(23) U skladu s uvriježenim pojmom bitne izmjene za proizvode uređene zakonodavstvom Unije o usklađivanju primjereno je da se za proizvod s digitalnim elementima provede provjera sukladnosti i, prema potrebi, novi postupak ocjenjivanja sukladnosti kad god nastupi bitna izmjena koja može utjecati na sukladnost tog proizvoda s ovom Uredbom ili kad se promijeni njegova namjena. Kad je to primjenjivo, ako proizvođač provodi ocjenjivanje sukladnosti koje uključuje treću stranu, treću stranu trebalo bi obavijestiti o promjenama koje bi mogle dovesti do bitnih izmjena.

(24) Obnova, održavanje i popravak proizvoda s digitalnim elementima, kako je definirano u Uredbi [Uredba o ekološkom dizajnu], ne uzrokuju nužno bitnu izmjenu proizvoda, primjerice ako se ne promjene namjena, funkcije i razina rizika. Međutim, nadogradnja proizvoda koju je učinio proizvođač može uzrokovati promjene u projektu i razvoju proizvoda pa može utjecati na namjenu proizvoda i njegovu sukladnost sa zahtjevima iz ove Uredbe.

(25) Proizvodi s digitalnim elementima trebali bi se smatrati rizičnima ako štetne posljedice iskorištavanja njihovih potencijalnih kibersigurnosnih ranjivosti mogu biti teške zbog, među ostalim, njihove funkcionalnosti povezane s kibersigurnošću ili namjene. Točnije, ranjivosti proizvoda s digitalnim elementima koji imaju funkcionalnost povezanu s kibersigurnošću, kao što su sigurni elementi, mogu prouzročiti širenje sigurnosnih problema cijelim lancem opskrbe. Posljedice kiberincidenta mogu biti teže i zbog namjene proizvoda, primjerice ako je namijenjen za rad u industrijskom okruženju ili u kontekstu ključnog subjekta koji pripada vrsti iz Priloga [Prilog I.] Direktivi [Direktiva XXX/XXXX (NIS2)] ili pak za obavljanje ključnih ili osjetljivih funkcija kao što je obrada osobnih podataka.

(26) Rizični proizvodi s digitalnim elementima trebali bi podlijegati strožim postupcima ocjenjivanja sukladnosti, pri čemu bi se trebao zadržati proporcionalan pristup. U tu bi svrhu rizične proizvode s digitalnim elementima trebalo podijeliti u dva razreda prema razini kibersigurnosnog rizika povezanog s tim kategorijama proizvoda. Potencijalni kiberincident koji obuhvaća proizvode II. razreda mogao bi imati teže štetne posljedice od incidenta koji obuhvaća proizvode I. razreda, primjerice zbog prirode njihove funkcije povezane s kibersigurnošću ili namjene za rad u osjetljivim okruženjima, pa bi trebali podlijegati strožem postupku ocjenjivanja sukladnosti.

(27) Kategorije rizičnih proizvoda s digitalnim elementima iz Priloga III. ovoj Uredbi treba smatrati proizvodima čija osnovna funkcionalnost pripada vrsti navedenoj u Prilogu III. ovoj Uredbi. Na primjer, u Prilogu III. ovoj Uredbi navedeni su proizvodi koji su prema osnovnoj funkcionalnosti definirani kao općenamjenski mikroprocesori II. razreda. Zato općenamjenski mikroprocesori podliježu obveznom ocjenjivanju sukladnosti koje provodi treća strana. To se ne odnosi na druge proizvode koji nisu izričito navedeni u Prilogu III. ovoj Uredbi koji bi mogli imati integriran općenamjenski mikroprocesor. Komisija bi trebala donijeti delegirane akte [u roku od 12 mjeseci od stupanja na snagu ove Uredbe] radi određivanja definicija kategorija proizvoda obuhvaćenih I. i II. razredom kako je utvrđeno u Prilogu III.

(28) Ovom se Uredbom ciljano uređuju kibersigurnosni rizici. Međutim, proizvodi s digitalnim elementima mogu predstavljati druge sigurnosne rizike koji nisu povezani s kibersigurnošću. Takvi bi rizici i dalje trebali biti uređeni drugim relevantnim zakonodavstvom Unije o proizvodima. Ako drugo zakonodavstvo Unije o usklađivanju nije primjenjivo, na njih bi se trebala primjenjivati Uredba [Uredba o općoj sigurnosti proizvoda]. Dakle, s obzirom na ciljanu prirodu ove Uredbe i odstupajući od članka 2. stavka 1. trećeg podstavka točke (b) Uredbe [Uredba o općoj sigurnosti proizvoda], kad je riječ o sigurnosnim rizicima koji nisu obuhvaćeni ovom Uredbom, na proizvode s digitalnim elementima trebali bi se primjenjivati zahtjevi iz poglavlja III. odjeljka 1., poglavlja V. i VII. i poglavlja od IX. do XI. Uredbe [Uredba o općoj sigurnosti proizvoda] osim ako se na njih primjenjuju posebni zahtjevi iz drugog zakonodavstva Unije o usklađivanju u smislu [članka 3. točke 25. Uredbe o općoj sigurnosti proizvoda].

(29) Proizvodi s digitalnim elementima koji su klasificirani u visokorizične UI sustave u skladu s člankom 6. Uredbe[15] [Uredba o umjetnoj inteligenciji] i obuhvaćeni su područjem primjene ove Uredbe trebali bi biti sukladni s bitnim zahtjevima iz ove Uredbe. Ako ti visokorizični UI sustavi ispunjavaju bitne zahtjeve iz ove Uredbe, trebali bi se smatrati sukladnima sa zahtjevima za kibersigurnost iz članka [članak 15.] Uredbe [Uredba o umjetnoj inteligenciji] u mjeri u kojoj su ti zahtjevi obuhvaćeni EU izjavom o sukladnosti, ili njezinim dijelovima, izdanom na temelju ove Uredbe. Kad je riječ o postupcima ocjenjivanja sukladnosti koji se odnose na bitne kibersigurnosne zahtjeve za proizvode s digitalnim elementima koji su obuhvaćeni ovom Uredbom i klasificirani su u visokorizične UI sustave, umjesto odgovarajućih odredbi ove Uredbe u pravilu bi se trebale primjenjivati relevantne odredbe članka 43. Uredbe [Uredba o umjetnoj inteligenciji]. Međutim, to pravilo ne bi trebalo dovesti do smanjenja potrebne razine jamstva za rizične proizvode s digitalnim elementima obuhvaćene ovom Uredbom. Stoga bi se, odstupajući od tog pravila, na visokorizične UI sustave koji su obuhvaćeni područjem primjene Uredbe [Uredba o umjetnoj inteligenciji] i pripadaju rizičnim proizvodima s digitalnim elementima na temelju ove Uredbe te na koje se primjenjuje postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga VI. Uredbi [Uredba o umjetnoj inteligenciji] trebale primjenjivati odredbe ove Uredbe o ocjenjivanju sukladnosti u mjeri u kojoj se na njih odnose bitni zahtjevi iz ove Uredbe. U tom bi se slučaju za sve ostale aspekte obuhvaćene Uredbom [Uredba o umjetnoj inteligenciji] trebale primjenjivati odgovarajuće odredbe o ocjenjivanju sukladnosti na temelju unutarnje kontrole iz Priloga VI. Uredbi [Uredba o umjetnoj inteligenciji].

(30) Strojarski proizvodi obuhvaćeni područjem primjene Uredbe [Prijedlog uredbe o strojevima] koji su proizvodi s digitalnim elementima u smislu ove Uredbe i za koje je izdana izjava o sukladnosti na temelju ove Uredbe trebali bi se smatrati sukladnima s bitnim zdravstvenim i sigurnosnim zahtjevima iz [Prilog III., odjeljci 1.1.9. i 1.2.1.] Uredbi [Prijedlog uredbe o strojevima] u pogledu zaštite od kvarenja te sigurnosti i pouzdanosti kontrolnih sustava u mjeri u kojoj je EU izjavom o sukladnosti izdanom na temelju ove Uredbe dokazana sukladnost s tim zahtjevima.

(31) Uredba [Prijedlog uredbe o europskom prostoru za zdravstvene podatke] dopunjuje bitne zahtjeve utvrđene ovom Uredbom. Stoga bi i sustavi elektroničkih zdravstvenih zapisa obuhvaćeni područjem primjene Uredbe [Prijedlog uredbe o europskom prostoru za zdravstvene podatke] koji su proizvodi s digitalnim elementima u smislu ove Uredbe trebali biti sukladni s bitnim zahtjevima utvrđenima ovom Uredbom. Njihovi bi proizvođači trebali dokazati sukladnost kako se zahtijeva Uredbom [Prijedlog uredbe o europskom prostoru za zdravstvene podatke]. Kako bi lakše ispunili taj zahtjev, proizvođači mogu sastaviti jedinstvenu tehničku dokumentaciju koja sadržava elemente koji se zahtijevaju prema oba ta zakonska akta. Budući da ova Uredba ne obuhvaća softver kao uslugu, sustavi elektroničkih zdravstvenih zapisa koji se nude putem modela licenciranja i korištenja softvera kao usluge nisu obuhvaćeni područjem primjene ove Uredbe. Slično tome, sustavi elektroničkih zdravstvenih zapisa koji se razvijaju i upotrebljavaju interno nisu obuhvaćeni područjem primjene ove Uredbe jer se ne stavljaju na tržište.

(32) Kako bi proizvodi s digitalnim elementima bili sigurni i u trenutku njihova stavljanja na tržište i tijekom njihova cijelog životnog ciklusa, potrebno je utvrditi bitne zahtjeve

[15] Uredba [Uredba o umjetnoj inteligenciji].

za upravljanje ranjivostima i bitne kibersigurnosne zahtjeve koji se odnose na svojstva proizvoda s digitalnim elementima. Iako bi proizvođači trebali poštovati sve bitne zahtjeve u pogledu upravljanja ranjivostima i pobrinuti se da se svi njihovi proizvodi isporučuju bez poznatih iskoristivih ranjivosti, trebali bi odrediti koji su drugi bitni zahtjevi u pogledu svojstava proizvoda relevantni za tu vrstu proizvoda. U tu bi svrhu proizvođači trebali provesti procjenu kibersigurnosnih rizika povezanih s proizvodom s digitalnim elementima kako bi ustanovili relevantne rizike i bitne zahtjeve te kako bi na odgovarajući način primijenili odgovarajuće usklađene norme ili zajedničke specifikacije.

(33) Kako bi se povećala sigurnost proizvoda s digitalnim elementima koji se stavljaju na unutarnje tržište, potrebno je utvrditi bitne zahtjeve. Tim bitnim zahtjevima ne bi se trebale dovesti u pitanje koordinirane procjene rizika ključnih lanaca opskrbe u EU-u utvrđene [člankom X.] Direktive [Direktiva XXX/XXXX (NIS2)][16] u kojima se uzimaju u obzir tehnički i, prema potrebi, netehnički čimbenici rizika, kao što je nedopušteni utjecaj treće zemlje na dobavljače. Nadalje, ne bi se trebale dovesti u pitanje ovlasti država članica za utvrđivanje dodatnih zahtjeva kojima se uzimaju u obzir netehnički čimbenici za potrebe osiguravanja visoke razine otpornosti, uključujući one definirane u Preporuci (EU) 2019/534, koordiniranoj procjeni rizika za sigurnost 5G mreža u Uniji i paketu instrumenata EU-a za kibersigurnost 5G mreža koji je dogovorila skupina za suradnju u području sigurnosti mrežnih i informacijskih sustava iz [Direktive XXX/XXXX (NIS2)].

(34) Kako bi se osiguralo da nacionalni CSIRT-ovi i jedinstvene kontaktne točke imenovane u skladu s člankom [članak X.] Direktive [Direktiva XX/XXXX (NIS2)] dobivaju informacije potrebne za ispunjavanje svojih zadaća i povećanje ukupne razine kibersigurnosti ključnih i važnih subjekata te kako bi se osiguralo djelotvorno funkcioniranje tijela za nadzor tržišta, proizvođači proizvoda s digitalnim elementima trebali bi obavješćivati ENISA-u o ranjivostima koje se iskorištavaju. Budući da se većina proizvoda s digitalnim elementima stavlja na cijelo unutarnje tržište, svaka iskorištena ranjivost proizvoda s digitalnim elementima trebala bi se smatrati prijetnjom funkcioniranju unutarnjeg tržišta. Proizvođači bi trebali razmotriti i mogućnost unošenja popravljenih ranjivosti u europsku bazu podataka o ranjivostima koja je uspostavljena na temelju Direktive [Direktiva XX/XXXX (NIS2)] i kojom upravlja ENISA ili u bilo koju drugu javno dostupnu bazu podataka o ranjivostima.

(35) Proizvođači ujedno trebaju prijaviti ENISA-i svaki incident koji utječe na sigurnost proizvoda s digitalnim elementima. Neovisno o obvezama izvješćivanja o incidentima na temelju Direktive [Direktiva XXX/XXXX (NIS2)] za ključne i važne subjekte, presudno je da ENISA, jedinstvene kontaktne točke koje su države članice imenovale u skladu s člankom [članak X.] Direktive [Direktiva XXX/XXXX (NIS2)] i tijela za nadzor tržišta od proizvođača proizvoda s digitalnim elementima primaju informacije koje im omogućuju ocjenu sigurnosti tih proizvoda. Kako bi korisnici mogli brzo reagirati na incidente koji utječu na sigurnost njihovih proizvoda s digitalnim elementima, proizvođači bi i njih trebali obavijestiti o svakom takvom incidentu i, prema potrebi, o svim korektivnim mjerama koje oni mogu poduzeti za ublažavanje posljedica incidenta, primjerice objavljivanjem relevantnih informacija na svojim

[16] Direktiva XXX Europskog parlamenta i Vijeća od [datum] [o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije i stavljanju izvan snage Direktive (EU) 2016/1148 (SL L xx, datum, str. x.)].

internetskim stranicama ili, ako proizvođač može stupiti u kontakt s njima i rizici to opravdavaju, izravnim obraćanjem korisnicima.

(36) Proizvođači proizvoda s digitalnim elementima trebali bi uspostaviti politike koordiniranog otkrivanja ranjivosti kako bi pojedincima ili subjektima olakšali njihovo prijavljivanje. U politici koordiniranog otkrivanja ranjivosti trebalo bi utvrditi strukturirani postupak prijavljivanja ranjivosti proizvođaču koji omogućuje proizvođaču njihovo dijagnosticiranje i otklanjanje prije otkrivanja detaljnih informacija o njima trećim stranama ili javnosti. S obzirom na činjenicu da se informacije o iskoristivim ranjivostima proizvoda s digitalnim elementima koji se nalaze u širokoj uporabi mogu skupo prodati na crnom tržištu, proizvođači takvih proizvoda trebali bi moći provoditi, u okviru svojih politika koordiniranog otkrivanja ranjivosti, programe poticanja pojedinaca ili subjekata na prijavljivanje ranjivosti priznanjima i naknadama za njihov trud (tzv. „programi nagrađivanja pronalaska pogrešaka”).

(37) Kako bi se olakšala analiza ranjivosti, proizvođači bi trebali utvrditi i dokumentirati komponente proizvoda s digitalnim elementima, među ostalim sastavljanjem popisa softverskog materijala. Popis softverskog materijala može onima koji proizvode, kupuju i rabe softver pružiti informacije koje će im omogućiti da bolje razumiju lanac opskrbe, što donosi višestruke koristi, a ponajviše pomaže proizvođačima i korisnicima da prate poznate nove ranjivosti i rizike. Osobito je važno da se proizvođači pobrinu da njihovi proizvodi ne sadržavaju ranjive komponente koje su razvile treće strane.

(38) Kako bi se olakšalo ocjenjivanje sukladnosti sa zahtjevima iz ove Uredbe, trebala bi postojati pretpostavka sukladnosti proizvoda s digitalnim elementima koji su sukladni s usklađenim normama kojima su bitni zahtjevi iz ove Uredbe preneseni u detaljne tehničke specifikacije i koje su donesene u skladu s Uredbom (EU) br. 1025/2012 Europskog parlamenta i Vijeća[17]. Uredbom (EU) br. 1025/2012 propisan je postupak podnošenja prigovora na usklađene norme ako te norme ne udovoljavaju u potpunosti zahtjevima ove Uredbe.

(39) Uredbom (EU) 2019/881 uspostavljen je dobrovoljni europski okvir za kibersigurnosnu certifikaciju IKT proizvoda, procesa i usluga. Europski programi kibersigurnosne certifikacije mogu obuhvaćati proizvode s digitalnim elementima obuhvaćene ovom Uredbom. Ovom bi se Uredbom trebale stvoriti sinergije s Uredbom (EU) 2019/881. Kako bi se olakšalo ocjenjivanje sukladnosti sa zahtjevima utvrđenima ovom Uredbom, proizvodi s digitalnim elementima koji su certificirani ili za koje je izdana izjava o sukladnosti u okviru programa kibersigurnosti u skladu s Uredbom (EU) 2019/881 i koji je Komisija odredila provedbenim aktom smatraju se sukladnima s bitnim zahtjevima ove Uredbe u mjeri u kojoj kibersigurnosni certifikat ili izjava o sukladnosti, ili njihovi dijelovi, obuhvaćaju te zahtjeve. U kontekstu ove Uredbe trebalo bi procijeniti postoji li potreba za novim europskim programima kibersigurnosne certifikacije za proizvode s digitalnim elementima. U okviru takvih budućih europskih programa kibersigurnosne certifikacije koji bi obuhvaćali proizvode s digitalnim elementima trebalo bi uzeti u obzir bitne zahtjeve iz ove

[17] Uredba (EU) br. 1025/2012 Europskog parlamenta i Vijeća od 25. listopada 2012. o europskoj normizaciji, o izmjeni direktiva Vijeća 89/686/EEZ i 93/15/EEZ i direktiva 94/9/EZ, 94/25/EZ, 95/16/EZ, 97/23/EZ, 98/34/EZ, 2004/22/EZ, 2007/23/EZ, 2009/23/EZ i 2009/105/EZ Europskog parlamenta i Vijeća te o stavljanju izvan snage Odluke Vijeća 87/95/EEZ i Odluke br. 1673/2006/EZ Europskog parlamenta i Vijeća (SL L 316, 14.11.2012., str. 12.).

Uredbe i olakšati sukladnost s ovom Uredbom. Komisiju bi trebalo ovlastiti da provedbenim aktima odredi europske programe kibersigurnosne certifikacije koji se mogu primijeniti za dokazivanje sukladnosti s bitnim zahtjevima iz ove Uredbe. Nadalje, kako bi se izbjeglo neopravdano administrativno opterećenje proizvođača kad je to moguće, Komisija bi trebala odrediti oslobađa li kibersigurnosni certifikat izdan u okviru takvog europskog programa kibersigurnosne certifikacije proizvođače obveze ocjenjivanja sukladnosti koje provodi treća strana kako je propisano ovom Uredbom za odgovarajuće zahtjeve.

(40) Nakon stupanja na snagu provedbenog akta kojim se utvrđuje [Provedbena uredba Komisije (EU) br. …/… od XXX o europskom programu kibersigurnosne certifikacije koji se temelji na zajedničkim kriterijima] (EUCC) koji se odnosi na hardverske proizvode obuhvaćene ovom Uredbom, kao što su hardverski sigurnosni moduli i mikroprocesori, Komisija može provedbenim aktom utvrditi kako se EUCC-om stvara pretpostavku sukladnosti s bitnim zahtjevima iz Priloga I. ovoj Uredbi ili njihovim dijelovima. Nadalje, takvim provedbenim aktom može se odrediti na koji način certifikat izdan na temelju EUCC-a oslobađa proizvođače obveze ocjenjivanja koje provodi treća strana kako se zahtijeva ovom Uredbom za odgovarajuće zahtjeve.

(41) Ako usklađene norme nisu donesene ili njima nisu u dovoljnoj mjeri zahvaćeni bitni zahtjevi iz ove Uredbe, Komisija bi trebala moći provedbenim aktima donijeti zajedničke specifikacije. Takve se zajedničke specifikacije mogu izraditi umjesto usklađenih normi na primjer ako neka od europskih organizacija za normizaciju odbije zahtjev za normizaciju, ako postoje neopravdana kašnjenja u uspostavi odgovarajućih usklađenih normi ili ako izrađene norme nisu u dovoljnoj mjeri u skladu sa zahtjevima ove Uredbe ili na zahtjev Komisije. Kako bi se olakšalo ocjenjivanje sukladnosti s bitnim zahtjevima iz ove Uredbe, trebala bi postojati pretpostavka sukladnosti za proizvode s digitalnim elementima koji su sukladni sa zajedničkim specifikacijama koje je Komisija donijela u skladu s ovom Uredbom u svrhu utvrđivanja detaljnih tehničkih specifikacija tih zahtjeva.

(42) Proizvođači bi trebali sastaviti EU izjavu o sukladnosti kako bi dali informacije koje se zahtijevaju ovom Uredbom o sukladnosti proizvoda s digitalnim elementima s bitnim zahtjevima iz ove Uredbe i, prema potrebi, drugog relevantnog zakonodavstva Unije o usklađivanju koje se primjenjuju na taj proizvod. Od proizvođača se može zahtijevati i sastavljanje EU izjave o sukladnosti u skladu s drugim zakonodavstvom Unije. Kako bi se osigurao djelotvoran pristup informacijama u svrhu nadzora tržišta, trebalo bi sastaviti jedinstvenu EU izjavu o sukladnosti koja se odnosi na sukladnost sa svim relevantnim aktima Unije. Kako bi se smanjilo administrativno opterećenje gospodarskih subjekata, tu jedinstvenu EU izjavu o sukladnosti trebala bi moći činiti dokumentacija sastavljena od relevantnih pojedinačnih izjava o sukladnosti.

(43) Oznaka CE, koja označuje sukladnost proizvoda, vidljiva je posljedica cijelog postupka koji obuhvaća ocjenjivanje sukladnosti u širem smislu. Opća načela stavljanja oznake CE utvrđena su Uredbom (EZ) br. 765/2008 Europskog parlamenta i Vijeća[18]. Ovom Uredbom trebala bi se utvrditi pravila za stavljanje oznake CE na proizvode s digitalnim elementima. Oznaka CE trebala bi biti jedina oznaka koja jamči sukladnost proizvoda s digitalnim elementima sa zahtjevima ove Uredbe.

[18] Uredba (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i o stavljanju izvan snage Uredbe (EEZ) br. 339/93 (SL L 218, 13.8.2008., str. 30.).

(44) Kako bi se gospodarskim subjektima omogućilo da dokažu sukladnost s bitnim zahtjevima utvrđenima ovom Uredbom, a tijelima za nadzor tržišta da osiguraju da su proizvodi s digitalnim elementima koji su stavljeni na raspolaganje na tržištu sukladni s njima, potrebno je utvrditi postupke ocjenjivanja sukladnosti. Odlukom br. 768/2008/EZ Europskog parlamenta i Vijeća[19] utvrđeni su moduli za postupke ocjenjivanja sukladnosti razmjerno razini uključenog rizika i potrebnoj razini sigurnosti. Kako bi se postigla međusektorska usklađenost i izbjegle *ad hoc* varijante, postupci ocjenjivanja sukladnosti primjereni za provjeru sukladnosti proizvoda s digitalnim elementima s bitnim zahtjevima iz ove Uredbe temelje se na tim modulima. U postupcima ocjenjivanja sukladnosti trebalo bi ispitati i provjeriti zahtjeve u pogledu proizvoda i procesa koji se odnose cijeli životni ciklus proizvoda s digitalnim elementima, uključujući planiranje, projektiranje, razvoj ili proizvodnju, ispitivanje i održavanje proizvoda.

(45) Kao opće pravilo, ocjenjivanje sukladnosti proizvoda s digitalnim elementima trebao bi provoditi proizvođač na vlastitu odgovornost primjenom postupka koji se temelji na modulu A iz Odluke br. 768/2008/EZ. Proizvođač bi i dalje trebao imati mogućnost odabira strožeg postupka ocjenjivanja sukladnosti koji uključuje treću stranu. Ako je proizvod svrstan u rizične proizvode I. razreda, potrebno je dodatno jamstvo za dokazivanje sukladnosti s bitnim zahtjevima utvrđenima ovom Uredbom. Ako proizvođač želi provesti ocjenjivanje sukladnosti na vlastitu odgovornost (modul A), trebao bi primjenjivati usklađene norme, zajedničke specifikacije ili programe kibersigurnosne certifikacije na temelju Uredbe (EU) 2019/881 koje je potvrdila Komisija u provedbenom aktu. Ako proizvođač ne primjenjuje takve usklađene norme, zajedničke specifikacije ili programe kibersigurnosne certifikacije, trebao bi se podvrgnuti ocjenjivanju sukladnosti koje uključuje treću stranu. Uzimajući u obzir administrativno opterećenje proizvođača i to da kibersigurnost ima važnu ulogu u fazi projektiranja i razvoja materijalnih i nematerijalnih proizvoda s digitalnim elementima, postupci ocjenjivanja sukladnosti koji se temelje na modulima B+C ili modulu H iz Odluke br. 768/2008/EZ odabrani su kao najprikladniji za ocjenjivanje sukladnosti rizičnih proizvoda s digitalnim elementima na proporcionalan i učinkovit način. Proizvođač koji provodi ocjenjivanje sukladnosti kao treća strana može odabrati postupak koji najbolje odgovara njegovu procesu projektiranja i proizvodnje. S obzirom na još veći kibersigurnosni rizik povezan s uporabom proizvoda svrstanih u rizične proizvode II. razreda, ocjenjivanje sukladnosti uvijek bi trebalo uključivati treću stranu.

(46) Dok izrada materijalnih proizvoda s digitalnim elementima obično zahtijeva znatan trud proizvođača u fazama projektiranja, razvoja i proizvodnje, u izradi proizvoda s digitalnim elementima u obliku softvera najvažniji su projektiranje i razvoj, a faza proizvodnje ima manju ulogu. Međutim, mnogo puta softverske proizvode i dalje treba sastaviti, izraditi, upakirati, staviti na raspolaganje za preuzimanje ili kopirati na fizički medij prije stavljanja na tržište. Kad se za provjeru sukladnosti proizvoda s bitnim zahtjevima iz ove Uredbe u fazama projektiranja, razvoja i proizvodnje primjenjuju relevantni moduli ocjenjivanja sukladnosti, te bi se aktivnosti trebale smatrati proizvodnjom.

---

[19] Odluka br. 768/2008/EZ Europskog parlamenta i Vijeća od 9. srpnja 2008. o zajedničkom okviru za stavljanje na tržište proizvoda i o stavljanju izvan snage Odluke Vijeća 93/465/EEZ (SL L 218, 13.8.2008., str. 82.).

(47) Radi provedbe ocjenjivanja sukladnosti proizvoda s digitalnim elementima koje provodi treća strana nacionalna tijela koja provode prijavljivanje trebala bi Komisiji i drugim državama članicama prijaviti tijela za ocjenjivanje sukladnosti, pod uvjetom da ispunjavaju niz zahtjeva, ponajprije u pogledu neovisnosti, stručnosti i nepostojanja sukoba interesa.

(48) Kako bi se osigurala dosljedna razina kvalitete u ocjenjivanju sukladnosti proizvoda s digitalnim elementima, potrebno je utvrditi i zahtjeve za tijela koja provode prijavljivanje i druga tijela uključena u ocjenjivanje, prijavljivanje i praćenje prijavljenih tijela. Sustav utvrđen ovom Uredbom trebalo bi dopuniti akreditacijskim sustavom utvrđenim u Uredbi (EZ) br. 765/2008. Budući da je akreditacija bitno sredstvo za provjeru stručnosti tijela za ocjenjivanje sukladnosti, trebala bi se upotrebljavati i u svrhu prijavljivanja.

(49) Nacionalna javna tijela u Uniji trebala bi transparentnu akreditaciju propisanu Uredbom (EZ) br. 765/2008, kojom se osigurava potrebna razina povjerenja u certifikate o sukladnosti, smatrati prefereriranim sredstvom dokazivanja tehničke stručnosti tijela za ocjenjivanje sukladnosti. Međutim, nacionalna tijela mogu smatrati da raspolažu primjerenim sredstvima kojima samostalno mogu obaviti tu evaluaciju. U takvim slučajevima, kako bi se osigurala odgovarajuća razina vjerodostojnosti evaluacija koje provode druga nacionalna tijela, ona bi Komisiji i drugim državama članicama trebala dostaviti potrebnu dokumentaciju kojom potvrđuju da evaluirana tijela za ocjenjivanje sukladnosti ispunjavaju relevantne regulatorne zahtjeve.

(50) Tijela za ocjenjivanje sukladnosti često podugovaraju dio svojih poslova povezanih s ocjenjivanjem sukladnosti ili ih prenose na društvo kćer. Kako bi se osigurala propisana razina zaštite za proizvod s digitalnim elementima koji se stavlja na tržište, bitno je da podugovaratelji i društva kćeri koji ocjenjuju sukladnost ispunjavaju jednake zahtjeve kao prijavljena tijela u pogledu ocjenjivanja sukladnosti.

(51) Tijelo koje provodi prijavljivanje trebalo bi Komisiji i drugim državama članicama dostaviti prijavu tijela za ocjenjivanje sukladnosti putem informacijskog sustava prijavljenih i imenovanih tijela prema novom pristupu (NANDO). NANDO je elektronički alat za prijavljivanje koji je razvila i vodi Komisija u kojem se može pronaći popis svih prijavljenih tijela.

(52) Budući da prijavljena tijela mogu nuditi svoje usluge u cijeloj Uniji, primjereno je drugim državama članicama i Komisiji omogućiti da iznesu prigovore u pogledu pojedinog prijavljenog tijela. Stoga je važno utvrditi razdoblje u kojem se sve sumnje ili pitanja koja se odnose na stručnost tijela za ocjenjivanje sukladnosti mogu razjasniti prije nego što to tijelo počne raditi kao prijavljeno tijelo.

(53) U interesu tržišnog natjecanja ključno je da prijavljena tijela primjenjuju postupke ocjenjivanja sukladnosti bez nepotrebnog opterećivanja gospodarskih subjekata. Iz istog razloga i radi jednakog postupanja prema gospodarskim subjektima treba se pobrinuti da tehnička primjena postupaka ocjenjivanja sukladnosti bude dosljedna. Primjerena koordinacija i suradnja prijavljenih tijela trebali bi biti najbolji načini da se to postigne.

(54) Nadzor tržišta ključan je instrument za osiguravanje odgovarajuće i ujednačene primjene zakonodavstva Unije. Stoga je primjereno uspostaviti pravni okvir na temelju kojeg se nadzor tržišta može provoditi na odgovarajući način. Na proizvode s digitalnim elementima obuhvaćene ovom Uredbom primjenjuju se pravila o nadzoru

tržišta Unije i kontroli proizvoda koji ulaze na tržište Unije propisana Uredbom (EU) 2019/1020 Europskog parlamenta i Vijeća[20].

(55) U skladu s Uredbom (EU) 2019/1020 tijela za nadzor tržišta provode nadzor tržišta na državnom području određene države članice. Ova Uredba ne bi trebala onemogućiti države članice da odaberu nadležna tijela za obavljanje tih zadaća. Svaka država članica trebala bi odrediti jedno ili više tijela za nadzor tržišta na svojem državnom području. Države članice mogu kao tijelo za nadzor tržišta imenovati bilo koje postojeće ili novo tijelo, uključujući nacionalna nadležna tijela iz članka [članak X.] Direktive [Direktiva XXX/XXXX (NIS2)] ili imenovana nacionalna tijela za kibersigurnosnu certifikaciju iz članka 58. Uredbe (EU) 2019/881. Gospodarski subjekti trebali bi u potpunosti surađivati s tijelima za nadzor tržišta i drugim nadležnim tijelima. Svaka država članica trebala bi obavijestiti Komisiju i druge države članice o svojim tijelima za nadzor tržišta i područjima nadležnosti svakog od tih tijela te osigurati potrebne resurse i vještine za obavljanje nadzornih zadaća koje se odnose na ovu Uredbu. U skladu s člankom 10. stavcima 2. i 3. Uredbe (EU) 2019/1020 svaka država članica trebala bi imenovati jedinstveni ured za vezu koji bi trebao biti odgovoran, među ostalim, za zastupanje koordiniranog stajališta tijela za nadzor tržišta i pružanje pomoći u suradnji tijela za nadzor tržišta iz različitih država članica.

(56) Radi ujednačene primjene ove Uredbe, trebalo bi uspostaviti posebnu administrativnu skupinu za koordinaciju (skupina za ADCO) u skladu s člankom 30. stavkom 2. Uredbe (EU) 2019/1020. Ta skupina za ADCO trebala bi se sastojati od predstavnika imenovanih tijela za nadzor tržišta i, prema potrebi, predstavnika jedinstvenih ureda za vezu. Komisija bi trebala podupirati i poticati suradnju tijelâ za nadzor tržišta u okviru Mreže Unije za sukladnost proizvoda, koja je uspostavljena na temelju članka 29. Uredbe (EU) 2019/1020 i sastoji se od predstavnika svake države članice, uključujući predstavnika svakog jedinstvenog ureda za vezu iz članka 10. Uredbe (EU) 2019/1020 i, prema potrebi, nacionalnog stručnjaka, predsjednikâ skupina za ADCO i predstavnikâ Komisije. Komisija bi trebala sudjelovati na sastancima Mreže, njezinih podskupina i posebne skupine za ADCO. Ona bi trebala i pomagati toj skupini za ADCO preko izvršnog tajništva koje pruža tehničku i logističku potporu.

(57) Kako bi se poduzimale pravodobne, proporcionalne i učinkovite mjere povezane s proizvodima s digitalnim elementima koji predstavljaju znatan kibersigurnosni rizik, trebalo bi predvidjeti zaštitni postupak Unije u okviru kojeg bi se zainteresirane strane obavješćivalo o mjerama koje se namjeravaju poduzeti u vezi s takvim proizvodima. Time bi se ujedno tijelima za nadzor tržišta omogućilo da, u suradnji s relevantnim gospodarskim subjektima, prema potrebi djeluju u ranijoj fazi. Ako se države članice i Komisija slažu da je mjera koju je poduzela država članica opravdana, daljnje sudjelovanje Komisije ne bi trebalo biti potrebno, osim ako se nesukladnost može pripisati nedostacima usklađene norme.

(58) U određenim slučajevima proizvod s digitalnim elementima koji je sukladan s ovom Uredbom može ipak predstavljati znatan kibersigurnosni rizik, rizik za zdravlje ili sigurnost osoba, rizik za ispunjavanje obveza na temelju prava Unije ili nacionalnog prava za zaštitu temeljnih prava, rizik za dostupnost, autentičnost, cjelovitost ili

[20] Uredba (EU) 2019/1020 Europskog parlamenta i Vijeća od 20. lipnja 2019. o nadzoru tržišta i sukladnosti proizvoda i o izmjeni Direktive 2004/42/EZ i uredbi (EZ) br. 765/2008 i (EU) br. 305/2011 (SL L 169, 25.6.2019., str. 1.).

povjerljivost usluga koje pomoću elektroničkog informacijskog sustava nude ključni subjekti koji pripadaju vrsti iz [Priloga I. Direktivi XXX/XXXX (NIS2)] ili rizik za druge aspekte zaštite javnog interesa. Stoga je potrebno uspostaviti pravila za ublažavanje tih rizika. Tijela za nadzor tržišta zato bi trebala poduzeti mjere kojima će od gospodarskog subjekta zahtijevati da se pobrine da proizvod više ne predstavlja taj rizik ili da ga opozove ili povuče, ovisno o riziku. Čim tijelo za nadzor tržišta ograniči ili zabrani slobodno kretanje proizvoda na takav način, država članica trebala bi bez odgode obavijestiti Komisiju i druge države članice o privremenim mjerama te pritom obrazložiti tu odluku. Ako tijelo za nadzor tržišta donese takve mjere za proizvode koji predstavljaju rizik, Komisija bi se trebala bez odgode savjetovati s državama članicama i relevantnim gospodarskim subjektima te evaluirati nacionalnu mjeru. Na temelju rezultata te evaluacije Komisija bi trebala odlučiti je li nacionalna mjera opravdana. Komisija bi svoju odluku trebala dostaviti svim državama članicama te o njoj odmah obavijestiti sve države članice i relevantne gospodarske subjekte. Ako se mjera smatra opravdanom, Komisija može razmotriti i donošenje prijedloga za reviziju odgovarajućeg zakonodavstva Unije.

(59) Za proizvode s digitalnim elementima koji predstavljaju znatan kibersigurnosni rizik i ako postoji razlog za sumnju da nisu sukladni s ovom Uredbom ili za proizvode koji su sukladni s ovom Uredbom, ali predstavljaju druge važne rizike, kao što su rizici za zdravlje ili sigurnost osoba, temeljna prava ili pružanje usluga ključnih subjekata koji pripadaju vrsti iz [Priloga I. Direktivi XXX/XXXX (NIS2)], Komisija može zatražiti od ENISA-e da provede evaluaciju. Na temelju te evaluacije Komisija može provedbenim aktima donijeti korektivne ili restriktivne mjere na razini Unije, uključujući nalaganje povlačenja s tržišta ili opoziva odgovarajućih proizvoda u razumnom roku, razmjerno vrsti rizika. Komisija može pribjeći takvoj intervenciji samo u iznimnim okolnostima u kojima je brza intervencija opravdana radi očuvanja dobrog funkcioniranja unutarnjeg tržišta i samo ako nadzorna tijela nisu poduzela djelotvorne mjere za ispravljanje situacije. Takve iznimne okolnosti mogu biti izvanredne situacije kao, na primjer, kad nesukladan proizvod koji je proizvođač stavio na raspolaganje u velikim količinama u nekoliko država članica, koji usto u ključnim sektorima rabe subjekti obuhvaćeni područjem primjene [Direktive XXX/XXXX (NIS2)], sadržava poznate ranjivosti koje zlonamjerni akteri iskorištavaju i za koje proizvođač ne pruža zakrpe. Komisija može intervenirati u takvim izvanrednim situacijama samo dok traju iznimne okolnosti i ako nesukladnost s ovom Uredbom ili važni rizici koje proizvod predstavlja potraju.

(60) Ako postoje naznake nesukladnosti s ovom Uredbom u nekoliko država članica, tijela za nadzor tržišta trebala bi moći provoditi zajedničke aktivnosti s drugim tijelima radi provjere sukladnosti i utvrđivanja kibersigurnosnih rizika proizvoda s digitalnim elementima.

(61) Istodobne koordinirane kontrolne mjere („opsežne provjere”) posebne su provedbene mjere tijela za nadzor tržišta kojima se može dodatno povećati sigurnost proizvoda. Opsežne provjere trebalo bi ponajprije provoditi kad tržišni trendovi, pritužbe potrošača ili druge naznake upućuju na to da određene kategorije proizvoda često predstavljaju kibersigurnosne rizike. ENISA bi tijelima za nadzor tržišta trebala dostavljati prijedloge kategorija proizvoda za koje bi se mogle organizirati opsežne provjere, na temelju, među ostalim, obavijesti o ranjivostima proizvoda i incidentima koje primi.

(62) Kako bi se regulatorni okvir mogao prema potrebi prilagođavati, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. Ugovora radi ažuriranja

popisa rizičnih proizvoda iz Priloga III. i određivanja definicija tih kategorija proizvoda. Ovlast za donošenje akata u skladu s tim člankom Komisiji bi trebalo delegirati radi utvrđivanja proizvoda s digitalnim elementima koji su obuhvaćeni drugim pravilima Unije kojima se postiže jednaka razina zaštite kao i ovom Uredbom, pri čemu, prema potrebi, treba odrediti je li potrebno ograničenje ili izuzeće iz područja primjene ove Uredbe te opseg tog ograničenja. Ovlast za donošenje akata u skladu s tim člankom Komisiji bi trebalo delegirati i u pogledu potencijalnog uvođenje obveze certifikacije određenih visokorizičnih proizvoda s digitalnim elementima na temelju kriterija rizičnosti utvrđenih u ovoj Uredbi te radi određivanja minimalnog sadržaja EU izjave o sukladnosti i dodatnih elemenata koje treba uključiti u tehničku dokumentaciju. Posebno je važno da Komisija tijekom svojeg pripremnog rada provede odgovarajuća savjetovanja, uključujući ona na razini stručnjaka, te da se ta savjetovanja provedu u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016[21]. Osobito, s ciljem osiguravanja ravnopravnog sudjelovanja u pripremi delegiranih akata, Europski parlament i Vijeće primaju sve dokumente istodobno kada i stručnjaci iz država članica te njihovi stručnjaci sustavno imaju pristup sastancima stručnih skupina Komisije koji se odnose na pripremu delegiranih akata.

(63) Radi osiguranja jedinstvenih uvjeta za provedbu ove Uredbe, Komisiji bi trebalo dodijeliti provedbene ovlasti za: određivanje formata i elemenata popisa softverskog materijala, pobliže određivanje vrste informacija, formata i postupka podnošenja obavijesti o iskorištenim ranjivostima i incidentima koje proizvođači dostavljaju ENISA-i, određivanje europskih programa kibersigurnosne certifikacije donesenih na temelju Uredbe (EU) 2019/881 koji se mogu primijeniti za dokazivanje sukladnosti s bitnim zahtjevima ili njihovim dijelovima iz Priloga I. ovoj Uredbi, donošenje zajedničkih specifikacija povezanih s bitnim zahtjevima iz Priloga I., utvrđivanje tehničkih specifikacija za piktograme i sve druge oznake povezane sa sigurnošću proizvoda s digitalnim elementima te mehanizama za promicanje njihove uporabe te odlučivanje o korektivnim ili restriktivnim mjerama na razini Unije u iznimnim okolnostima koje opravdavaju brzu intervenciju radi očuvanja dobrog funkcioniranja unutarnjeg tržišta. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća[22].

(64) Kako bi se osigurala pouzdana i konstruktivna suradnja tijela za nadzor tržišta na razini Unije i na nacionalnoj razini, sve strane uključene u primjenu ove Uredbe trebale bi poštovati povjerljivost informacija i podataka prikupljenih pri obavljanju svojih zadaća.

(65) Kako bi se osiguralo učinkovito izvršavanje obveza utvrđenih u ovoj Uredbi, svako tijelo za nadzor tržišta trebalo bi imati ovlast izricati ili zahtijevati izricanje upravnih novčanih kazni. Stoga bi u nacionalnim propisima trebalo utvrditi najviše upravne novčane kazne za nepoštovanje obveza utvrđenih ovom Uredbom. Pri odlučivanju o iznosu upravne novčane kazne u svakom pojedinačnom slučaju u obzir bi trebalo uzeti sve relevantne okolnosti konkretne situacije, a minimalno one izričito utvrđene ovom Uredbom, među ostalim i to jesu li druga tijela za nadzor tržišta već izrekla upravne novčane kazne istom subjektu za slične povrede. Takve okolnosti mogu biti otegotne,

[21] SL L 123, 12.5.2016., str. 1.

[22] Uredba (EU) br. 182/2011 Europskog parlamenta i Vijeća od 16. veljače 2011. o utvrđivanju pravila i općih načela u vezi s mehanizmima nadzora država članica nad izvršavanjem provedbenih ovlasti Komisije (SL L 55, 28.2.2011., str. 13.).

u situacijama kad isti subjekt nastavlja s povredom na državnim područjima drugih država članica osim one u kojoj mu je upravna novčana kazna već izrečena, ili olakotne, jer bi trebale osigurati da druga tijela za nadzor tržišta pri razmatranju bilo koje druge upravne novčane kazne za isti gospodarski subjekt ili istu vrstu povrede uzmu u obzir, zajedno s drugim relevantnim posebnim okolnostima, vrstu i visinu sankcije izrečene u drugim državama članicama. U svim takvim slučajevima kumulativna upravna novčana kazna koju bi tijela za nadzor tržišta nekoliko država članica mogla izreći istom gospodarskom subjektu za istu vrstu povrede trebala bi biti u skladu s načelom proporcionalnosti.

(66) Ako su upravne novčane kazne izrečene osobama koje nisu poduzeće, pri razmatranju odgovarajućeg iznosa novčane kazne nadležno tijelo trebalo bi uzeti u obzir opću razinu dohotka u državi članici te ekonomsko stanje osobe. Države članice trebale bi utvrditi i trebaju li i do koje mjere primjenjivati upravne novčane kazne za državna tijela.

(67) U svojim odnosima s trećim zemljama EU nastoji promicati međunarodnu trgovinu reguliranim proizvodima. Za olakšavanje trgovine može se primijeniti širok raspon mjera, uključujući nekoliko pravnih instrumenata kao što su bilateralni (međuvladini) sporazumi o uzajamnom priznavanju ocjenjivanja sukladnosti i označivanja reguliranih proizvoda. Sporazumi o uzajamnom priznavanju sklapaju se između Unije i trećih zemalja koje su na usporedivoj razini tehničkog razvoja i imaju kompatibilan pristup ocjenjivanju sukladnosti. Ti se sporazumi temelje na uzajamnom priznavanju potvrda, oznaka sukladnosti i rezultata ispitivanja koje izdaju tijela za ocjenjivanje sukladnosti bilo koje stranke u skladu sa zakonodavstvom druge stranke. Trenutačno ti sporazumi postoje s nekoliko zemalja. Sklapaju se u više raznih sektora koji se mogu razlikovati od države do države. Kako bi se dodatno olakšala trgovina i s obzirom na to da su lanci opskrbe proizvoda s digitalnim elementima globalni, sporazumi o uzajamnom priznavanju ocjenjivanja sukladnosti mogu se sklopiti za proizvode koje Unija regulira ovom Uredbom u skladu s člankom 218. UFEU-a. Važna je i suradnja s partnerskim zemljama radi povećanja kiberotpornosti na globalnoj razini jer će to dugoročno doprinijeti učvršćivanju okvira kibersigurnosti unutar i izvan EU-a.

(68) Komisija bi periodično trebala preispitivati ovu Uredbu, uz savjetovanje sa zainteresiranim stranama, posebno radi utvrđivanja potrebe za njezinom izmjenom u svjetlu promjene društvenih, političkih, tehnoloških i tržišnih uvjeta.

(69) Gospodarskim subjektima trebalo bi dati dovoljno vremena za prilagodbu zahtjevima iz ove Uredbe. Ova bi se Uredba trebala početi primjenjivati [24 mjeseca] od njezina stupanja na snagu, uz iznimku obveza izvješćivanja povezanih s iskorištenim ranjivostima i incidentima, koje bi se trebale početi primjenjivati [12 mjeseci] od stupanja na snagu ove Uredbe.

(70) S obzirom na to da cilj ove Uredbe ne mogu dostatno ostvariti države članice, nego se zbog učinaka djelovanja on na bolji način može ostvariti na razini Unije, Unija može donijeti mjere u skladu s načelom supsidijarnosti utvrđenim u članku 5. Ugovora o Europskoj uniji. U skladu s načelom proporcionalnosti utvrđenim u tom članku ova Uredba ne prelazi ono što je potrebno za ostvarivanje tog cilja.

(71) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća[23] te je on dao mišljenje […],

DONIJELI SU OVU UREDBU:

POGLAVLJE I.

OPĆE ODREDBE

Članak 1.

Predmet

Ovom se Uredbom utvrđuju:

(a) pravila za stavljanje na tržište proizvoda s digitalnim elementima kako bi se osigurala kibersigurnost takvih proizvoda;

(b) bitni zahtjevi za projektiranje, razvoj i proizvodnju proizvoda s digitalnim elementima te obveze gospodarskih subjekata u pogledu tih proizvoda s obzirom na kibersigurnost;

(c) bitni zahtjevi za postupke upravljanja ranjivostima koje su proizvođači uspostavili kako bi zajamčili kibersigurnost proizvoda s digitalnim elementima tijekom cijelog životnog ciklusa i obveze gospodarskih subjekata u pogledu tih postupaka;

(d) pravila o nadzoru tržišta i provedbi tih pravila i zahtjeva.

Članak 2.

Područje primjene

1. Ova se Uredba primjenjuje na proizvode s digitalnim elementima čija namjena ili razumno predvidljiva uporaba uključuje izravnu ili neizravnu logičku ili fizičku podatkovnu vezu s uređajem ili mrežom.

2. Ova se Uredba ne primjenjuje na proizvode s digitalnim elementima na koje se primjenjuju sljedeći akti Unije:

   (a) Uredba (EU) 2017/745;

   (b) Uredba (EU) 2017/746;

   (c) Uredba (EU) 2019/2144.

3. Ova se Uredba ne primjenjuje na proizvode s digitalnim elementima koji su certificirani u skladu s Uredbom (EU) 2018/1139.

4. Kad je riječ o proizvodima s digitalnim elementima obuhvaćenima drugim pravilima Unije kojima su utvrđeni zahtjevi koji se odnose na sve ili neke rizike obuhvaćene

[23] Uredba (EU) 2018/1725 Europskog parlamenta i Vijeća od 23. listopada 2018. o zaštiti pojedinaca u vezi s obradom osobnih podataka u institucijama, tijelima, uredima i agencijama Unije i o slobodnom kretanju takvih podataka te o stavljanju izvan snage Uredbe (EZ) br. 45/2001 i Odluke br. 1247/2002/EZ (SL L 295, 21.11.2018., str. 39.).

bitnim zahtjevima iz Priloga I., primjena ove Uredbe može se ograničiti ili se ona ne mora primjenjivati na njih:

(a) ako je takvo ograničenje ili neprimjena u skladu s cjelokupnim regulatornim okvirom koji se primjenjuje na te proizvode; i

(b) ako se sektorskim pravilima postiže ista razina zaštite kao ona propisana ovom Uredbom.

Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 50. radi izmjene ove Uredbe kojima se utvrđuje potreba za takvim ograničenjem ili neprimjenom, proizvode ili pravila na koje se odnosi i, prema potrebi, opseg ograničenja.

5. Ova se Uredba ne primjenjuje na proizvode s digitalnim elementima koji su razvijeni isključivo za potrebe nacionalne sigurnosti ili u vojne svrhe niti na proizvode koji su posebno namijenjeni za obradu klasificiranih podataka.

Članak 3.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

(1) „proizvod s digitalnim elementima” znači svaki softverski ili hardverski proizvod i njegova rješenja za daljinsku obradu podataka, uključujući softverske ili hardverske komponente koje se zasebno stavljaju na tržište;

(2) „daljinska obrada podataka” znači svaka obrada podataka na daljinu čiji je softver projektirao i razvio proizvođač ili za koju je proizvođač odgovoran, a bez koje proizvod s digitalnim elementima ne bi mogao obavljati neku od svojih funkcija;

(3) „rizični proizvod s digitalnim elementima” znači proizvod s digitalnim elementima koji predstavlja kibersigurnosni rizik u skladu s kriterijima utvrđenima u članku 6. stavku 2., a čija je osnovna funkcionalnost utvrđena u Prilogu III.;

(4) „visokorizični proizvod s digitalnim elementima” znači proizvod s digitalnim elementima koji predstavlja kibersigurnosni rizik u skladu s kriterijima utvrđenima u članku 6. stavku 5.;

(5) „operativna tehnologija” znači digitalni sustavi ili uređaji koji se mogu programirati i koji su u interakciji s fizičkim okruženjem ili upravljaju uređajima koji su u interakciji s fizičkim okruženjem;

(6) „softver” znači dio elektroničkog informacijskog sustava koji se sastoji od računalnog koda;

(7) „hardver” znači fizički elektronički informacijski sustav ili njegovi dijelovi sa sposobnošću obrađivanja, pohranjivanja ili prenošenja digitalnih podataka;

(8) „komponenta” znači softver ili hardver namijenjen za integraciju u elektronički informacijski sustav;

(9) „elektronički informacijski sustav” znači svaki sustav, uključujući električnu ili elektroničku opremu, koji može obrađivati, pohranjivati ili prenositi digitalne podatke;

(10) „logička veza” znači virtualni prikaz podatkovne veze izvedene u obliku softverskog sučelja;

(11) „fizička veza” znači svaka veza između elektroničkih informacijskih sustava ili komponenata izvedena fizičkim sredstvima, uključujući električna ili mehanička sučelja, žice ili radijske valove;

(12) „neizravna veza” znači veza s uređajem ili mrežom koja nije izvedena izravno nego kao dio većeg sustava koji se može izravno povezati s takvim uređajem ili mrežom;

(13) „ovlast” znači pravo pristupa koje se dodjeljuje određenim korisnicima ili programima radi izvođenja operacija važnih za sigurnost unutar elektroničkog informacijskog sustava;

(14) „podignuta ovlast” znači pravo pristupa koje se dodjeljuje određenim korisnicima ili programima za izvođenje proširenog skupa operacija važnih za sigurnost unutar elektroničkog informacijskog sustava koje bi, ako se krivo uporabi ili bude kompromitirano, moglo omogućiti zlonamjernom akteru da dobije širi pristup resursima sustava ili organizacije;

(15) „krajnja točka” znači svaki uređaj koji je priključen na mrežu i služi kao ulazna točka u tu mrežu;

(16) „mrežni ili računalni resursi” znači podatkovna, hardverska ili softverska funkcionalnost koja je dostupna lokalno, kroz mrežu ili s drugog povezanog uređaja;

(17) „gospodarski subjekt” znači proizvođač, ovlašteni zastupnik, uvoznik, distributer ili svaka druga fizička ili pravna osoba koja podliježe obvezama utvrđenima ovom Uredbom;

(18) „proizvođač” znači svaka fizička ili pravna osoba koja razvija ili proizvodi proizvode s digitalnim elementima ili pod svojim imenom ili žigom stavlja na tržište za nju projektirane, razvijene ili proizvedene proizvode s digitalnim elementima, uz naplatu ili besplatno;

(19) „ovlašteni zastupnik” znači svaka fizička ili pravna osoba s poslovnim nastanom u Uniji koju je proizvođač napismeno ovlastio da u njegovo ime nastupa u vezi s određenim zadaćama;

(20) „uvoznik” znači svaka fizička ili pravna osoba s poslovnim nastanom u Uniji koja stavlja na tržište proizvod s digitalnim elementima s imenom ili žigom fizičke ili pravne osobe s poslovnim nastanom izvan Unije;

(21) „distributer” znači svaka fizička ili pravna osoba u opskrbnom lancu koja nije proizvođač ni uvoznik, a koja stavlja proizvod s digitalnim elementima na tržište Unije, pri čemu ne mijenja njegova svojstva;

(22) „stavljanje na tržište” znači prvo stavljanje proizvoda s digitalnim elementima na raspolaganje na tržištu Unije;

(23) „stavljanje na raspolaganje na tržištu” znači svaka isporuka proizvoda s digitalnim elementima za distribuciju ili uporabu na tržištu Unije u okviru trgovačke djelatnosti uz naplatu ili besplatno;

(24) „namjena” znači uporaba za koju je proizvođač namijenio proizvod s digitalnim elementima, uključujući specifični kontekst i uvjete uporabe, kako je određena u informacijama koje je proizvođač naveo u uputama za uporabu, promotivnim ili prodajnim materijalima i izjavama te u tehničkoj dokumentaciji;

(25) „razumno predvidljiva uporaba” znači uporaba koja nije nužno namjena koju je proizvođač naveo u uputama za uporabu, promotivnim ili prodajnim materijalima,

izjavama i tehničkoj dokumentaciji, ali do koje vjerojatno može doći iz razumno predvidljivog ljudskog ponašanja, tehničkih operacija ili interakcija;

(26) „razumno predvidljiva kriva uporaba” znači uporaba proizvoda s digitalnim elementima na način koji nije u skladu s njegovom namjenom, ali koja može biti posljedica razumno predvidljivog čovjekova ponašanja ili interakcije s drugim sustavima;

(27) „tijelo koje provodi prijavljivanje” znači nacionalno tijelo odgovorno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje, imenovanje, obavješćivanje i praćenje tijela za ocjenjivanje sukladnosti;

(28) „ocjenjivanje sukladnosti” znači postupak kojim se provjerava jesu li ispunjeni bitni zahtjevi iz Priloga I.;

(29) „tijelo za ocjenjivanje sukladnosti” znači tijelo definirano u članku 2. točki 13. Uredbe (EU) br. 765/2008;

(30) „prijavljeno tijelo” znači tijelo za ocjenjivanje sukladnosti imenovano u skladu s člankom 33. ove Uredbe i drugim relevantnim zakonodavstvom Unije o usklađivanju;

(31) „bitna izmjena” znači promjena proizvoda s digitalnim elementima nakon njegova stavljanja na tržište koja utječe na sukladnost proizvoda s digitalnim elementima s bitnim zahtjevima iz odjeljka 1. Priloga I. ove Uredbe ili koja prouzroči promjenu namjene prema kojoj je proizvod s digitalnim elementima bio ocijenjen;

(32) „oznaka CE” znači oznaka kojom proizvođač označuje da su proizvod s digitalnim elementima i procesi koje je proizvođač uspostavio sukladni s bitnim zahtjevima iz Priloga I. i drugog primjenjivog zakonodavstva Unije o usklađivanju uvjeta za stavljanje proizvoda na tržište („zakonodavstvo Unije o usklađivanju”) kojim se propisuje označivanje tom oznakom;

(33) „tijelo za nadzor tržišta” znači tijelo kako je definirano u članku 3. točki 4. Uredbe (EU) 2019/1020;

(34) „usklađena norma” znači usklađena norma kako je definirana u članku 2. stavku 1. točki (c) Uredbe (EU) br. 1025/2012.

(35) „kibersigurnosni rizik” znači rizik kako je definiran u članku [članku X.] Direktive [Direktiva XXX/XXXX (NIS2)];

(36) „znatan kibersigurnosni rizik” znači kibersigurnosni rizik za koji se na temelju njegovih tehničkih karakteristika može pretpostaviti da ima veliku vjerojatnost izazivanja incidenta koji može prouzročiti teške štetne posljedice, među ostalim znatan materijalni ili nematerijalni gubitak ili poremećaj;

(37) „popis softverskog materijala” znači službena evidencija u kojoj su navedene pojedinosti i odnosi u lancu opskrbe komponenata koje se nalaze u softverskim elementima proizvoda s digitalnim elementima;

(38) „ranjivost” znači ranjivost kako je definirana u članku [članku X.] Direktive [Direktiva XXX/XXXX (NIS2)];

(39) „iskorištena ranjivost” znači ranjivost za koju postoje pouzdani dokazi da je kroz nju neki akter ili sustav izvršio zlonamjerni kod bez dopuštenja vlasnika sustava;

(40) „osobni podaci” znači podaci kako su definirani u članku 4. stavku 1. Uredbe (EU) 2016/679.

Članak 4.

Slobodno kretanje

1. Države članice ne sprečavaju, kad je riječ o pitanjima obuhvaćenima ovom Uredbom, stavljanje na raspolaganje na tržištu proizvoda s digitalnim elementima koji su u skladu s ovom Uredbom.

2. Države članice ne sprečavaju izlaganje ni uporabu proizvoda s digitalnim elementima koji nije u skladu s ovom Uredbom na sajmovima, izložbama i predstavljanjima ili sličnim događanjima.

3. Države članice ne sprečavaju stavljanje na raspolaganje nedovršenog softvera koji nije u skladu s ovom Uredbom ako se takav softver stavlja na raspolaganje samo u ograničenom razdoblju potrebnom u svrhu ispitivanja i ako postoji vidljiv znak koji jasno upućuje na to da taj softver nije u skladu s ovom Uredbom te da neće biti na raspolaganju na tržištu u druge svrhe osim u svrhu ispitivanja.

Članak 5.

Zahtjevi za proizvode s digitalnim elementima

Proizvodi s digitalnim elementima stavljaju se na raspolaganje na tržištu samo ako:

(1) ispunjavaju bitne zahtjeve iz odjeljka 1. Priloga I. kad su ispravno instalirani i održavani, kad se upotrebljavaju u skladu s namjenom ili u uvjetima koji se mogu razumno predvidjeti te kad su, prema potrebi, ažurirani; i

(2) postupci koje je uspostavio proizvođač ispunjavaju bitne zahtjeve utvrđene u odjeljku 2. Priloga I.

Članak 6.

Rizični proizvodi s digitalnim elementima

1. Proizvodi s digitalnim elementima koji pripadaju u jednu od kategorija navedenih u Prilogu III. smatraju se rizičnim proizvodima s digitalnim elementima. Smatra se da pojedina kategorija iz Priloga III. ovoj Uredbi obuhvaća proizvode čija osnovna funkcionalnost pripada u tu kategoriju. Kategorije rizičnih proizvoda s digitalnim elementima razvrstane su u I. i II. razred kako je utvrđeno u Prilogu III. prema razini kibersigurnosnog rizika povezanog s tim proizvodima.

2. Komisija je ovlaštena donositi delegirane akte u skladu s člankom 50. radi izmjene Priloga III. uvrštavanjem nove kategorije u popis kategorija rizičnih proizvoda s digitalnim elementima ili uklanjanjem postojeće kategorije s tog popisa. Komisija pri procjeni potrebe za izmjenom popisa iz Priloga III. uzima u obzir razinu kibersigurnosnog rizika povezanog s kategorijom proizvoda s digitalnim elementima. Pri određivanju razine kibersigurnosnog rizika u obzir se uzima najmanje jedan od sljedećih kriterija:

   (a) funkcionalnost proizvoda s digitalnim elementima povezana s kibersigurnošću i ima li proizvod s digitalnim elementima barem jednu od sljedećih karakteristika:

      (i) projektiran je za rad s podignutom ovlasti ili za upravljanje ovlastima;

      (ii) ima izravan ili povlašten pristup mrežnim ili računalnim resursima;

(iii) projektiran je za kontrolu pristupa podacima ili operativnoj tehnologiji;

(iv) obavlja funkciju koja je ključna za povjerenje, što se posebice odnosi na sigurnosne funkcije kao što su kontrola mreže, sigurnost krajnje točke i zaštita mreže;

(b) namjena za rad u osjetljivim okruženjima, među ostalim u industrijskim okruženjima, ili za ključne subjekte koji pripadaju vrsti navedenoj u Prilogu [Prilog I.] Direktivi [Direktiva XXX/XXXX (NIS2)];

(c) namjena za obavljanje rizičnih ili osjetljivih funkcija, kao što je obrada osobnih podataka;

(d) potencijalni razmjeri štetnih posljedica, osobito u smislu intenziteta i mogućnosti da zahvati mnogo osoba;

(e) stupanj u kojem je uporaba proizvoda s digitalnim elementima već prouzročila materijalni ili nematerijalni gubitak ili poremećaj ili u kojem izaziva znatnu zabrinutost zbog mogućih štetnih posljedica.

3. Komisija je ovlaštena donijeti delegirani akt u skladu s člankom 50. radi dopune ove Uredbe utvrđivanjem definicija kategorija proizvoda I. i II. razreda kako su utvrđeni u Prilogu III. Delegirani akt donosi se [u roku od 12 mjeseci od stupanja na snagu ove Uredbe].

4. Rizični proizvodi s digitalnim elementima podliježu postupcima ocjenjivanja sukladnosti iz članka 24. stavaka 2. i 3.

5. Komisija je ovlaštena donositi delegirane akte u skladu s člankom 50. radi dopune ove Uredbe određivanjem kategorija visokorizičnih proizvoda s digitalnim elementima za koje su proizvođači dužni ishoditi europski kibersigurnosni certifikat u okviru europskog programa kibersigurnosne certifikacije na temelju Uredbe (EU) 2019/881 kako bi dokazali sukladnost s bitnim zahtjevima iz Priloga I. ili njihovim dijelovima. Pri određivanju takvih kategorija visokorizičnih proizvoda s digitalnim elementima Komisija uzima u obzir razinu kibersigurnosnog rizika povezanog s kategorijom proizvoda s digitalnim elementima prema jednom ili više kriterija navedenih u stavku 2. te na temelju procjene:

(a) je li to kategorija proizvoda koju koriste ili o kojoj ovise ključni subjekti koji pripadaju vrsti iz Priloga [Prilog I.] Direktivi [Direktiva XXX/XXXX (NIS2)] ili koja bi u budućnosti mogla biti važna za aktivnosti tih subjekata; ili

(b) je li ta kategorija proizvoda relevantna za otpornost cjelokupnog lanca opskrbe proizvoda s digitalnim elementima na remetilačke događaje.

Članak 7.

Opća sigurnost proizvoda

Odstupajući od članka 2. stavka 1. trećeg podstavka točke (b) Uredbe [Uredba o općoj sigurnosti proizvoda], ako proizvodi s digitalnim elementima ne podliježu posebnim zahtjevima utvrđenima u drugom zakonodavstvu Unije o usklađivanju u smislu [članka 3. točke 25. Uredbe o općoj sigurnosti proizvoda], u pogledu sigurnosnih rizika koji nisu obuhvaćeni ovom Uredbom na njih se primjenjuju poglavlje III. odjeljak 1., poglavlja V. i VII. i poglavlja od IX. do XI. Uredbe [Uredba o općoj sigurnosti proizvoda].

Članak 8.

Visokorizični UI sustavi

1. Proizvodi s digitalnim elementima koji su klasificirani u visokorizične UI sustave u skladu s člankom [članak 6.] Uredbe [Uredba o umjetnoj inteligenciji], obuhvaćeni područjem primjene ove Uredbe i ispunjavaju bitne zahtjeve iz odjeljka 1. Priloga I. ovoj Uredbi, pod uvjetom da su postupci koje je proizvođač uspostavio sukladni s bitnim zahtjevima iz odjeljka 2. Priloga I., smatraju se sukladnima sa zahtjevima koji se odnose na kibersigurnost iz članka [članak 15.] Uredbe [Uredba o umjetnoj inteligenciji], ne dovodeći u pitanje druge zahtjeve koji se odnose na točnost i robusnost iz tog članka i u mjeri u kojoj je postizanje razine zaštite koja se traži tim zahtjevima dokazano EU izjavom o sukladnosti izdanom na temelju ove Uredbe.

2. Za proizvode i kibersigurnosne zahtjeve iz stavka 1. primjenjuje se odgovarajući postupak ocjenjivanja sukladnosti u skladu s člankom [članak 43.] Uredbe [Uredba o umjetnoj inteligenciji]. Za potrebe tog ocjenjivanja prijavljena tijela koja imaju pravo kontrolirati sukladnost visokorizičnih UI sustava na temelju Uredbe [Uredba o umjetnoj inteligenciji] imaju pravo kontrolirati i sukladnost visokorizičnih UI sustava obuhvaćenih područjem primjene ove Uredbe sa zahtjevima iz Priloga I. ovoj Uredbi, pod uvjetom da je u kontekstu postupka prijavljivanja prema Uredbi [Uredba o umjetnoj inteligenciji] ocijenjeno ispunjavaju li ta prijavljena tijela zahtjeve iz članka 29. ove Uredbe.

3. Odstupajući od stavka 2., rizični proizvodi s digitalnim elementima navedeni u Prilogu III. ovoj Uredbi za koje se primjenjuju postupci ocjenjivanja sukladnosti iz članka 24. stavka 2. točaka (a) i (b) i članka 24. stavka 3. točaka (a) i (b) prema ovoj Uredbi te su klasificirani u visokorizične UI sustave u skladu s člankom [članak 6.] Uredbe [Uredba o umjetnoj inteligenciji] i podliježu postupku ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga [Prilog VI.] Uredbi [Uredba o umjetnoj inteligenciji] podliježu postupcima ocjenjivanja sukladnosti prema ovoj Uredbi u mjeri u kojoj su na njih odnose bitni zahtjevi iz ove Uredbe.

Članak 9.

Strojarski proizvodi

Strojarski proizvodi obuhvaćeni područjem primjene Uredbe [Prijedlog uredbe o strojevima] koji su proizvodi s digitalnim elementima u smislu ove Uredbe i za koje je izdana EU izjava o sukladnosti na temelju ove Uredbe smatraju se sukladnima s bitnim zdravstvenim i sigurnosnim zahtjevima iz Priloga [Prilog III., odjeljci 1.1.9. i 1.2.1.] Uredbe [Prijedlog uredbe o strojevima] u pogledu zaštite od kvarenja te sigurnosti i pouzdanosti kontrolnih sustava i u mjeri u kojoj je postizanje razine zaštite koju treba ostvariti prema tim zahtjevima dokazano EU izjavom o sukladnosti izdanom na temelju ove Uredbe.

POGLAVLJE II.

OBVEZE GOSPODARSKIH SUBJEKATA

Članak 10.

Obveze proizvođačâ

1. Pri stavljanju proizvoda s digitalnim elementima na tržište proizvođači osiguravaju da je on projektiran, razvijen i proizveden u skladu s bitnim zahtjevima iz odjeljka 1. Priloga I.

2. U svrhu ispunjavanja obveze iz stavka 1. proizvođači ocjenjuju kibersigurnosne rizike povezane s proizvodom s digitalnim elementima te u fazama planiranja, projektiranja, razvoja, proizvodnje, isporuke i održavanja proizvoda s digitalnim elementima uzimaju u obzir rezultate tog ocjenjivanja radi smanjenja kibersigurnosnih rizika, sprečavanja sigurnosnih incidenata i smanjivanja posljedica takvih incidenata, među ostalim na zdravlje i sigurnost korisnika.

3. Pri stavljanju na tržište proizvoda s digitalnim elementima proizvođač u tehničku dokumentaciju uključuje procjenu kibersigurnosnog rizika kako je utvrđeno u članku 23. i Prilogu V. Za proizvode s digitalnim elementima iz članka 8. i članka 24. stavka 4. koji podliježu i drugim aktima Unije procjena kibersigurnosnog rizika može biti dio procjene rizika koja se zahtijeva tim aktima Unije. Ako određeni bitni zahtjevi nisu primjenjivi na proizvod s digitalnim elementima stavljen na tržište, proizvođač u tu dokumentaciju uključuje jasno obrazloženje.

4. U svrhu ispunjavanja obveze iz stavka 1. proizvođači koji u proizvode s digitalnim elementima ugrađuju komponente koje potječu od trećih strana moraju postupati s dužnom pažnjom. Oni osiguravaju da takve komponente ne ugrožavaju sigurnost proizvoda s digitalnim elementima.

5. Proizvođač mora sustavno dokumentirati, na način koji je razmjeran vrsti i kibersigurnosnim rizicima, relevantne kibersigurnosne aspekte u povezane s proizvodom s digitalnim elementima, uključujući ranjivosti za koje je doznao i sve relevantne informacije koje pružaju treće strane te, prema potrebi, ažurira procjenu rizika proizvoda.

6. Pri stavljanju na tržište proizvoda s digitalnim elementima i tijekom očekivanog životnog vijeka proizvoda ili tijekom razdoblja od pet godina nakon stavljanja proizvoda na tržište, ovisno o tome koje je razdoblje kraće, proizvođači osiguravaju da se s ranjivostima tog proizvoda upravlja djelotvorno i u skladu s bitnim zahtjevima iz odjeljka 2. Priloga I.

   Proizvođači moraju imati odgovarajuće politike i postupke, uključujući politike koordiniranog otkrivanja ranjivosti, iz odjeljka 2. točke 5. Priloga I. za obradu i otklanjanje potencijalnih ranjivosti proizvoda s digitalnim elementima koje je prijavio unutarnji ili vanjski izvor.

7. Tehničku dokumentaciju iz članka 23. proizvođači moraju sastaviti prije stavljanja na tržište proizvoda s digitalnim elementima.

   Oni provode ili daju provesti odabrane postupke ocjenjivanja sukladnosti iz članka 24.

   Ako je tim postupkom ocjenjivanja sukladnosti dokazana sukladnost proizvoda s digitalnim elementima s bitnim zahtjevima iz odjeljka 1. Priloga I. i sukladnost postupaka koje je proizvođač uspostavio s bitnim zahtjevima iz odjeljka 2. Priloga I., proizvođači sastavljaju EU izjavu o sukladnosti u skladu s člankom 20. i stavljaju na proizvod oznaku CE u skladu s člankom 22.

8. Proizvođači su dužni čuvati tehničku dokumentaciju i, prema potrebi, EU izjavu o sukladnosti kako bi bila na raspolaganju tijelima za nadzor tržišta deset godina nakon što je proizvod s digitalnim elementima stavljen na tržište.

9. Proizvođači osiguravaju uspostavu postupaka za očuvanje sukladnosti serijski proizvedenih proizvoda s digitalnim elementima. Proizvođač na primjeren način uzima u obzir promjene povezane s razvojem i proizvodnim procesom ili s projektiranjem ili karakteristikama proizvoda s digitalnim elementima te promjene usklađenih normi, europskih programa kibersigurnosne certifikacije ili zajedničkih specifikacija iz članka 19. na temelju kojih je izjavljena ili čijom je primjenom provjerena sukladnost proizvoda s digitalnim elementima.

10. Proizvođači osiguravaju da su uz proizvode s digitalnim elementima priložene informacije i upute iz Priloga II. u elektroničkom ili fizičkom obliku. Takve informacije i upute moraju biti na jeziku koji korisnici bez poteškoća razumiju. Moraju biti jasne, razumljive i čitljive. Moraju omogućiti sigurnu ugradnju, rad i uporabu proizvoda s digitalnim elementima.

11. Proizvođači su dužni EU izjavu o sukladnosti priložiti uz proizvod s digitalnim elementima ili u uputama i informacijama iz Priloga II. navesti internetsku adresu na kojoj se može pristupiti toj izjavi.

12. Nakon stavljanja na tržište i tijekom očekivanog vijeka trajanja proizvoda ili razdoblja od pet godina nakon stavljanja na tržište proizvoda s digitalnim elementima, ovisno o tome koje je razdoblje kraće, proizvođači koji znaju ili imaju razloga vjerovati da proizvod s digitalnim elementima ili postupci koje je proizvođač uspostavio nisu sukladni s bitnim zahtjevima iz Priloga I. odmah poduzimaju potrebne korektivne mjere da se ponovno uspostavi sukladnost tog proizvoda s digitalnim elementima ili postupaka proizvođača ili da se proizvod prema potrebi povuče ili opozove.

13. Na obrazložen zahtjev tijela za nadzor tržišta proizvođači tom tijelu dostavljaju, na jeziku koje to tijelo bez poteškoća razumije te u papirnatom ili elektroničkom obliku, sve informacije i dokumentaciju potrebne za dokazivanje sukladnosti proizvoda s digitalnim elementima i postupaka koje je proizvođač uspostavio s bitnim zahtjevima iz Priloga I. Na zahtjev tog tijela oni s njim surađuju u pogledu svake mjere koja je poduzeta kako bi se otklonili kibersigurnosni rizici proizvoda s digitalnim elementima koji su stavili na tržište.

14. Proizvođač koji ne može ispunjavati obveze utvrđene ovom Uredbom jer prestaje s radom o toj situaciji obavješćuje, prije nego što prestane s radom, nadležna tijela za nadzor tržišta te, na bilo koji raspoloživ način i u mjeri u kojoj je to moguće, korisnike predmetnih proizvoda s digitalnim elementima koji su stavljeni na tržište.

15. Komisija može provedbenim aktima odrediti format i elemente popisa softverskog materijala iz odjeljka 2. točke 1. Priloga I. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 51. stavka 2.

Članak 11.

Obveze proizvođačâ u pogledu izvješćivanja

1. Proizvođač mora obavijestiti ENISA-u o svakoj iskorištenoj ranjivosti proizvoda s digitalnim elementima bez nepotrebne odgode i u svakom slučaju u roku od 24 sata nakon što je doznao za nju. Ta obavijest uključuje pojedinosti o toj ranjivosti i, prema potrebi, sve poduzete korektivne mjere ili mjere ublažavanja. Nakon primitka te obavijesti ENISA je bez nepotrebne odgode, osim ako postoje opravdani razlozi povezani s kibersigurnosnim rizikom, prosljeđuje CSIRT-ovima imenovanima za potrebe koordiniranog otkrivanja ranjivosti u pogođenim državama članicama u

skladu s člankom [članak X.] Direktive [Direktiva XXX/XXXX (NIS2)] i o dojavljenoj ranjivosti obavješćuje tijelo za nadzor tržišta.

2. Proizvođač mora obavijestiti ENISA-u o svakom incidentu koji utječe na sigurnost proizvoda s digitalnim elementima bez nepotrebne odgode i u svakom slučaju u roku od 24 sata nakon što je doznao za njega. ENISA bez nepotrebne odgode, osim ako postoje opravdani razlozi povezani s kibersigurnosnim rizikom, te obavijesti prosljeđuje jedinstvenim kontaktnim točkama pogođenih država članica određenima u skladu s člankom [članak X.] Direktive [Direktiva XXX/XXXX (NIS2)] i o dojavljenim incidentima obavješćuje tijelo za nadzor tržišta. Prijava incidenta uključuje informacije o težini i posljedicama incidenta te, prema potrebi, informacije o tome sumnja li proizvođač na to da je incident prouzročen nezakonitim ili zlonamjernim radnjama ili smatra li da ima prekogranične posljedice.

3. ENISA dostavlja Europskoj mreži organizacija za vezu za kiberkrize (EU-CyCLONe), uspostavljenoj člankom [članak X.] Direktive [Direktiva XXX/XXXX (NIS2)], informacije prijavljene u skladu sa stavcima 1. i 2. ako su takve informacije važne za koordinirano upravljanje velikim kibersigurnosnim incidentima i krizama na operativnoj razini.

4. Proizvođač mora obavijestiti korisnike proizvoda s digitalnim elementima o incidentu i, prema potrebi, o korektivnim mjerama koje mogu poduzeti za ublažavanje posljedica incidenta bez nepotrebne odgode nakon što dozna za njega.

5. Komisija može provedbenim aktima pobliže odrediti vrstu informacija te format i postupak dostavljanja obavijesti u skladu sa stavcima 1. i 2. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 51. stavka 2.

6. Na temelju obavijesti zaprimljenih u skladu sa stavcima 1. i 2. ENISA izrađuje dvogodišnje tehničko izvješće o novim trendovima u području kibersigurnosnih rizika proizvoda s digitalnim elementima i dostavlja ga skupini za suradnju iz članka [članak X.] Direktive [Direktiva XXX/XXXX (NIS2)]. Prvo takvo izvješće mora se dostaviti u roku od 24 mjeseca nakon početka primjene obveza iz stavaka 1. i 2.

7. Ako u komponenti, uključujući komponentu otvorenog koda, koja je integrirana u proizvod s digitalnim elementima utvrde ranjivost, proizvođači o njoj obavješćuju osobu ili subjekt koji održava tu komponentu.

Članak 12.

Ovlašteni zastupnici

1. Proizvođač može pisanim ovlaštenjem imenovati ovlaštenog zastupnika.

2. Obveze utvrđene u članku 10. stavcima od 1. do 7. prvoj alineji i članku 10. stavku 9. nisu dio zadaća ovlaštenog zastupnika.

3. Ovlašteni zastupnik obavlja zadaće navedene u ovlaštenju koje mu je dao proizvođač. Tim se ovlaštenjem ovlaštenom zastupniku omogućuje da čini barem sljedeće:

   (a) da EU izjavu o sukladnosti iz članka 20. i tehničku dokumentaciju iz članka 23. čuva kako bi bila na raspolaganju tijelima za nadzor tržišta deset godina nakon što je proizvod s digitalnim elementima stavljen na tržište;

(b) da na obrazloženi zahtjev tijela za nadzor tržišta tom tijelu dostavi sve informacije i dokumentaciju potrebne za dokazivanje sukladnosti proizvoda s digitalnim elementima;

(c) da na zahtjev tijela za nadzor tržišta surađuje s njima u svakoj radnji poduzetoj radi otklanjanja rizika koje predstavlja proizvod s digitalnim elementima obuhvaćen ovlaštenjem ovlaštenog zastupnika.

Članak 13.

Obveze uvoznikâ

1. Uvoznici stavljaju na tržište samo proizvode s digitalnim elementima koji su sukladni s bitnim zahtjevima iz odjeljka 1. Priloga I. i ako su postupci koje je proizvođač uspostavio sukladni s bitnim zahtjevima iz odjeljka 2. Priloga I.

2. Prije stavljanja proizvoda s digitalnim elementima na tržište uvoznici su dužni provjeriti:

(a) da je proizvođač proveo odgovarajuće postupke ocjenjivanja sukladnosti iz članka 24.;

(b) da je proizvođač sastavio tehničku dokumentaciju;

(c) da proizvod s digitalnim elementima ima oznaku CE iz članka 22. i da su mu priložene informacije i upute za uporabu kako je utvrđeno u Prilogu II.

3. Ako uvoznik smatra ili ima razloga vjerovati da proizvod s digitalnim elementima ili postupci koje je proizvođač uspostavio nisu sukladni s bitnim zahtjevima iz Priloga I., ne smije staviti taj proizvod na tržište dok taj proizvod ili postupci koje je proizvođač uspostavio ne budu sukladni s bitnim zahtjevima iz Priloga I. Nadalje, ako proizvod s digitalnim elementima predstavlja znatan kibersigurnosni rizik, uvoznik o tome obavješćuje proizvođača i tijela za nadzor tržišta.

4. Uvoznici na proizvodu s digitalnim elementima ili, ako to nije moguće, na pakiranju ili u dokumentu priloženom uz proizvod s digitalnim elementima navode svoje ime, registrirano trgovačko ime ili registrirani žig, adresu i e-adresu za kontakt. Podaci za kontakt moraju biti na jeziku koji bez poteškoća razumiju korisnici i tijela za nadzor tržišta.

5. Uvoznici su se dužni pobrinuti da su uz proizvod s digitalnim elementima priložene upute i informacije iz Priloga II. na jeziku koji korisnici bez poteškoća razumiju.

6. Uvoznici koji znaju ili imaju razloga vjerovati da proizvod s digitalnim elementima koji su stavili na tržište ili postupci koje je proizvođač uspostavio nisu sukladni s bitnim zahtjevima iz Priloga I. odmah poduzimaju potrebne korektivne mjere da se ponovno uspostavi sukladnost tog proizvoda s digitalnim elementima ili postupaka koje je proizvođač uspostavio s bitnim zahtjevima iz Priloga I. ili da se proizvod prema potrebi povuče ili opozove..

Nakon što ustanove ranjivost proizvoda s digitalnim elementima uvoznici o njoj bez neopravdane odgode obavješćuju proizvođača. Nadalje, ako proizvod s digitalnim elementima predstavlja znatan kibersigurnosni rizik, uvoznici o tome odmah obavješćuju tijela za nadzor tržišta država članica u kojima su proizvod s digitalnim elementima stavili na raspolaganje na tržištu, pri čemu u prvom redu navode pojedinosti o nesukladnosti i o svim poduzetim korektivnim mjerama.

7. Uvoznici su dužni deset godina od stavljanja proizvoda s digitalnim elementima na tržište čuvati primjerak EU izjave o sukladnosti kako bi bila na raspolaganju tijelima za nadzor tržišta i osiguravati da se tehnička dokumentacija može staviti na raspolaganje tim tijelima na zahtjev.

8. Na obrazložen zahtjev tijela za nadzor tržišta uvoznici tom tijelu dostavljaju, u papirnatom ili elektroničkom obliku, sve informacije i dokumentaciju potrebne za dokazivanje sukladnosti proizvoda s digitalnim elementima s bitnim zahtjevima iz odjeljka 2. Priloga I. te postupaka koje je proizvođač uspostavio s bitnim zahtjevima iz odjeljka 1. Priloga I. na jeziku koje to tijelo bez poteškoća razumije. Na zahtjev tog tijela oni s njim surađuju u pogledu svake mjere koja je poduzeta kako bi se uklonili kibersigurnosni rizici koje predstavlja proizvod s digitalnim elementima koji su stavili na tržište.

9. Ako uvoznik proizvoda s digitalnim elementima sazna da je proizvođač tog proizvoda prestao s radom i zato ne može ispunjavati obveze utvrđene ovom Uredbom, uvoznik o toj situaciji obavješćuje nadležna tijela za nadzor tržišta te, na bilo koji raspoloživi način i u mjeri u kojoj je to moguće, korisnike proizvoda s digitalnim elementima koji su stavljeni na tržište.

Članak 14.

Obveze distributerâ

1. Pri stavljanju proizvoda s digitalnim elementima na raspolaganje na tržištu distributeri djeluju u skladu sa zahtjevima ove Uredbe.

2. Prije stavljanja na raspolaganje na tržištu proizvoda s digitalnim elementima distributeri moraju provjeriti:

   (a) ima li proizvod s digitalnim elementima oznaku CE;

   (b) jesu li proizvođač i uvoznik ispunili obveze iz članka 10. stavaka 10. i 11. te članka 13. stavka 4.

3. Ako distributer smatra ili ima razloga vjerovati da proizvod s digitalnim elementima ili postupci koje je proizvođač uspostavio nisu sukladni s bitnim zahtjevima iz Priloga I., distributer ne smije staviti na raspolaganje na tržištu proizvod s digitalnim elementima dok taj proizvod ili postupci koje je proizvođač uspostavio ne budu sukladni. Nadalje, ako proizvod s digitalnim elementima predstavlja znatan kibersigurnosni rizik, distributer o tome obavješćuje proizvođača i tijela za nadzor tržišta.

4. Distributeri koji znaju ili imaju razloga vjerovati da proizvod s digitalnim elementima koji su stavili na raspolaganje na tržištu ili postupci koje je proizvođač uspostavio nisu sukladni s bitnim zahtjevima iz Priloga I. dužni su se pobrinuti da se poduzmu potrebne korektivne mjere da se ponovno uspostavi sukladnosti tog proizvoda s digitalnim elementima ili postupaka koje je proizvođač uspostavio ili da se proizvod prema potrebi povuče ili opozove.

   Nakon što utvrde ranjivost proizvoda s digitalnim elementima, distributeri bez neopravdane odgode obavješćuju proizvođača o toj ranjivosti. Nadalje, ako proizvod s digitalnim elementima predstavlja znatan kibersigurnosni rizik, distributeri o tome bez odgode obavješćuju tijela za nadzor tržišta država članica u kojima su proizvod s digitalnim elementima stavili na raspolaganje na tržištu navodeći u prvom redu pojedinosti o nesukladnosti i o svim poduzetim korektivnim mjerama.

5. Na obrazložen zahtjev tijela za nadzor tržišta distributeri tom tijelu dostavljaju, u papirnatom ili elektroničkom obliku, sve informacije i dokumentaciju potrebne za dokazivanje sukladnosti proizvoda s digitalnim elementima i postupaka koje je proizvođač uspostavio s bitnim zahtjevima iz Priloga I. na jeziku koje to tijelo bez poteškoća razumije. Na zahtjev tog tijela distributeri s njim surađuju u pogledu svake mjere koja je poduzeta radi uklanjanja kibersigurnosnih rizika koje predstavljaju proizvodi s digitalnim elementima koje su stavili na raspolaganje na tržištu.

6. Ako distributer proizvoda s digitalnim elementima sazna da je proizvođač tog proizvoda prestao s radom i zato ne može ispunjavati obveze utvrđene ovom Uredbom, distributer o toj situaciji obavješćuje nadležna tijela za nadzor tržišta te, na bilo koji raspoloživi način i u mjeri u kojoj je to moguće, korisnike proizvoda s digitalnim elementima koji su stavljeni na tržište.

Članak 15.

Slučajevi u kojima se obveze proizvođačâ primjenjuju na uvoznike i distributere

Uvoznik ili distributer smatra se proizvođačem za potrebe ove Uredbe te podliježe obvezama proizvođača iz članka 10. i članka 11. stavaka 1., 2., 4. i 7. ako stavi proizvod s digitalnim elementima na tržište pod svojim imenom ili žigom ili ako učini bitnu izmjenu proizvoda s digitalnim elementima koji je već stavljen na tržište.

Članak 16.

Drugi slučajevi u kojima se primjenjuju obveze proizvođača

Fizička ili pravna osoba, osim proizvođača, uvoznika ili distributera, koja učini bitnu izmjenu proizvoda s digitalnim elementima smatra se proizvođačem za potrebe ove Uredbe.

Ta osoba podliježe obvezama proizvođača iz članka 10. i članka 11. stavaka 1., 2., 4. i 7. za dio proizvoda na koji utječe bitna izmjena ili, ako bitna izmjena utječe na kibersigurnost proizvoda s digitalnim elementima u cjelini, za cijeli proizvod.

Članak 17.

Identifikacija gospodarskih subjekata

1. Gospodarski subjekti dužni su tijelima za nadzor tržišta na njihov zahtjev dostaviti sljedeće informacije ako su takve informacije raspoložive:

   (a) ime i adresu svakog gospodarskog subjekta koji im je isporučio proizvod s digitalnim elementima;

   (b) ime i adresu svakog gospodarskog subjekta kojem su isporučili proizvod s digitalnim elementima.

2. Gospodarski subjekti moraju moći predočiti informacije iz stavka 1. deset godina nakon što im je proizvod s digitalnim elementima isporučen i deset godina nakon što su isporučili proizvod s digitalnim elementima.

POGLAVLJE III.

SUKLADNOST PROIZVODA S DIGITALNIM ELEMENTIMA

Članak 18.

Pretpostavka sukladnosti

1. Za proizvode s digitalnim elementima i postupke koje je proizvođač uspostavio koji su sukladni s usklađenim normama ili dijelovima usklađenih normi na koje su upućivanja objavljena u *Službenom listu Europske unije* pretpostavlja se da su sukladni s bitnim zahtjevima iz Priloga I. obuhvaćenima tim normama ili njihovim dijelovima.
2. Za proizvode s digitalnim elementima i postupke koje je proizvođač uspostavio koji su sukladni sa zajedničkim specifikacijama iz članka 19. pretpostavlja se da su sukladni s bitnim zahtjevima iz Priloga I. u mjeri u kojoj te zajedničke specifikacije obuhvaćaju te zahtjeve.
3. Za proizvode s digitalnim elementima i postupke koje je proizvođač uspostavio za koje su izdani EU izjava o sukladnosti ili certifikat u okviru europskog programa kibersigurnosne certifikacije donesenog na temelju Uredbe (EU) 2019/881 i određenog u skladu sa stavkom 4. pretpostavlja se da su sukladni s bitnim zahtjevima iz Priloga I. u mjeri u kojoj EU izjava o sukladnosti ili kibersigurnosni certifikat, ili njihovi dijelovi, obuhvaćaju te zahtjeve.
4. Komisija je ovlaštena provedbenim aktima odrediti europske programe kibersigurnosne certifikacije donesene na temelju Uredbe (EU) 2019/881 koji se mogu primijeniti za dokazivanje sukladnosti s bitnim zahtjevima ili njihovim dijelovima iz Priloga I. Nadalje, Komisija prema potrebi određuje oslobađa li kibersigurnosni certifikat izdan u okviru takvih programa proizvođače obveze ocjenjivanja sukladnosti koje provodi treća strana za odgovarajuće zahtjeve, kako je utvrđeno u članku 24. stavku 2. točkama (a) i (b) i članku 24. stavku 3. točkama (a) i (b). Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 51. stavka 2.

Članak 19.

Zajedničke specifikacije

Ako usklađene norme iz članka 18. ne postoje ili ako Komisija smatra da relevantne usklađene norme nisu dovoljne za ispunjavanje zahtjeva iz ove Uredbe ili za ispunjavanje Komisijina zahtjeva za normizaciju, ili ako postoje neopravdana kašnjenja u postupku normizacije ili ako europske organizacije za normizaciju nisu prihvatile zahtjev Komisije za usklađene norme, Komisija je ovlaštena provedbenim aktima donijeti zajedničke specifikacije u pogledu bitnih zahtjeva iz Priloga I. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 51. stavka 2.

Članak 20.

EU izjava o sukladnosti

1. EU izjavu o sukladnosti sastavljaju proizvođači u skladu s člankom 10. stavkom 7. i u njoj se navodi da je dokazano ispunjavanje primjenjivih bitnih zahtjeva iz Priloga I.

2. EU izjava o sukladnosti ima strukturu predloška iz Priloga IV. i sadržava elemente određene u odgovarajućim postupcima ocjenjivanja sukladnosti iz Priloga VI. Takva se izjava redovito ažurira. Stavlja se na raspolaganje na jezicima koje zahtijeva država članica u kojoj je proizvod s digitalnim elementima stavljen na tržište ili na raspolaganje na tržištu.

3. Ako se na proizvod s digitalnim elementima primjenjuje više akata Unije kojima se zahtijeva EU izjava o sukladnosti, u vezi sa svim takvim aktima Unije sastavlja se samo jedna EU izjava o sukladnosti. U toj izjavi navodi se o kojim je aktima Unije riječ, uključujući upućivanja na njihove objave.

4. Sastavljanjem EU izjave o sukladnosti proizvođač preuzima odgovornost za sukladnost proizvoda.

5. Kako bi se uzele u obzir tehnološke promjene, Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 50. radi dopune ove Uredbe dodavanjem elemenata minimalnom sadržaju EU izjave o sukladnosti iz Priloga IV.

Članak 21.

Opća načela za oznaku CE

Za oznaku CE kako je definirana u članku 3. stavku 32. vrijede opća načela utvrđena člankom 30. Uredbe (EZ) br. 765/2008.

Članak 22.

Pravila i uvjeti stavljanja oznake CE

1. Oznaka CE stavlja se na proizvod s digitalnim elementima tako da bude vidljiva, čitljiva i neizbrisiva. Ako to nije moguće ili nije opravdano zbog same prirode proizvoda s digitalnim elementima, oznaka se stavlja na pakiranje i na EU izjavu o sukladnosti iz članka 20. koja se prilaže proizvodu s digitalnim elementima. Za proizvode s digitalnim elementima koji su u obliku softvera oznaka CE stavlja se na EU izjavu o sukladnosti iz članka 20. ili na internetske stranice softverskog proizvoda.

2. Zbog prirode proizvoda s digitalnim elementima visina oznake CE koja se stavlja na proizvod s digitalnim elementima može biti manja od 5 mm, pod uvjetom da ostane vidljiva i čitljiva.

3. Oznaka CE stavlja se prije stavljanja proizvoda s digitalnim elementima na tržište. Iza nje može biti piktogram ili bilo koja druga oznaka koja označava poseban rizik ili uporaba utvrđeni u provedbenim aktima iz stavka 6.

4. Iza oznake CE navodi se identifikacijski broj prijavljenog tijela ako je to tijelo uključeno u postupak ocjenjivanja sukladnosti na temelju potpunog osiguranja kvalitete (na temelju modula H) iz članka 24.

   Identifikacijski broj prijavljenog tijela stavlja samo prijavljeno tijelo ili, prema njegovim uputama, proizvođač ili proizvođačev ovlašteni zastupnik.

5. Države članice oslanjaju se na postojeće mehanizme kako bi osigurale pravilnu primjenu sustava pravila za stavljanje oznake CE i poduzimaju odgovarajuće mjere u slučaju nepravilne uporabe te oznake. Ako proizvod s digitalnim elementima podliježe drugom zakonodavstvu Unije kojim se također propisuje stavljanje oznake

CE, na oznaci CE navodi se da proizvod ispunjava i zahtjeve tog drugog zakonodavstva.

6. Komisija može provedbenim aktima utvrditi tehničke specifikacije za piktograme ili bilo koje druge oznake povezane sa sigurnošću proizvoda s digitalnim elementima te mehanizme za promicanje njihove upotrebe. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 51. stavka 2.

Članak 23.

Tehnička dokumentacija

1. Tehnička dokumentacija sadržava sve relevantne podatke ili pojedinosti o načinima na koje proizvođač osigurava sukladnost proizvoda s digitalnim elementima i postupaka koje je uspostavio s bitnim zahtjevima iz Priloga I. Ona sadržava barem elemente utvrđene u Prilogu V.

2. Tehnička dokumentacija sastavlja se prije stavljanja na tržište proizvoda s digitalnim elementima i redovito se ažurira, prema potrebi, tijekom očekivanog vijeka trajanja proizvoda ili tijekom razdoblja od pet godina nakon stavljanja proizvoda s digitalnim elementima na tržište, ovisno o tome koje je razdoblje kraće.

3. Za proizvode s digitalnim elementima iz članka 8. i članka 24. stavka 4. koji podliježu i drugim aktima Unije sastavlja se jedinstvena tehnička dokumentacija koja sadržava informacije iz Priloga V. ovoj Uredbi i informacije koje se zahtijevaju tim aktima Unije.

4. Tehnička dokumentacija i korespondencija koje se odnose na bilo koji postupak ocjenjivanja sukladnosti sastavljaju se na jednom od službenih jezika države članice u kojoj prijavljeno tijelo ima poslovni nastan ili na njemu prihvatljivom jeziku.

5. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 50. radi dopune ove Uredbe elementima koje treba uključiti u tehničku dokumentaciju iz Priloga V. s obzirom na tehnološke promjene i iskustva u procesu provedbe ove Uredbe.

Članak 24.

Postupci ocjenjivanja sukladnosti proizvoda s digitalnim elementima

1. Proizvođač mora provesti ocjenjivanje sukladnosti proizvoda s digitalnim elementima i postupaka koje je uspostavio kako bi ustanovio jesu li ispunjeni bitni zahtjevi iz Priloga I. Proizvođač ili proizvođačev ovlašteni zastupnik dokazuje sukladnost s bitnim zahtjevima primjenom jednog od sljedećih postupaka:

   (a) postupak unutarnje kontrole (na temelju modula A) iz Priloga VI.; ili

   (b) postupak EU ispitivanja tipa (na temelju modula B) iz Priloga VI., nakon čega slijedi provjera sukladnosti s EU tipom koja se temelji na unutarnjoj kontroli proizvodnje (na temelju modula C) iz Priloga VI.; ili

   (c) ocjenjivanje sukladnosti na temelju potpunog osiguranja kvalitete (na temelju modula H) iz Priloga VI.

2. Ako proizvođač ili proizvođačev ovlašteni zastupnik pri ocjenjivanju sukladnosti rizičnog proizvoda s digitalnim elementima I. razreda iz Priloga III. i postupaka koje je njegov proizvođač uspostavio s bitnim zahtjevima iz Priloga I. nije primijenio ili je

samo djelomično primijenio usklađene norme, zajedničke specifikacije ili europske programe kibersigurnosne certifikacije iz članka 18. ili ako takve usklađene norme, zajedničke specifikacije ili europski programi kibersigurnosne certifikacije ne postoje, predmetni proizvod s digitalnim elementima i postupci koje je proizvođač uspostavio podvrgavaju se, s obzirom na te bitne zahtjeve, jednom od sljedećih postupaka:

(a) postupak EU ispitivanja tipa (na temelju modula B) iz Priloga VI., nakon čega slijedi provjera sukladnosti s EU tipom koja se temelji na unutarnjoj kontroli proizvodnje (na temelju modula C) iz Priloga VI.; ili

(b) ocjenjivanje sukladnosti na temelju potpunog osiguranja kvalitete (na temelju modula H) iz Priloga VI.

3. Ako je proizvod rizični proizvod s digitalnim elementima razreda II. iz Priloga III., proizvođač ili proizvođačev ovlašteni zastupnik sukladnost s bitnim zahtjevima iz Priloga I. dokazuje primjenom jednog od sljedećih postupaka:

(a) postupak EU ispitivanja tipa (na temelju modula B) iz Priloga VI., nakon čega slijedi provjera sukladnosti s EU tipom koja se temelji na unutarnjoj kontroli proizvodnje (na temelju modula C) iz Priloga VI.; ili

(b) ocjenjivanje sukladnosti na temelju potpunog osiguranja kvalitete (na temelju modula H) iz Priloga VI.

4. Proizvođači proizvoda s digitalnim elementima koji se smatraju sustavima elektroničkih zdravstvenih zapisa obuhvaćenima područjem primjene Uredbe [Uredba o europskom prostoru za zdravstvene podatke] sukladnost s bitnim zahtjevima iz Priloga I. ovoj Uredbi dokazuju primjenom odgovarajućeg postupka ocjenjivanja sukladnosti kako se zahtijeva Uredbom [poglavlje III. Uredbe o europskom prostoru za zdravstvene podatke].

5. Pri određivanju naknada za postupke ocjenjivanja sukladnosti prijavljena tijela uzimaju u obzir posebne interese i potrebe malih i srednjih poduzeća (MSP-ovi) i smanjuju te naknade razmjerno njihovim posebnim interesima i potrebama.

POGLAVLJE IV.

PRIJAVLJIVANJE TIJELÂ ZA OCJENJIVANJE SUKLADNOSTI

Članak 25.

Prijavljivanje

Države članice Komisiji i drugim državama članicama prijavljuju tijela za ocjenjivanje sukladnosti ovlaštena za provođenje ocjenjivanja sukladnosti u skladu s ovom Uredbom.

Članak 26.

Tijela koja provode prijavljivanje

1. Države članice imenuju tijelo koje provodi prijavljivanje nadležno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje i prijavljivanje tijela za ocjenjivanje sukladnosti te praćenje prijavljenih tijela, uključujući usklađenost s člankom 31.

2. Države članice mogu odlučiti da ocjenjivanje i praćenje iz stavka 1. provodi nacionalno akreditacijsko tijelo u smislu Uredbe (EZ) br. 765/2008 i u skladu s njom.

Članak 27.

Zahtjevi u pogledu tijela koja provode prijavljivanje

1. Tijelo koje provodi prijavljivanje osniva se tako da ne dolazi do sukoba interesa s tijelima za ocjenjivanje sukladnosti.
2. Tijelo koje provodi prijavljivanje organizirano je i radi tako da štiti objektivnost i nepristranost svojih aktivnosti.
3. Tijelo koje provodi prijavljivanje organizirano je tako da svaku odluku koja se odnosi na prijavljivanje tijela za ocjenjivanje sukladnosti donose nadležne osobe koje nisu provodile ocjenjivanje.
4. Tijelo koje provodi prijavljivanje ne nudi niti obavlja aktivnosti koje provode tijela za ocjenjivanje sukladnosti ni savjetodavne usluge na tržišnoj ili konkurentskoj osnovi.
5. Tijelo koje provodi prijavljivanje štiti povjerljivost prikupljenih informacija.
6. Tijelo koje provodi prijavljivanje raspolaže dovoljnim brojem stručnog osoblja za uredno obavljanje svojih zadaća.

Članak 28.

Obveze tijela koja provode prijavljivanje u pogledu obavješćivanja

1. Države članice obavješćuju Komisiju o svojim postupcima za ocjenjivanje i prijavljivanje tijelâ za ocjenjivanje sukladnosti, o praćenju prijavljenih tijela i o svim povezanim promjenama.
2. Komisija čini te informacije javno dostupnima.

Članak 29.

Zahtjevi u pogledu prijavljenih tijela

1. Za potrebe prijavljivanja tijelo za ocjenjivanje sukladnosti mora ispunjavati zahtjeve utvrđene u stavcima od 2. do 12.
2. Tijelo za ocjenjivanje sukladnosti osniva se na temelju nacionalnog prava te ima pravnu osobnost.
3. Tijelo za ocjenjivanje sukladnosti je tijelo koje ima svojstvo treće strane i neovisno je o organizaciji ili proizvodu koji ocjenjuje.

   Tijelo koje je član poslovnog udruženja ili strukovne udruge koje predstavlja poduzeća uključena u projektiranje, proizvodnju, dobavu, sastavljanje, uporabu ili održavanje proizvoda s digitalnim elementima koje ocjenjuje može se smatrati takvim tijelom za ocjenjivanje sukladnosti pod uvjetom da dokaže svoju neovisnost i nepostojanje bilo kakvog sukoba interesa.
4. Tijelo za ocjenjivanje sukladnosti, njegovo najviše rukovodstvo i osoblje zaduženo za provedbu zadaća ocjenjivanja sukladnosti ne smiju biti projektant, programer, proizvođač, dobavljač, instalater, kupac, vlasnik, korisnik ili održavatelj proizvoda s digitalnim elementima koji ocjenjuju, kao ni ovlašteni zastupnik bilo koje od tih

strana. To ne znači da tijelo za ocjenjivanje sukladnosti ne smije rabiti ocijenjene proizvode koji su mu nužni za rad niti da se ti proizvodi ne smiju rabiti u osobne svrhe.

Tijelo za ocjenjivanje sukladnosti, njegovo najviše rukovodstvo i osoblje zaduženo za provedbu zadaća ocjenjivanja sukladnosti ne smiju izravno sudjelovati u projektiranju, razvoju, proizvodnji, stavljanju na tržište, instaliranju, uporabi ili održavanju tih proizvoda ni zastupati strane koje sudjeluju u tim aktivnostima. Ne smiju sudjelovati ni u kakvoj aktivnosti koja može ugroziti neovisnost njihove prosudbe ili integritet u odnosu na aktivnosti ocjenjivanja sukladnosti za koje su prijavljeni. To se osobito odnosi na savjetodavne usluge.

Tijela za ocjenjivanje sukladnosti dužna su se pobrinuti da aktivnosti njihovih društava kćeri ili podugovaratelja ne utječu na povjerljivost, objektivnost ili nepristranost njihovih aktivnosti ocjenjivanja sukladnosti.

5. Tijela za ocjenjivanje sukladnosti i njihovo osoblje provode aktivnosti ocjenjivanja sukladnosti na najvišem stupnju profesionalnog integriteta i potrebne tehničke stručnosti u određenom području, bez pritisaka i poticaja, posebno financijskih, koji bi mogli utjecati na njihovu prosudbu ili rezultate aktivnosti ocjenjivanja sukladnosti, posebno u vezi s osobama ili skupinama osoba koje su zainteresirane za rezultate tih aktivnosti.

6. Tijelo za ocjenjivanje sukladnosti mora biti u stanju obavljati sve zadaće ocjenjivanja sukladnosti iz Priloga VI. i za koje je prijavljeno bez obzira na to obavlja li te zadaće samo ili se obavljaju u njegovo ime i pod njegovom odgovornošću.

Tijelo za ocjenjivanje sukladnosti u svakom trenutku te za svaki zasebni postupak ocjenjivanja sukladnosti i svaku vrstu ili kategoriju proizvoda s digitalnim elementima za koje je prijavljeno mora raspolagati potrebnim:

(a) osobljem s tehničkim znanjem te dostatnim i primjerenim iskustvom za obavljanje zadaća ocjenjivanja sukladnosti;

(b) opisima postupaka u skladu s kojima se provodi ocjenjivanje sukladnosti, čime se osigurava transparentnost i mogućnost ponavljanja tih postupaka; Mora imati uspostavljene odgovarajuće politike i postupke za razlikovanje zadaća koje provodi kao prijavljeno tijelo od drugih aktivnosti;

(c) postupcima za obavljanje aktivnosti u kojima se vodi računa o veličini poduzeća, sektoru u kojemu posluje, njegovoj strukturi, stupnju složenosti tehnologije proizvoda o kojima je riječ i masovnom ili serijskom karakteru proizvodnog procesa.

Raspolaže sredstvima potrebnima za pravilno obavljanje tehničkih i administrativnih zadaća povezanih s aktivnostima ocjenjivanja sukladnosti te ima pristup svoj potrebnoj opremi ili objektima.

7. Osoblje zaduženo za zadaće ocjenjivanja sukladnosti mora imati:

(a) dobru tehničku i stručnu osposobljenost kojom su obuhvaćene sve aktivnosti ocjenjivanja sukladnosti za koje je tijelo za ocjenjivanje sukladnosti prijavljeno;

(b) zadovoljavajuće poznavanje zahtjeva za ocjenjivanja koja provodi i odgovarajuće ovlaštenje za ta ocjenjivanja;

(c) odgovarajuće poznavanje i razumijevanje bitnih zahtjeva, primjenjivih usklađenih normi i relevantnih odredaba zakonodavstva Unije o usklađivanju te njegovih provedbenih akata;

(d) sposobnost za sastavljanje potvrda, vođenje evidencije i pripremu izvješća kojima se dokazuje da su ocjenjivanja provedena.

8. Nepristranost tijelâ za ocjenjivanje sukladnosti, njihova najvišeg rukovodstva i osoblja zaduženog za ocjenjivanje mora biti zajamčena.

Naknada za rad najvišeg rukovodstva i osoblja zaduženog za ocjenjivanje u tijelu za ocjenjivanje sukladnosti ne ovisi o broju ocjenjivanja sukladnosti ni o rezultatima tih ocjenjivanja.

9. Tijela za ocjenjivanje sukladnosti sklapaju ugovor o osiguranju od odgovornosti osim ako je odgovornost preuzela država članica u skladu s nacionalnim pravom ili ako je sama država članica izravno odgovorna za ocjenjivanje sukladnosti.

10. Osoblje tijela za ocjenjivanje sukladnosti čuva poslovnu tajnu koja se odnosi na sve podatke prikupljene pri provođenju svojih zadaća na temelju Priloga VI. ili bilo koje odredbe nacionalnog prava kojim ga se provodi, osim ako ih zahtijevaju tijela za nadzor tržišta države članice u kojoj se provode njegove aktivnosti. Vlasnička su prava zaštićena. Tijelo za ocjenjivanje sukladnosti ima uspostavljene dokumentirane postupke kojima se osigurava sukladnost s ovim stavkom.

11. Tijela za ocjenjivanje sukladnosti sudjeluju u odgovarajućim aktivnostima normizacije i aktivnostima koordinacijske skupine prijavljenog tijela osnovane na temelju članka 40. ili osiguravaju da je njihovo osoblje koje provodi ocjenjivanje informirano o tim aktivnostima te primjenjuju administrativne odluke i dokumente koji su rezultat rada te skupine kao opće smjernice.

12. Tijela za ocjenjivanje sukladnosti djeluju u skladu s nizom dosljednih, pravednih i razumnih uvjeta, posebice uzimajući u obzir interese MSP-ova u vezi s naknadama.

Članak 30.

Pretpostavka sukladnosti prijavljenih tijela

Ako tijelo za ocjenjivanje sukladnosti dokaže da ispunjava kriterije utvrđene u relevantnim usklađenim normama ili njihovim dijelovima, na koje su upućivanja objavljena u *Službenom listu Europske unije*, pretpostavlja se da ispunjava zahtjeve iz članka 29. u mjeri u kojoj primjenjive usklađene norme obuhvaćaju te zahtjeve.

Članak 31.

Društva kćeri i podugovaranje prijavljenih tijela

1. Ako prijavljeno tijelo određene zadaće povezane s ocjenjivanjem sukladnosti da u podugovor ili ih prenese društvu kćeri, dužno se pobrinuti da taj podugovaratelj ili to društvo kći ispunjava zahtjeve iz članka 29. te o tome obavijestiti tijelo koje provodi prijavljivanje.

2. Prijavljena tijela preuzimaju punu odgovornost za zadaće koje obavljaju podugovaratelji ili društva kćeri bez obzira na to gdje imaju poslovni nastan.

3. Aktivnosti se mogu dati u podugovor ili ih može provoditi društvo kći samo uz suglasnost proizvođača

4. Prijavljena tijela čuvaju na raspolaganju tijelu koje provodi prijavljivanje relevantne dokumente koji se odnose na ocjenu kvalifikacija podugovaratelja ili društva kćeri i poslova koje oni obavljaju na temelju ove Uredbe.

Članak 32.

Zahtjev za prijavljivanje

1. Tijelo za ocjenjivanje sukladnosti podnosi zahtjev za prijavljivanje tijelu koje provodi prijavljivanje u državi članici u kojoj ima poslovni nastan.

2. Tom zahtjevu prilaže se opis aktivnosti ocjenjivanja sukladnosti, postupaka ocjenjivanja sukladnosti te proizvoda za koje to tijelo tvrdi da je nadležno te, ako postoji, potvrda o akreditaciji koju je izdalo nacionalno akreditacijsko tijelo kojom se potvrđuje da tijelo za ocjenjivanje sukladnosti ispunjava zahtjeve iz članka 29.

3. Ako predmetno tijelo za ocjenjivanje sukladnosti ne može dostaviti potvrdu o akreditaciji, ono tijelu koje provodi prijavljivanje dostavlja svu dokaznu dokumentaciju potrebnu za provjeru, priznavanje i redovito praćenje njegove usklađenosti sa zahtjevima iz članka 29.

Članak 33.

Postupak prijavljivanja

1. Tijela koja provode prijavljivanje mogu prijaviti samo tijela za ocjenjivanje sukladnosti koja ispunjavaju zahtjeve iz članka 29.

2. Tijelo koje provodi prijavljivanje dostavlja prijavu Komisiji i drugim državama članicama putem informacijskog sustava prijavljenih i imenovanih tijela prema novom pristupu (NANDO) koji je izradila i vodi Komisija.

3. Prijava obuhvaća sve pojedinosti o aktivnostima ocjenjivanja sukladnosti, modulima za ocjenjivanje sukladnosti te predmetnim proizvodima i odgovarajućoj potvrdi o stručnosti.

4. Ako se prijavljivanje ne temelji na potvrdi o akreditaciji iz članka 32. stavka 2., tijelo koje provodi prijavljivanje Komisiji i drugim državama članicama dostavlja dokaznu dokumentaciju kojom se potvrđuju stručnost tijela za ocjenjivanje sukladnosti i uspostavljeni mehanizmi kako bi se osiguralo da će se tijelo redovito pratiti i da će nastaviti ispunjavati zahtjeve iz članka 29.

5. Predmetno tijelo može obavljati aktivnosti prijavljenog tijela samo ako Komisija i druge države članice ne podnesu prigovor u roku od dva tjedna od prijavljivanja ako je upotrijebljena potvrda o akreditaciji ili u roku od dva mjeseca od prijavljivanja ako akreditacija nije upotrijebljena.

   Samo se takvo tijelo smatra prijavljenim tijelom za potrebe ove Uredbe.

6. Komisija i ostale države članice obavješćuju se o svim naknadnim relevantnim izmjenama prijave.

Članak 34.

Identifikacijski brojevi i popisi prijavljenih tijela

1. Komisija prijavljenom tijelu dodjeljuje identifikacijski broj.

Dodjeljuje mu samo jedan takav broj, čak i ako je tijelo prijavljeno na temelju više akata Unije.

2. Komisija objavljuje popis tijela prijavljenih na temelju ove Uredbe, uključujući identifikacijske brojeve koji su im dodijeljeni i aktivnosti za koje su prijavljena.

Komisija osigurava ažuriranje tog popisa.

Članak 35.

Izmjene prijava

1. Ako tijelo koje provodi prijavljivanje utvrdi ili sazna da prijavljeno tijelo više ne ispunjava zahtjeve iz članka 29. ili da ne ispunjava obveze, tijelo koje provodi prijavljivanje prema potrebi ograničava, suspendira ili povlači prijavu, ovisno o ozbiljnosti neispunjavanja tih zahtjeva ili obveza. O tome odmah obavješćuje Komisiju i druge države članice.

2. U slučaju ograničenja, suspenzije ili povlačenja prijave, ili ako je prijavljeno tijelo prestalo s radom, država članica koja provodi prijavljivanje poduzima odgovarajuće korake kako bi osigurala da predmete tog tijela obradi drugo prijavljeno tijelo ili da se stave na raspolaganje nadležnim tijelima koja provode prijavljivanje i tijelima za nadzor tržišta na njihov zahtjev.

Članak 36.

Osporavanje stručnosti prijavljenih tijela

1. Komisija istražuje sve slučajeve u kojima sumnja ili u kojima je upozorena na sumnju u stručnost prijavljenog tijela ili u to da ono kontinuirano ispunjava zahtjeve i obveze.

2. Država članica koja provodi prijavljivanje Komisiji na zahtjev dostavlja sve informacije o osnovi za prijavljivanje ili održavanju stručnosti predmetnog tijela.

3. Komisija osigurava da se sa svim osjetljivim informacijama prikupljenima tijekom njezinih istraga postupa kao s povjerljivim informacijama.

4. Ako Komisija utvrdi da prijavljeno tijelo ne ispunjava ili da više ne ispunjava zahtjeve za svoju prijavu, o tome obavješćuje državu članicu koje ga je prijavila i od nje zahtijeva da poduzme potrebne korektivne mjere, uključujući povlačenje prijave ako je to potrebno.

Članak 37.

Radne obveze prijavljenih tijela

1. Prijavljena tijela provode ocjenjivanja sukladnosti u skladu s postupcima ocjenjivanja sukladnosti iz članka 24. i Priloga VI.

2. Ocjenjivanja sukladnosti provode se razmjerno tako da se izbjegne nepotrebno opterećivanje gospodarskih subjekata. Tijela za ocjenjivanje sukladnosti obavljaju svoje aktivnosti vodeći računa o veličini poduzeća, sektoru u kojem posluje, njegovoj strukturi, stupnju složenosti tehnologije proizvoda o kojoj je riječ i masovnoj ili serijskoj prirodu proizvodnog procesa.

3. Međutim, prijavljena tijela poštuju stupanj strogosti i razinu zaštite koji su potrebni za sukladnost proizvoda s odredbama Uredbe.

4. Ako prijavljeno tijelo ustanovi da proizvođač ne ispunjava zahtjeve iz Priloga I. ili odgovarajućih usklađenih normi ili zajedničkih specifikacija iz članka 19., ono zahtijeva od proizvođača da poduzme odgovarajuće korektivne mjere i ne izdaje certifikat o sukladnosti.

5. Ako tijekom praćenja sukladnosti nakon izdavanja potvrde prijavljeno tijelo ustanovi da proizvod više nije sukladan sa zahtjevima iz ove Uredbe, ono zahtijeva od proizvođača da poduzme primjerene korektivne mjere te po potrebi obustavlja ili povlači certifikat.

6. Ako korektivne mjere nisu poduzete ili nemaju traženi učinak, prijavljeno tijelo prema potrebi ograničava, suspendira ili povlači certifikate.

Članak 38.

Obveze prijavljenih tijela u pogledu obavješćivanja

1. Prijavljena tijela obavješćuju tijelo koje provodi prijavljivanje o sljedećem:

   (a) svakom odbijanju, ograničenju, suspenziji ili povlačenju certifikata;

   (b) svim okolnostima koje utječu na opseg ili uvjete njegove prijave;

   (c) svim zahtjevima za dostavu informacija koje su primila od tijela za nadzor tržišta o aktivnostima ocjenjivanja sukladnosti;

   (d) na zahtjev, aktivnostima ocjenjivanja sukladnosti provedenima u području za koje je prijavljeno i svim drugim provedenim aktivnostima, uključujući prekogranične aktivnosti i davanje u podugovor.

2. Prijavljena tijela drugim tijelima koja su prijavljena na temelju ove Uredbe i koja provode slične aktivnosti ocjenjivanja sukladnosti kojima su obuhvaćeni isti proizvodi dostavljaju relevantne informacije o pitanjima koja se odnose na negativne i, na zahtjev, pozitivne rezultate ocjenjivanja sukladnosti.

Članak 39.

Razmjena iskustva

Komisija organizira razmjenu iskustava među nacionalnim tijelima država članica koja su odgovorna za politiku prijavljivanja.

Članak 40.

Koordinacija prijavljenih tijela

1. Komisija uspostavlja prikladnu koordinaciju i suradnju među prijavljenim tijelima te osigurava pravilno upravljanje tom koordinacijom i suradnjom u okviru međusektorske skupine prijavljenih tijela.

2. Države članice osiguravaju da tijela koja su prijavile sudjeluju u radu te skupine izravno ili posredstvom imenovanih predstavnika.

POGLAVLJE V.

NADZOR TRŽIŠTA I PROVEDBA

Članak 41.

Nadzor tržišta i kontrola proizvoda s digitalnim elementima na tržištu Unije

1. Uredba (EU) 2019/1020 primjenjuje se na proizvode s digitalnim elementima obuhvaćene područjem primjene ove Uredbe.

2. Svaka država članica određuje jedno ili više tijela za nadzor tržišta za potrebe osiguravanja djelotvorne provedbe ove Uredbe. Države članice mogu imenovati postojeće ili novo tijelo koje će djelovati kao tijelo za nadzor tržišta za potrebe ove Uredbe.

3. Tijela za nadzor tržišta prema potrebi surađuju i redovito razmjenjuju informacije s nacionalnim tijelima za kibersigurnosnu certifikaciju imenovanima na temelju članka 58. Uredbe (EU) 2019/881. Imenovana tijela za nadzor tržišta surađuju s ENISA-om u pogledu nadzora provedbe obveza izvješćivanja na temelju članka 11. ove Uredbe.

4. Tijela za nadzor tržišta prema potrebi surađuju i redovito razmjenjuju informacije s drugim tijelima za nadzor tržišta imenovanima na temelju drugog zakonodavstva Unije o usklađivanju za druge proizvode .

5. Tijela za nadzor tržišta prema potrebi surađuju s tijelima za nadzor prava Unije o zaštiti podataka. Takva suradnja uključuje informiranje tih tijela o svim nalazima relevantnima za ispunjavanje njihovih nadležnosti, među ostalim pri davanju smjernica i savjeta na temelju stavka 8. ovog članka ako se te smjernice i ti savjeti odnose na obradu osobnih podataka.

   Tijela za nadzor prava Unije o zaštiti podataka ovlaštena su zatražiti svaku dokumentaciju koja je izrađena ili se vodi na temelju ove Uredbe ili joj pristupiti ako je pristup toj dokumentaciji nužan za ispunjavanje njihovih zadaća. Ona obavješćuju imenovana tijela za nadzor tržišta predmetne države članice o svakom takvom zahtjevu.

6. Države članice osiguravaju da imenovana tijela za nadzor tržišta imaju odgovarajuće financijske i ljudske resurse za obavljanje svojih zadaća na temelju ove Uredbe.

7. Komisija olakšava razmjenu iskustava među imenovanim tijelima za nadzor tržišta.

8. Tijela za nadzor tržišta mogu gospodarskim subjektima pružati smjernice i savjete o provedbi ove Uredbe, uz potporu Komisije.

9. Tijela za nadzor tržišta na godišnjoj osnovi izvješćuju Komisiju o ishodima relevantnih aktivnosti nadzora tržišta. Imenovano tijelo za nadzor tržišta bez odgode dostavlja Komisiji i relevantnim nacionalnim tijelima za tržišno natjecanje sve informacije utvrđene tijekom aktivnosti nadzora tržišta koje bi mogle biti od interesa za primjenu prava Unije o tržišnom natjecanju.

10. Za proizvode s digitalnim elementima obuhvaćene područjem primjene ove Uredbe koji su klasificirani u visokorizične UI sustave u skladu s člankom [članak 6.] Uredbe [Uredba o umjetnoj inteligenciji] tijela za nadzor tržišta imenovana za potrebe Uredbe [Uredba o umjetnoj inteligenciji] su tijela nadležna za aktivnosti nadzora tržišta koje se zahtijevaju ovom Uredbom. Tijela za nadzor tržišta

imenovana na temelju Uredbe [Uredba o umjetnoj inteligenciji] prema potrebi surađuju s tijelima za nadzor tržišta imenovanima na temelju ove Uredbe i, u pogledu nadzora provedbe obveza izvješćivanja na temelju članka 11., s ENISA-om. Tijela za nadzor tržišta imenovana na temelju Uredbe [Uredba o umjetnoj inteligenciji] posebice su dužna obavijestiti tijela za nadzor tržišta imenovana na temelju ove Uredbe o svakom nalazu relevantnom za ispunjavanje njihovih zadaća koje se odnose na provedbu ove Uredbe.

11. Radi ujednačene primjene ove Uredbe osniva se posebna administrativna skupina za koordinaciju (skupina za ADCO) u skladu s člankom 30. stavkom 2. Uredbe (EU) 2019/1020. Skupina za ADCO sastoji se od predstavnika imenovanih tijela za nadzor tržišta i prema potrebi predstavnika jedinstvenih ureda za vezu.

Članak 42.

Pristup podacima i dokumentaciji

Ako je potrebno radi ocjenjivanja sukladnosti proizvoda s digitalnim elementima i postupaka koje su njihovi proizvođači uspostavili s bitnim zahtjevima iz Priloga I. i na obrazložen zahtjev, tijelima za nadzor tržišta dopušta se pristup podacima potrebnima za ocjenjivanje projektiranja, razvoja i proizvodnje takvih proizvoda te upravljanja njihovim ranjivostima, uključujući povezanu internu dokumentaciju predmetnog gospodarskog subjekta.

Članak 43.

Postupak na nacionalnoj razini za proizvode s digitalnim elementima koji predstavljaju znatan kibersigurnosni rizik

1. Ako tijelo za nadzor tržišta države članice ima dovoljno razloga smatrati da proizvod s digitalnim elementima, uključujući upravljanje njegovim ranjivostima, predstavlja znatan kibersigurnosni rizik, ono provodi evaluaciju tog proizvoda s digitalnim elementima koja se odnosi na njegovu sukladnost sa svim zahtjevima iz ove Uredbe. Relevantni gospodarski subjekti prema potrebi surađuju s tijelom za nadzor tržišta.

   Ako tijelo za nadzor tržišta tijekom te evaluacije ustanovi da proizvod s digitalnim elementima nije sukladan sa zahtjevima iz ove Uredbe, ono od relevantnog subjekta mora bez odgode zatražiti da poduzme sve odgovarajuće korektivne mjere kako bi se proizvod uskladio s tim zahtjevima, povukao s tržišta ili opozvao u razumnom roku, razmjerno vrsti rizika i ovisno o tome što propiše.

   Tijelo za nadzor tržišta o tome je dužno na odgovarajući način obavijestiti relevantno prijavljeno tijelo. Na odgovarajuće korektivne mjere primjenjuje se članak 18. Uredbe (EU) 2019/1020.

2. Ako smatra da nesukladnost nije ograničena samo na područje njegove države, tijelo za nadzor tržišta mora obavijestiti Komisiju i druge države članice o rezultatima evaluacije i mjerama koje je zahtijevalo od subjekta.

3. Proizvođač osigurava da su poduzete sve odgovarajuće korektivne mjere u pogledu predmetnih proizvoda s digitalnim elementima koje je stavio na raspolaganje na tržištu u Uniji.

4. Ako proizvođač proizvoda s digitalnim elementima ne poduzme prikladne korektivne mjere u razdoblju iz stavka 1. drugog podstavka, tijelo za nadzor tržišta poduzima sve odgovarajuće privremene mjere kako bi zabranilo ili ograničilo stavljanje na

raspolaganje na svojem nacionalnom tržištu tog proizvoda, povuklo ga s tržišta ili ga opozvalo.

To tijelo o tim mjerama bez odgode obavješćuje Komisiju i druge države članice.

5. Informacije iz stavka 4. uključuju sve dostupne pojedinosti, posebno podatke nužne za identifikaciju nesukladnih proizvoda s digitalnim elementima, podrijetlo proizvoda s digitalnim elementima, vrstu navodne nesukladnosti i povezanog rizika, prirodu i trajanje poduzetih nacionalnih mjera te argumente relevantnog subjekta. Tijela za nadzor tržišta posebno navode je li nesukladnost uzrokovana nečim od sljedećeg:

   (a) proizvod ili postupci koje je proizvođač uspostavio ne ispunjavaju bitne zahtjeve iz Priloga I.;

   (b) nedostaci usklađenih normi, programa kibersigurnosne certifikacije ili zajedničkih specifikacija iz članka 18.

6. Tijela za nadzor tržišta država članica, osim tijela za nadzor tržišta države članice koje je pokrenulo postupak, bez odgode obavješćuju Komisiju i druge države članice o svim donesenim mjerama i o svim dodatnim informacijama koje su im na raspolaganju u vezi s nesukladnošću predmetnog proizvoda te, u slučaju neslaganja s prijavljenom nacionalnom mjerom, o svojim prigovorima.

7. Ako u roku od tri mjeseca od primitka informacija iz stavka 4. nijedna država članica ni Komisija ne podnese prigovor na privremenu mjeru koju je poduzela određena država članica, mjera se smatra opravdanom. Time se ne dovode u pitanje postupovna prava predmetnog subjekta u skladu s člankom 18. Uredbe (EU) 2019/1020.

8. Tijela za nadzor tržišta svih država članica osiguravaju da se odgovarajuće restriktivne mjere za predmetni proizvod, primjerice povlačenje proizvoda s njihovih tržišta, poduzmu bez odgode.

Članak 44.

Zaštitni postupak Unije

1. Ako država članica u roku od tri mjeseca od primitka obavijesti iz članka 43. stavka 4. podnese prigovore na mjeru koju je poduzela druga država članica ili ako Komisija smatra da je mjera protivna zakonodavstvu Unije, Komisija bez odgode započinje savjetovanje s relevantnom državom članicom i gospodarskim subjektom ili gospodarskim subjektima te evaluira nacionalnu mjeru. Na temelju rezultata te evaluacije Komisija u roku od devet mjeseci od obavijesti iz članka 43. stavka 4. odlučuje je li nacionalna mjera opravdana te o toj odluci obavješćuje predmetnu državu članicu.

2. Ako se nacionalna mjera smatra opravdanom, sve države članice poduzimaju mjere potrebne kako bi osigurale povlačenje nesukladnog proizvoda s digitalnim elementima s njihova tržišta te o tome obavješćuju Komisiju. Ako se nacionalna mjera smatra neopravdanom, predmetna država članica mora tu mjeru povući.

3. Ako se nacionalna mjera smatra opravdanom i ako je nesukladnost proizvoda s digitalnim elementima pripisana nedostacima usklađenih normi, Komisija primjenjuje postupak iz članka 10. Uredbe (EU) br. 1025/2012.

4. Ako se nacionalna mjera smatra opravdanom i ako je nesukladnost proizvoda s digitalnim elementima pripisana nedostacima europskog programa kibersigurnosne certifikacije iz članka 18., Komisija je dužna razmotriti izmjenu ili stavljanje izvan snage provedbenog akta iz članka 18. stavka 4. kojim je utvrđena pretpostavka sukladnosti koja se odnosi na taj program certifikacije.

5. Ako se nacionalna mjera smatra opravdanom i ako je nesukladnost proizvoda s digitalnim elementima pripisana nedostacima zajedničkih specifikacija iz članka 19., Komisija je dužna razmotriti izmjenu ili stavljanje izvan snage provedbenog akta iz članka 19. kojim su te zajedničke specifikacije utvrđene.

Članak 45.

Postupak na razini EU-a za proizvode s digitalnim elementima koji predstavljaju znatan kibersigurnosni rizik

1. Ako Komisija ima dovoljno razloga smatrati, među ostalim na temelju informacija koje je pružila ENISA, da proizvod s digitalnim elementima koji predstavlja znatan kibersigurnosni rizik nije sukladan sa zahtjevima iz ove Uredbe, ona može zahtijevati od relevantnih tijela za nadzor tržišta da provedu evaluaciju sukladnosti i primijene postupke iz članka 43.

2. U iznimnim okolnostima koje opravdavaju brzu intervenciju radi očuvanja dobrog funkcioniranja unutarnjeg tržišta i ako Komisija ima dovoljno razloga smatrati da proizvod iz stavka 1. i dalje nije sukladan sa zahtjevima iz ove Uredbe, a nadležna tijela za nadzor tržišta nisu poduzela nikakve učinkovite mjere, Komisija može zahtijevati od ENISA-e da provede evaluaciju sukladnosti. Komisija o tome na odgovarajući način obavješćuje relevantna tijela za nadzor tržišta. Relevantni gospodarski subjekti prema potrebi surađuju s ENISA-om.

3. Na temelju ENISA-ine evaluacije Komisija može odlučiti da je potrebna korektivna ili restriktivna mjera na razini Unije. U tu svrhu Komisija se bez odgode savjetuje s predmetnim državama članicama i relevantnim gospodarskim subjektom ili subjektima.

4. Na temelju savjetovanja iz stavka 3. Komisija može donijeti provedbene akte o odluci o korektivnim ili restriktivnim mjerama na razini Unije, uključujući nalaganje povlačenja s tržišta ili opoziva u razumnom roku, razmjerno vrsti rizika. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 51. stavka 2.

5. Komisija o odluci iz stavka 4. bez odgode obavješćuje relevantne gospodarske subjekte. Države članice bez odgode provode akte iz stavka 4. i o tome obavješćuju Komisiju.

6. Stavci od 2. do 5. primjenjivi su dok traje iznimna situacija koja opravdava intervenciju Komisije i do ponovne uspostave sukladnosti tog proizvoda s ovom Uredbom.

Članak 46.

Sukladni proizvodi s digitalnim elementima koji predstavljaju znatan kibersigurnosni rizik

1. Ako tijelo za nadzor tržišta države članice nakon provedene evaluacije na temelju članka 43. ustanovi da proizvod s digitalnim elementima i postupci koje je proizvođač uspostavio, iako su sukladni s ovom Uredbom, ipak predstavljaju znatan kibersigurnosni rizik i, usto, rizik za zdravlje ili sigurnost osoba, rizik za

ispunjavanje obveza na temelju prava Unije ili nacionalnog prava za zaštitu temeljnih prava, rizik za dostupnost, autentičnost, cjelovitost ili povjerljivost usluga koje pomoću elektroničkog informacijskog sustava nude ključni subjekti koji pripadaju vrsti iz [Priloga I. Direktivi XXX/XXXX (NIS2)] ili rizik za druge aspekte zaštite javnog interesa, ono od relevantnog subjekta zahtijeva da poduzme sve odgovarajuće mjere kojima se osigurava da predmetni proizvod s digitalnim elementima i postupci koje je uspostavio proizvođač, nakon stavljanja na tržište, više ne predstavljaju taj rizik, povuče taj proizvod s digitalnim elementima s tržišta ili ga opozove u razumnom roku, razmjerno prirodi rizika.

2. Proizvođač ili drugi relevantni subjekti osiguravaju poduzimanje korektivnih mjera u pogledu predmetnih proizvoda s digitalnim elementima koje su stavili na raspolaganje na tržištu u Uniji u roku koji je utvrdilo tijelo za nadzor tržišta države članice iz stavka 1.

3. Država članica odmah obavješćuje Komisiju i druge države članice o mjerama poduzetima u skladu sa stavkom 1. Ta obavijest uključuje sve dostupne pojedinosti, osobito identifikacijske podatke predmetnih proizvoda s digitalnim elementima, podrijetlo i lanac opskrbe tih proizvoda s digitalnim elementima, vrstu rizika te vrstu i trajanje poduzetih nacionalnih mjera.

4. Komisija se bez odgode savjetuje s državama članicama i relevantnim gospodarskim subjektom te evaluira poduzete nacionalne mjere. Na temelju rezultata te evaluacije Komisija odlučuje o opravdanosti poduzete mjere i prema potrebi predlaže odgovarajuće mjere.

5. Komisija svoju odluku upućuje državama članicama.

6. Ako Komisija ima dovoljno razloga smatrati, među ostalim na temelju informacija koje je pružila ENISA, da proizvod s digitalnim elementima, iako sukladan s ovom Uredbom, predstavlja rizike iz stavka 1., ona može od relevantnih tijela za nadzor tržišta zahtijevati da provedu evaluaciju sukladnosti i primijene postupke iz članka 43. i stavaka 1., 2. i 3. ovog članka.

7. U iznimnim okolnostima koje opravdavaju brzu intervenciju radi očuvanja dobrog funkcioniranja unutarnjeg tržišta i ako Komisija ima dovoljno razloga smatrati da proizvod iz stavka 6. i dalje predstavlja rizike iz stavka 1., a relevantna tijela za nadzor tržišta nisu poduzela nikakve učinkovite mjere, Komisija može od ENISA-e zahtijevati da provede evaluaciju rizika koje taj proizvod predstavlja te o tome obavješćuje relevantna tijela za nadzor tržišta. Relevantni gospodarski subjekti prema potrebi surađuju s ENISA-om.

8. Na temelju ENISA-ine evaluacije iz stavka 7. Komisija može utvrditi da je potrebna korektivna ili restriktivna mjera na razini Unije. U tu se svrhu Komisija bez odgode savjetuje s predmetnim državama članicama i relevantnim subjektima.

9. Na temelju savjetovanja iz stavka 8. Komisija može donijeti provedbene akte o odluci o korektivnim ili restriktivnim mjerama na razini Unije, uključujući nalaganje povlačenja s tržišta ili opoziva u razumnom roku, razmjerno vrsti rizika. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 51. stavka 2.

10. Komisija o odluci iz stavka 9. odmah obavješćuje relevantne subjekte. Države članice bez odgode provode takve akte i o tome obavješćuju Komisiju.

11. Stavci od 6. do 10. primjenjivi su dok traje iznimna situacija koja opravdava intervenciju Komisije i dok predmetni proizvod predstavlja rizike iz stavka 1.

Članak 47.

Formalna nesukladnost

1. Tijelo za nadzor tržišta države članice zahtijeva od relevantnog proizvođača da otkloni predmetnu nesukladnost ako ustanovi nešto od sljedećeg:

   (a) oznaka sukladnosti stavljena je tako da se krše članci 21. i 22.;

   (b) oznaka sukladnosti nije stavljena;

   (c) EU izjava o sukladnosti nije sastavljena;

   (d) EU izjava o sukladnosti nije pravilno sastavljena;

   (e) identifikacijski broj prijavljenog tijela uključenog u postupak ocjenjivanja sukladnosti, ako je primjenjivo, nije stavljen;

   (f) tehnička dokumentacija nije dostupna ili nije potpuna.

2. Ako se nesukladnost iz stavka 1. ne otkloni, predmetna država članica poduzima sve odgovarajuće mjere kako bi ograničila ili zabranila stavljanje proizvoda s digitalnim elementima na raspolaganje na tržištu ili kako bi osigurala njegov opoziv ili povlačenje s tržišta.

Članak 48.

Zajedničke aktivnosti tijelâ za nadzor tržišta

1. Tijela za nadzor tržišta mogu s drugim relevantnim tijelima dogovoriti provedbu zajedničkih aktivnosti za kibersigurnost i zaštitu potrošača koje se odnose na određene proizvode s digitalnim elementima koji se stavljaju na tržište ili na raspolaganje na tržištu, posebice proizvode za koje se često ustanovi da predstavljaju kibersigurnosne rizike.

2. Komisija ili ENISA mogu predlagati zajedničke aktivnosti za provjeru sukladnosti s ovom Uredbom koje će provesti tijela za nadzor tržišta na temelju naznaka ili informacija o tome da u nekoliko država članica postoji potencijalna nesukladnost proizvoda obuhvaćenih područjem primjene ove Uredbe sa zahtjevima koji su u njoj utvrđeni.

3. Tijela za nadzor tržišta i Komisija prema potrebi osiguravaju da sporazum o provedbi zajedničkih aktivnosti ne dovede do nepoštenog tržišnog natjecanja između gospodarskih subjekata i da ne utječe štetno na objektivnost, neovisnost i nepristranost stranaka sporazuma.

4. Tijelo za nadzor tržišta može upotrijebiti sve informacije koje su rezultat aktivnosti u okviru bilo koje istrage koju je provelo.

5. Predmetno tijelo za nadzor tržišta i Komisija prema potrebi stavljaju na raspolaganje javnosti sporazum o zajedničkim aktivnostima, uključujući imena uključenih stranaka.

Članak 49.

Opsežne provjere

1. Tijela za nadzor tržišta mogu odlučiti provesti istodobne koordinirane kontrolne mjere („opsežne provjere”) nad određenim proizvodima s digitalnim elementima ili

kategorijama takvih proizvoda radi provjere sukladnosti s ovom Uredbom ili otkrivanja njezinih povreda.

2. Osim ako se uključena tijela za nadzor tržišta dogovore drukčije, opsežne provjere koordinira Komisija. Koordinator opsežne provjere može prema potrebi javno objaviti ukupne rezultate.

3. ENISA može pri obavljanju svojih zadaća utvrditi, među ostalim na temelju obavijesti primljenih u skladu s člankom 11. stavcima 1. i 2., kategorije proizvoda za koje se mogu organizirati opsežne provjere. Prijedlog o opsežnim provjerama dostavlja se potencijalnom koordinatoru iz stavka 2. kako bi ga tijela za nadzor tržišta mogla razmotriti.

4. Pri provedbi opsežnih provjera uključena tijela za nadzor tržišta mogu se koristiti istražnim ovlastima utvrđenima u člancima od 41. do 47. i svim drugim ovlastima koje su im dodijeljene nacionalnim pravom.

5. Tijela za nadzor tržišta mogu pozvati službenike Komisije i druge osobe u pratnji koje je ovlastila Komisija da sudjeluju u opsežnim provjerama.

POGLAVLJE VI.

DELEGIRANJE OVLASTI I POSTUPAK ODBORA

Članak 50.

Izvršavanje delegiranja ovlasti

1. Ovlast za donošenje delegiranih akata dodjeljuje se Komisiji u skladu s uvjetima utvrđenima u ovom članku.

2. Komisiji se dodjeljuje ovlast za donošenje delegiranih akata iz članka 2. stavka 4., članka 6. stavka 2., članka 6. stavka 3., članka 6. stavka 5., članka 20. stavka 5. i članka 23. stavka 5.

3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 2. stavka 4., članka 6. stavka 2., članka 6. stavka 3., članka 6. stavka 5., članka 20. stavka 5. i članka 23. stavka 5. Odlukom o opozivu prekida se delegiranje ovlasti koje je u njoj navedeno. Opoziv počinje proizvoditi učinke sljedećeg dana od dana objave spomenute odluke u Službenom listu Europske unije ili na kasniji dan naveden u spomenutoj odluci. On ne utječe na valjanost delegiranih akata koji su već na snazi.

4. Prije donošenja delegiranog akta Komisija se savjetuje sa stručnjacima koje je imenovala svaka država članica u skladu s načelima utvrđenima u Međuinstitucijskom sporazumu o boljoj izradi zakonodavstva od 13. travnja 2016.

5. Čim donese delegirani akt, Komisija ga istodobno priopćuje Europskom parlamentu i Vijeću.

6. Delegirani akt donesen na temelju članka 2. stavka 4., članka 6. stavaka 2., 3. i 5., članka 20. stavka 5. i članka 23. stavka 5. stupa na snagu samo ako ni Europski parlament ni Vijeće u roku od dva mjeseca od priopćenja tog akta Europskom parlamentu i Vijeću na njega ne podnesu nikakav prigovor ili ako su prije isteka tog roka i Europski parlament i Vijeće obavijestili Komisiju da neće podnijeti prigovore. Taj se rok produljuje za dva mjeseca na inicijativu Europskog parlamenta ili Vijeća.

Članak 51.

Postupak odbora

1. Komisiji pomaže odbor. Navedeni odbor je odbor u smislu Uredbe (EU) br. 182/2011.

2. Pri upućivanju na ovaj stavak primjenjuje se članak 5. Uredbe (EU) br. 182/2011.

3. Kad se mišljenje odbora treba dobiti pisanim postupkom, navedeni postupak završava bez rezultata kad u roku za davanje mišljenja to odluči predsjednik odbora ili to zahtijeva član odbora.

POGLAVLJE VII.

POVJERLJIVOST I SANKCIJE

Članak 52.

Povjerljivost

1. Sve strane uključene u primjenu ove Uredbe moraju poštovati povjerljivost informacija i podataka koje dobiju pri obavljanju svojih zadaća i aktivnosti tako da se osobito štiti sljedeće:

   (a) prava intelektualnog vlasništva i povjerljive poslovne informacije ili poslovne tajne fizičke ili pravne osobe, uključujući izvorni kôd, osim slučajeva iz članka 5. Direktive (EU) 2016/943 Europskog parlamenta i Vijeća[24];

   (b) učinkovita provedba ove Uredbe, posebice za potrebe inspekcija, istraga ili revizija;

   (c) interesi javne i nacionalne sigurnosti;

   (d) integritet kaznenih ili upravnih postupaka.

2. Ne dovodeći u pitanje stavak 1., informacije koje se povjerljivo razmjenjuju među tijelima za nadzor tržišta ili između tijela za nadzor tržišta i Komisije ne otkrivaju se bez prethodne suglasnosti tijela za nadzor tržišta od kojeg informacije potječu.

3. Stavci 1. i 2. ne utječu na prava i obveze Komisije, država članica i prijavljenih tijela u pogledu razmjene informacija i širenja upozorenja ni na obveze predmetnih osoba da pruže informacije na temelju kaznenog prava država članica.

4. Komisija i države članice mogu prema potrebi razmjenjivati osjetljive informacije s relevantnim tijelima trećih zemalja s kojima su sklopile bilateralne ili multilateralne sporazume o povjerljivosti kojima se jamči odgovarajuća razina zaštite.

Članak 53.

Sankcije

[24] Direktiva (EU) 2016/943 Europskog parlamenta i Vijeća od 8. lipnja 2016. o zaštiti neotkrivenih znanja i iskustva te poslovnih informacija (poslovne tajne) od nezakonitog pribavljanja, korištenja i otkrivanja (SL L 157, 15.6.2016., str. 1.).

1. Države članice utvrđuju pravila za sankcije koje se primjenjuju na gospodarske subjekte koji krše ovu Uredbu i poduzimaju sve potrebne mjere kako bi osigurale njihovu primjenu. Predviđene sankcije moraju biti učinkovite, proporcionalne i odvraćajuće.

2. Države članice bez odgode obavješćuju Komisiju o tim pravilima i tim mjerama te je bez odgode obavješćuju o svim naknadnim izmjenama koje na njih utječu.

3. Za nesukladnost s bitnim kibersigurnosnim zahtjevima utvrđenima u Prilogu I. i obvezama utvrđenima u člancima 10. i 11. izriču se upravne novčane kazne u iznosu do 15 000 000 EUR ili, ako je počinitelj povrede poduzeće, do 2,5 % njegova ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome koji je iznos veći.

4. Za nesukladnost s bilo kojim drugim obvezama iz ove Uredbe izriču se upravne novčane kazne u iznosu do 10 000 000 EUR ili, ako je počinitelj povrede poduzeće, do 2 % njegova ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome koji je iznos veći.

5. Za dostavljanje netočnih, nepotpunih ili obmanjujućih informacija prijavljenim tijelima i tijelima za nadzor tržišta kao odgovor na zahtjev izriču se upravne novčane kazne u iznosu do 5 000 000 EUR ili, ako je počinitelj povrede poduzeće, do 1 % njegova ukupnog godišnjeg prometa na svjetskoj razini za prethodnu financijsku godinu, ovisno o tome koji je iznos veći.

6. Pri odlučivanju o iznosu upravne novčane kazne u svakom pojedinom slučaju uzimaju se u obzir sve relevantne okolnosti specifične situacije i dužna se pozornost posvećuje sljedećem:

   (a) prirodi, težini i trajanju povrede te njezinim posljedicama;

   (b) eventualnim upravnim novčanim kaznama koje su druga tijela za nadzor tržišta već izrekla istom subjektu za sličnu povredu;

   (c) veličini i tržišnom udjelu subjekta koji je počinio povredu.

7. Tijela za nadzor tržišta koja izriču upravne novčane kazne dijele te informacije s tijelima za nadzor tržišta drugih država članica u okviru informacijskog i komunikacijskog sustava iz članka 34. Uredbe (EU) 2019/1020.

8. Svaka država članica utvrđuje pravila o tome mogu li se i u kojoj mjeri javnim tijelima te države članice izreći upravne novčane kazne.

9. Ovisno o pravnom sustavu država članica, pravila o upravnim novčanim kaznama mogu se primjenjivati tako da novčane kazne izriču nadležni nacionalni sudovi ili druga tijela, u skladu s nadležnostima utvrđenima na nacionalnoj razini u tim državama članicama. Primjena takvih pravila u tim državama članicama mora imati istovjetan učinak.

10. Upravne novčane kazne mogu se izreći, ovisno o okolnostima svakog pojedinog slučaja, uz sve druge korektivne ili restriktivne mjere koje tijela za nadzor tržišta primjenjuju za isti prekršaj.

POGLAVLJE VIII.

PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 54.

Izmjena Uredbe (EU) 2019/1020

U Prilogu I. Uredbi (EU) 2019/1020 dodaje se sljedeća točka:

„71. [Uredba XXX][Akt o kiberotpornosti]”.

Članak 55.

Prijelazne odredbe

1. Potvrde o EU ispitivanju tipa i odluke o odobrenju izdane u vezi s kibersigurnosnim zahtjevima za proizvode s digitalnim elementima koji podliježu drugom zakonodavstvu Unije o usklađivanju vrijede do [42 mjeseca nakon datuma stupanja na snagu ove Uredbe], osim ako isteknu prije tog datuma ili ako je drukčije utvrđeno u drugom zakonodavstvu Unije, u kojem slučaju vrijede koliko je navedeno u tom zakonodavstvu Unije.
2. Proizvodi s digitalnim elementima koji su stavljeni na tržište prije [datum početka primjene ove Uredbe iz članka 57.] podliježu zahtjevima iz ove Uredbe samo ako od tog datuma dođe do bitnih izmjena projekta ili namjene tih proizvoda.
3. Odstupajući od stavka 2., obveze utvrđene u članku 11. primjenjuju se na sve proizvode s digitalnim elementima obuhvaćene područjem primjene ove Uredbe koji su stavljeni na tržište prije [datum početka primjene ove Uredbe iz članka 57.].

Članak 56.

Evaluacija i preispitivanje

Najkasnije [36 mjeseci nakon datuma početka primjene ove Uredbe] i svake četiri godine nakon toga Komisija Europskom parlamentu i Vijeću podnosi izvješće o evaluaciji i preispitivanju ove Uredbe. Ta se izvješća objavljuju.

Članak 57.

Stupanje na snagu i primjena

Ova Uredba stupa na snagu dvadesetog dana od dana objave u *Službenom listu Europske unije*.

Primjenjuje se od [24 mjeseca od datuma stupanja na snagu ove Uredbe]. Međutim, članak 11. primjenjuje se od [12 mjeseci nakon datuma stupanja na snagu ove Uredbe].

Ova je Uredba u cijelosti obvezujuća i izravno se primjenjuje u svim državama članicama.

Sastavljeno u Bruxellesu,

Za Europski parlament	*Za Vijeće*
Predsjednica	*Predsjednik*

ZAKONODAVNI FINANCIJSKI IZVJEŠTAJ

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

1.2. Predmetna područja politike

1.3. Prijedlog/inicijativa odnosi se na:

1.4. Ciljevi

1.4.1. Općí ciljevi

1.4.2. Posebni ciljevi

1.4.3. Očekivani rezultati i učinak

1.4.4. Pokazatelji uspješnosti

1.5. Osnova prijedloga/inicijative

1.5.1. Zahtjevi koje treba ispuniti u kratkoročnom ili dugoročnom razdoblju, uključujući detaljan vremenski plan provedbe inicijative

1.5.2. Dodana vrijednost sudjelovanja Unije (može proizlaziti iz različitih čimbenika, npr. prednosti koordinacije, pravne sigurnosti, veće djelotvornosti ili komplementarnosti). Za potrebe ove točke „dodana vrijednost sudjelovanja Unije" vrijednost je koja proizlazi iz intervencije Unije i predstavlja dodatnu vrijednost u odnosu na vrijednost koju bi države članice inače ostvarile same.

1.5.3. Pouke iz prijašnjih sličnih iskustava

1.5.4. Usklađenost s višegodišnjim financijskim okvirom i moguće sinergije s drugim prikladnim instrumentima

1.5.5. Ocjena različitih dostupnih mogućnosti financiranja, uključujući mogućnost preraspodjele

1.6. Trajanje i financijski učinak prijedloga/inicijative

1.7. Predviđeni načini upravljanja

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

2.2. Sustavi upravljanja i kontrole

2.2.1. Obrazloženje načina upravljanja, mehanizama provedbe financiranja, načina plaćanja i predložene strategije kontrole

2.2.2. Informacije o utvrđenim rizicima i uspostavljenim sustavima unutarnje kontrole za ublažavanje rizika

2.2.3. Procjena i obrazloženje troškovne učinkovitosti kontrola (omjer troškova kontrole i vrijednosti sredstava kojima se upravlja) i procjena očekivane razine rizika od pogreške (pri plaćanju i pri zaključenju)

2.3. Mjere za sprečavanje prijevara i nepravilnosti

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslovi višegodišnjeg financijskog okvira i proračunske linije rashoda na koje prijedlog/inicijativa ima učinak

3.2. Procijenjeni financijski učinak prijedloga na odobrena sredstva

3.2.1. Sažetak procijenjenog učinka na odobrena sredstva za poslovanje

3.2.2. Procijenjeni rezultati financirani odobrenim sredstvima za poslovanje

3.2.3. Sažetak procijenjenog učinka na administrativna odobrena sredstva

3.2.4. Usklađenost s aktualnim višegodišnjim financijskim okvirom

3.2.5. Doprinos trećih strana

3.3. Procijenjeni učinak na prihode

ZAKONODAVNI FINANCIJSKI IZVJEŠTAJ

1. OKVIR PRIJEDLOGA/INICIJATIVE

1.1. Naslov prijedloga/inicijative

Prijedlog uredbe o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima (Akt o kiberotpornosti)

1.2. Predmetna područja politike

Komunikacijske mreže, sadržaji i tehnologije

1.3. Prijedlog/inicijativa odnosi se na:

× **novo djelovanje**

☐ **novo djelovanje nakon pilot-projekta/pripremnog djelovanja**[37]

☐ **produženje postojećeg djelovanja**

☐ **spajanje ili preusmjeravanje jednog ili više djelovanja u drugo/novo djelovanje**

1.4. Ciljevi

1.4.1. Opći ciljevi

Prijedlog uključuje dva glavna cilja kojima se nastoji osigurati ispravno funkcioniranje unutarnjeg tržišta: 1. **stvoriti uvjete za razvoj sigurnih proizvoda s digitalnim elementima** tako što će se urediti da se hardverski i softverski proizvodi stavljaju na tržište s manje ranjivosti i da proizvođači ozbiljno shvaćaju sigurnost tijekom cijelog životnog ciklusa proizvoda; i 2. **stvoriti uvjete koji korisnicima omogućuju da proizvode s digitalnim elementima odabiru i rabe vodeći računa o kibersigurnosti**.

1.4.2. Posebni ciljevi

Utvrđena su **četiri posebna cilja** Prijedloga: i. osigurati da proizvođači povećavaju sigurnost proizvoda s digitalnim elementima od faze projektiranja i razvoja te tijekom cijelog životnog ciklusa, ii. stvoriti usklađen okvir za kibersigurnost kako bi ga se proizvođači hardvera i softvera lakše pridržavali, iii. povećati transparentnost sigurnosnih svojstava proizvoda s digitalnim elementima i iv. poduzećima i potrošačima omogućiti sigurnu uporabu proizvoda s digitalnim elementima.

Očekivani rezultati i učinak

Navesti očekivane učinke prijedloga/inicijative na ciljane korisnike/skupine.

Prijedlog bi donio znatne koristi raznim dionicima. Kad je riječ o poduzećima, njime bi se spriječila različita sigurnosna pravila za proizvode s digitalnim elementima i smanjili troškovi usklađivanja s povezanim zakonodavstvom o kibersigurnosti. Smanjili bi se broj kiberincidenata, troškovi rješavanja incidenata i šteta za ugled. Procjenjuje se da bi inicijativa cijelom EU-u mogla smanjiti troškove od incidenata

[37] Kako je navedeno u članku 58. stavku 2. točkama (a) ili (b) Financijske uredbe.

koji pogađaju poduzeća za otprilike 180 do 290 milijardi EUR godišnje[38]. Dovela bi do povećanja prometa zbog veće prihvaćenosti proizvoda s digitalnim elementima. Poduzećima bi povećala globalni ugled, pa bi potražnja porasla i izvan EU-a. Korisnicima bi najpoželjnija opcija povećala transparentnost sigurnosnih svojstava i olakšala uporabu proizvoda s digitalnim elementima. Potrošači i građani koristi bi imali i od bolje zaštite temeljnih prava kao što su pravo na privatnost i zaštitu podataka.

Prijedlogom bi se dodali troškovi usklađivanja i provedbe za poduzeća, prijavljena tijela i javna tijela, uključujući akreditacijska tijela i tijela za nadzor tržišta. Programerima softvera i proizvođačima hardvera dodat će izravne troškove usklađivanja za nove sigurnosne zahtjeve, ocjenjivanje sukladnosti, dokumentiranje i obveze izvješćivanja, pa će ukupni troškovi usklađivanja iznositi najviše otprilike 29 milijardi EUR za procijenjenu tržišnu vrijednost od 1 485 milijardi EUR prometa[39]. Korisnici, uključujući poslovne korisnike, potrošače i građane, možda će se suočiti s višim cijenama proizvoda s digitalnim elementima. To, međutim, treba promatrati u kontekstu prethodno opisanih znatnih koristi.

1.4.3. Pokazatelji uspješnosti

Navesti pokazatelje za praćenje napretka i postignuća

Kako bi se testiralo povećavaju li proizvođači sigurnost svojih proizvoda s digitalnim elementima od faze projektiranja i razvoja te tijekom cijelog životnog ciklusa tih proizvoda, u obzir bi se moglo uzeti nekoliko pokazatelja. Oni bi mogli uključivati broj ozbiljnih incidenata u Uniji prouzročenih ranjivostima, udio proizvođača hardvera i softvera koji primjenjuju sustavni životni ciklus razvoja sigurnih proizvoda, kvalitativnu analizu sigurnosti proizvoda s digitalnim elementima, kvantitativnu i kvalitativnu ocjenu baza podataka o ranjivostima, učestalost sigurnosnih zakrpa koje proizvođači stavljaju na raspolaganje ili prosječan broj dana između otkrića ranjivosti i pružanja sigurnosnih zakrpa.

Pokazatelj usklađenog okvira za kibersigurnost mogao bi biti nedostatak ciljanog nacionalnog zakonodavstva o kibersigurnosti za pojedine proizvode.

Pokazatelj povećane transparentnosti u pogledu sigurnosnih svojstava proizvoda s digitalnim elementima mogao bi biti udio proizvoda s digitalnim elementima koji se isporučuju s informacijama o sigurnosnim svojstvima. Nadalje, udio proizvoda s digitalnim elementima koji se isporučuju s korisničkim uputama o sigurnoj uporabi mogao bi služiti kao pokazatelj je li organizacijama i potrošačima omogućena sigurna uporaba proizvoda s digitalnim elementima.

Kad je riječ o praćenju učinka Uredbe, u tu bi se svrhu razmotrili određeni pokazatelji koje će procijeniti Komisija, po potrebi uz potporu ENISA-e. Uspješnost horizontalnih kibersigurnosnih zahtjeva mogla bi se, ovisno o operativnom cilju koji se nastoji postići, ocjenjivati na temelju nekih od sljedećih pokazatelja za praćenje:

Za ocjenjivanje razine kibersigurnosti proizvoda s digitalnim elementima:

[38] Vidjeti [Radni dokument službi Komisije o izvješću o procjeni učinka priloženom Uredbi o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima]

[39] Vidjeti [Radni dokument službi Komisije o izvješću o procjeni učinka priloženom Uredbi o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima]

– statistički podaci o incidentima koji utječu na proizvode s digitalnim elementima i način na koji se njima upravljalo te njihova kvalitativna analiza. Takve bi podatke mogla prikupiti i procijeniti Komisija, uz potporu ENISA-e;

– evidencija poznatih ranjivosti i analiza načina na koji se njima upravljalo. Takvu bi analizu mogla provoditi ENISA na temelju europske baze podataka o ranjivostima uspostavljene [Direktivom XXX/XXXX (NIS2)];

– ankete među proizvođačima hardvera i softvera radi praćenje napretka.

Za ocjenjivanje razine informacija o sigurnosnim obilježjima, sigurnosnoj podršci, kraju životnog vijeka i obvezi postupanja s dužnom pažnjom: rezultati anketa koje će među korisnicima i poduzećima provesti Komisija, uz potporu ENISA-e.

Za ocjenjivanje provedbe Komisija bi se nastojala pobrinuti da se ocjenjivanja sukladnosti djelotvorno provode. U tu će se svrhu izdati zahtjev za normizaciju te će se pratiti njegova provedba. Komisija će ujedno provjeriti kapacitete prijavljenih tijela i, prema potrebi, certifikacijskih tijela.

Kad je riječ o primjeni, Komisija će na temelju izvješća država članica provjeriti da se nacionalne inicijative ne odnose na aspekte obuhvaćene Uredbom.

1.5. Osnova prijedloga/inicijative

1.5.1. Zahtjevi koje treba ispuniti u kratkoročnom ili dugoročnom razdoblju, uključujući detaljan vremenski plan provedbe inicijative

Uredba bi se trebala početi u potpunosti primjenjivati 24 mjeseca nakon stupanja na snagu. Međutim, elementi strukture upravljanja trebali bi biti uspostavljeni prije toga. Točnije, države članice moraju imenovati postojeća tijela i/ili uspostaviti nova tijela za zadaće utvrđene zakonodavstvom.

1.5.2. Dodana vrijednost sudjelovanja Unije (može proizlaziti iz različitih čimbenika, npr. prednosti koordinacije, pravne sigurnosti, veće djelotvornosti ili komplementarnosti). Za potrebe ove točke „dodana vrijednost sudjelovanja Unije" vrijednost je koja proizlazi iz intervencije Unije i predstavlja dodatnu vrijednost u odnosu na vrijednost koju bi države članice inače ostvarile same.

Zbog izrazite prekogranične prirode kibersigurnosti i sve češćih incidenata čiji se učinci prelijevaju preko granica te na druge sektore i proizvode države članice ne mogu same učinkovito postići te ciljeve. Zbog globalne prirode tržišta proizvoda s digitalnim elementima isti proizvod s digitalnim elementima ima iste sigurnosne rizike na državnim područjima različitih država članica. Rascjepkan okvir od potencijalno različitih nacionalnih pravila kakav se počeo pojavljivati mogao bi ugroziti otvoreno i konkurentno jedinstveno tržište proizvoda s digitalnim elementima. Dakle, zajedničko djelovanje na razini EU-a potrebno je radi povećanja povjerenja korisnika i privlačnosti proizvoda s digitalnim elementima iz EU-a.. Ono bi pogodovalo i unutarnjem tržištu pružanjem pravne sigurnosti i stvaranjem jednakih uvjeta za dobavljače proizvoda s digitalnim elementima.

1.5.3. Pouke iz prijašnjih sličnih iskustava

Akt o kiberotpornosti prvi je propis kojim se uvode kibersigurnosni zahtjevi za stavljanje na tržište proizvoda s digitalnim elementima. Temelji se, međutim, na novom zakonodavnom okviru i iskustvu iz provedbe postojećeg zakonodavstva Unije

o usklađivanju raznih proizvoda, osobito kad je riječ o pripremi provedbe, uključujući aspekte kao što je priprema usklađenih normi.

1.5.4. Usklađenost s višegodišnjim financijskim okvirom i moguće sinergije s drugim prikladnim instrumentima

U Uredbi o horizontalnim kibersigurnosnim zahtjevima za proizvode s digitalnim elementima definirani su novi kibersigurnosni zahtjevi za sve proizvode s digitalnim elementima koji se stavljaju na tržište EU-a, a koji nadilaze sve zahtjeve predviđene postojećim zakonodavstvom. Istodobno se Prijedlog zasniva na postojećem okruženju novog zakonodavnog okvira. Dakle, Prijedlog bi se temeljio na postojećim strukturama i postupcima novog zakonodavnog okvira kao što su suradnja prijavljenih tijela i nadzor tržišta, moduli za ocjenjivanje sukladnosti, razvoj usklađenih normi. Novi prijedlog oslanjao bi se i na neke strukture razvijene u skladu s drugim propisima o kibersigurnosti kao što je Direktiva 2016/1148 (Direktiva NIS), odnosno [Direktiva XXX/XXXX (NIS2)] ili Uredba 2019/881 (Akt o kibersigurnosti).

1.5.5. Ocjena različitih dostupnih mogućnosti financiranja, uključujući mogućnost preraspodjele

Područja djelovanja kojima bi ENISA trebala upravljati odgovaraju njezinu trenutačnom mandatu i općim zadaćama. Ta područja djelovanja možda će zahtijevati posebne profile ili utvrđivanje novih zadaća, ali takvi zahtjevi ne bi bili znatni i mogu se apsorbirati postojećim resursima ENISA-e i riješiti preraspodjelom ili povezivanjem raznih zadaća. Na primjer, jedno od glavnih područja djelovanja dodijeljenih ENISA-i odnosi se na prikupljanje i obradu obavijesti proizvođača o iskorištenim ranjivostima proizvoda. [Direktivom XXX/XXXX (NIS2)] ENISA je već zadužena za uspostavu europske baze podataka o ranjivostima u kojoj se javno poznate ranjivosti mogu objaviti i registrirati, na dobrovoljnoj osnovi, kako bi se korisnicima omogućilo da poduzmu odgovarajuće mjere ublažavanja. Resursi dodijeljeni u tu svrhu mogli bi se iskoristiti i za nove spomenute zadaće koje se odnose na obavijesti o ranjivostima proizvoda. Tako bi se mogli učinkovito koristiti postojeći resursi i stvoriti potrebne sinergije između takvih zadaća na temelju kojih bi ENISA mogla bolje analizirati kibersigurnosne rizike i prijetnje.

1.6. Trajanje i financijski učinak prijedloga/inicijative

☐ **ograničeno trajanje**

– ☐ na snazi od [DD/MM]GGGG do [DD/MM]GGGG

– ☐ financijski učinak od GGGG do GGGG za odobrena sredstva za preuzete obveze i od GGGG do GGGG za odobrena sredstva za plaćanje

× **neograničeno trajanje**

– provedba s početnim razdobljem od 2025.,

– nakon čega slijedi redovna provedba.

1.7. Predviđeni načini upravljanja[40]

☐ **Izravno upravljanje** koje provodi Komisija

– × putem svojih službi, uključujući osoblje u delegacijama Unije

– ☐ putem izvršnih agencija

☐ **Podijeljeno upravljanje** s državama članicama

☐ **Neizravno upravljanje** povjeravanjem zadaća izvršenja proračuna:

– ☐ trećim zemljama ili tijelima koja su one odredile

– ☐ međunarodnim organizacijama i njihovim agencijama (navesti)

– ☐ EIB-u i Europskom investicijskom fondu

– ☐ tijelima iz članaka 70. i 71. Financijske uredbe

– ☐ tijelima javnog prava

– ☐ tijelima uređenima privatnim pravom koja pružaju javne usluge, u mjeri u kojoj su im dana odgovarajuća financijska jamstva

– ☐ tijelima uređenima privatnim pravom države članice kojima je povjerena provedba javno-privatnog partnerstva i kojima su dana odgovarajuća financijska jamstva

– ☐ osobama kojima je povjerena provedba određenih djelovanja u području ZVSP-a u skladu s glavom V. UEU-a i koje su navedene u odgovarajućem temeljnom aktu.

– *Ako je navedeno više načina upravljanja, potrebno je pojasniti u odjeljku „Napomene”.*

Napomene

Ovom se Uredbom određena djelovanja dodjeljuju ENISA-i u skladu s njezinim trenutačnim mandatom, a posebno člankom 3. stavkom 2. Uredbe 2019/881 kojim je utvrđeno da ENISA treba obavljati zadaće koje su joj dodijeljene pravnim aktima Unije kojima su utvrđene mjere za usklađivanje zakona i drugih propisa država članica koji se odnose na kibersigurnost. Točnije, ENISA bi od proizvođača trebala primati obavijesti o iskorištenim ranjivostima proizvodâ s digitalnim elementima te o incidentima koji utječu na sigurnost tih proizvoda. ENISA bi te obavijesti trebala prosljeđivati relevantnim CSIRT-ovima ili relevantnim

[40] Informacije o načinima upravljanja i upućivanja na Financijsku uredbu dostupni su na internetskim stranicama BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx

jedinstvenim kontaktnim točkama država članica imenovanima u skladu s člankom [članak X.] Direktive [Direktiva XXX/XXXX (NIS2)] te obavijestiti nadležna tijela za nadzor tržišta. Na temelju informacija koje prikupi ENISA bi trebala izraditi dvogodišnje tehničko izvješće o novim trendovima u području kibersigurnosnih rizika proizvoda s digitalnim elementima i dostaviti ga skupini za suradnju u području sigurnosti mrežnih i informacijskih sustava. Nadalje, imajući u vidu ENISA-inu stručnost, prikupljene informacije i analize prijetnji, ona bi mogla pružati potporu procesu provedbe ove Uredbe predlaganjem zajedničkih aktivnosti koje bi na temelju naznaka ili informacija povezanih s potencijalnom nesukladnošću proizvoda s digitalnim elementima s ovom Uredbom provodila tijela za nadzor tržišta u nekoliko država članica ili utvrditi kategorije proizvoda za koje bi trebalo organizirati istodobne koordinirane kontrolne mjere. U iznimnim okolnostima, kad je potrebna brza intervencija kako bi se očuvalo dobro funkcioniranje unutarnjeg tržišta, ENISA bi, na zahtjev Komisije, trebala moći provoditi evaluacije povezane sa specifičnim proizvodima s digitalnim elementima koji predstavljaju znatan kibersigurnosni rizik.

Procijenjeno je da za sve te zadaće treba otprilike 4,5 EPRV-a iz postojećih resursa ENISA-e, pri čemu bi se te zadaće oslanjale na stručni i pripremni rad koji ENISA trenutačno obavlja, među ostalim u okviru pružanja potpore za predstojeću provedbu [Direktiva XXX/XXXX (NIS2)] za koju su resursi ENISA-e dopunjeni.

2. MJERE UPRAVLJANJA

2.1. Pravila praćenja i izvješćivanja

Navesti učestalost i uvjete.

Najkasnije 36 mjeseci nakon datuma početka primjene ove Uredbe i svake četiri godine nakon toga Komisija će Europskom parlamentu i Vijeću podnijeti izvješće o njezinoj evaluaciji i preispitivanju. Ta se izvješća objavljuju.

2.2. Sustavi upravljanja i kontrole

2.2.1. Obrazloženje načina upravljanja, mehanizama provedbe financiranja, načina plaćanja i predložene strategije kontrole

Ovom Uredbom uspostavlja se nova politika u pogledu usklađenih kibersigurnosnih zahtjeva za proizvode s digitalnim elementima koji se stavljaju na unutarnje tržište tijekom njihova cijelog životnog ciklusa. Nakon donošenja pravnog akta Komisija će od europskih tijela za normizaciju zatražiti da izrade norme.

Kako bi mogle obavljati te nove zadaće, službama Komisije potrebno je osigurati odgovarajuća sredstva. Procjenjuje se da će provedba nove Uredbe zahtijevati 7 EPRV-a (od kojih jedan UNS) za obavljanje sljedećih zadaća:

- priprema zahtjeva za normizaciju i/ili zajedničkih specifikacija putem provedbenih akata u slučaju neuspješnog postupka normizacije,
- priprema delegiranog akta [u roku od 12 mjeseci od stupanja na snagu Uredbe] kojim se utvrđuju definicije ključnih proizvoda s digitalnim elementima,
- potencijalna priprema delegiranih akata za ažuriranje popisa ključnih proizvoda I. i II. razreda, utvrđivanje je li potrebno ograničenje ili izuzeće za proizvode s digitalnim elementima obuhvaćene drugim pravilima Unije kojima se utvrđuju zahtjevi za postizanje iste razine zaštite kao i ovom Uredbom, uvođenje obveze certifikacije određenih visokorizičnih proizvoda s digitalnim elementima na temelju kriterija utvrđenih ovom Uredbom, određivanje minimalnog sadržaja EU izjave o sukladnosti i dodatnih elemenata koje treba uključiti u tehničku dokumentaciju,
- potencijalna priprema provedbenih akata o formatu ili elementima obveza izvješćivanja, popisu softverskog materijala, zajedničkim specifikacijama ili stavljanju oznake CE,
- potencijalna priprema brze intervencije za uvođenje korektivnih ili restriktivnih mjera u iznimnim okolnostima radi očuvanja dobrog funkcioniranja unutarnjeg tržišta, uključujući pripremu provedbenog akta,
- organizacija i koordinacija prijavljivanja prijavljenih tijela koje provode države članice i koordinacija prijavljenih tijela,
- podupiranje koordinacije tijela za nadzor tržišta država članica.

2.2.2. Informacije o utvrđenim rizicima i uspostavljenim sustavima unutarnje kontrole za ublažavanje rizika

Kako bi se osiguralo da prijavljena tijela i tijela za nadzor tržišta razmjenjuju informacije i dobro surađuju, Komisija je zadužena za njihovu koordinaciju. Kako bi

se osiguralo tehničko stručno znanje i stručno znanje u području tržišta, uspostavit će se stručna skupina.

2.2.3. Procjena i obrazloženje troškovne učinkovitosti kontrola (omjer troškova kontrole i vrijednosti sredstava kojima se upravlja) i procjena očekivane razine rizika od pogreške (pri plaćanju i pri zaključenju)

2.3. S obzirom na nisku vrijednost transakcija (npr. nadoknada putnih troškova delegatu za sastanak), čini se da su standardni postupci kontrole dostatni za rashode za sastanke. Mjere za sprečavanje prijevara i nepravilnosti

Navesti postojeće ili predviđene mjere za sprečavanje i zaštitu, npr. iz strategije za borbu protiv prijevara.

Postojećim mjerama za sprečavanje prijevara za koje je nadležna Komisija pokrit će se dodatna odobrena sredstva potrebna za ovu Uredbu.

3. PROCIJENJENI FINANCIJSKI UČINAK PRIJEDLOGA/INICIJATIVE

3.1. Naslovi višegodišnjeg financijskog okvira i proračunske linije rashoda na koje prijedlog/inicijativa ima učinak

- Postojeće proračunske linije

Sustav

- Zatražene nove proračunske linije

Nije primjenjivo

3.2. Procijenjeni financijski učinak prijedloga na odobrena sredstva

3.2.1. Sažetak procijenjenog učinka na odobrena sredstva za poslovanje

– ☑ Za prijedlog/inicijativu nisu potrebna odobrena sredstva za poslovanje.

– ☐ Za prijedlog/inicijativu potrebna su sljedeća odobrena sredstva za poslovanje:

U milijunima EUR (do 3 decimalna mjesta)

Naslov višegodišnjeg financijskog okvira	Broj	

GU: <…….>			Godina **N**[41]	Godina **N+1**	Godina **N+2**	Godina **N+3**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)			**UKUPNO**
• Odobrena sredstva za poslovanje										
Proračunska linija[42]	Obveze	(1a)								
	Plaćanja	(2a)								
Proračunska linija	Obveze	(1b)								
	Plaćanja	(2b)								
Administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe[43]										
Proračunska linija		(3)								
UKUPNA odobrena sredstva za GU <…….>	Obveze	=1a+1b +3								
	Plaćanja	=2a+2b								

41 Godina N je godina početka provedbe prijedloga/inicijative. Umjesto „N” upisati predviđenu prvu godinu provedbe (na primjer: 2021.) Isto vrijedi i za ostale godine.

42 Prema službenoj proračunskoj nomenklaturi.

43 Tehnička i/ili administrativna pomoć i rashodi za potporu provedbi programa i/ili djelovanja EU-a (prijašnje linije „BA”), neizravno istraživanje, izravno istraživanje.

		+3								

• UKUPNA odobrena sredstva za poslovanje	Obveze	(4)								
	Plaćanja	(5)								
• UKUPNA administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe		(6)								
UKUPNA odobrena sredstva iz NASLOVA <….> višegodišnjeg financijskog okvira	Obveze	=4+6								
	Plaćanja	=5+6								

Ako prijedlog/inicijativa utječe na više od jednog naslova za poslovanje, ponovite prethodni odjeljak:

• UKUPNA odobrena sredstva za poslovanje (svi naslovi za poslovanje)	Obveze	(4)								
	Plaćanja	(5)								
UKUPNA administrativna odobrena sredstva koja se financiraju iz omotnice za posebne programe (svi naslovi za poslovanje)		(6)								
UKUPNA odobrena sredstva iz NASLOVA 1.–6. višegodišnjeg financijskog okvira (referentni iznos)	Obveze	=4+6								
	Plaćanja	=5+6								

Naslov višegodišnjeg financijskog okvira	**7**	„Administrativni rashodi”

U ovaj se dio unose „administrativni proračunski podaci”, koji se najprije unose u prilog zakonodavnom financijskom izvještaju (Prilog V. internim pravilima), koji se učitava u sustav DECIDE za potrebe savjetovanja među službama.

U milijunima EUR (do 3 decimalna mjesta)

		Godina **2024.**	Godina **2025.**	Godina **2026.**	Godina **2027.**	**UKUPNO**
GU: CNECT						
• Ljudski resursi		1,030	1,030	1,030	1,030	**4,120**
• Ostali administrativni rashodi		**0,222**	**0,222**	**0,222**	**0,222**	**0,888**
UKUPNO GU CNECT	Odobrena sredstva	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

UKUPNA odobrena sredstva iz NASLOVA 7. višegodišnjeg financijskog okvira	(ukupne obveze = ukupna plaćanja)	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

U milijunima EUR (do 3 decimalna mjesta)

		Godina **2024.**	Godina **2025.**	Godina **2026.**	Godina **2027.**	**UKUPNO**
UKUPNA odobrena sredstva iz NASLOVA 1.–7. višegodišnjeg financijskog okvira	Obveze	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**
	Plaćanja	**1,252**	**1,252**	**1,252**	**1,252**	**5,008**

3.2.2. Procijenjeni rezultati financirani odobrenim sredstvima za poslovanje

Odobrena sredstva za preuzimanje obveza u milijunima EUR (do 3 decimalna mjesta)

Navesti ciljeve i rezultate ⇩			Godina **N**		Godina **N+1**		Godina **N+2**		Godina **N+3**		Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)						**UKUPNO**	
	REZULTATI																	
	Vrsta [44]	Prosječni trošak	br.	Trošak	br.	Trošak	br.	Trošak	br.	Trošak	br.	Trošak	br.	Trošak	br.	Trošak	Ukupni broj	Ukupni trošak
POSEBNI CILJ br. 1[45]…																		
– rezultat																		
– rezultat																		
– rezultat																		
Međuzbroj za posebni cilj br. 1																		
POSEBNI CILJ br. 2...																		
– rezultat																		
Međuzbroj za posebni cilj br. 2																		
UKUPNO																		

[44] Rezultati se odnose na proizvode i usluge koji se isporučuju (npr.: broj financiranih studentskih razmjena, kilometri izgrađenih prometnica itd.).

[45] Kako je opisan u odjeljku 1.4.2. „Posebni ciljevi…".

3.2.3. Sažetak procijenjenog učinka na administrativna odobrena sredstva

– ☐ Za prijedlog/inicijativu nisu potrebna administrativna odobrena sredstva.

– ☑ Za prijedlog/inicijativu potrebna su sljedeća administrativna odobrena sredstva:

U milijunima EUR (do 3 decimalna mjesta)

	Godina **2024.**	Godina **2025.**	Godina **2026.**	Godina **2027.**	
NASLOV 7. višegodišnjeg financijskog okvira					
Ljudski resursi	1,030	1,030	1,030	1,030	**4,120**
Ostali administrativni rashodi	0,222	0,222	0,222	0,222	**0,888**
Međuzbroj za NASLOV 7. višegodišnjeg financijskog okvira	1,252	1,252	1,252	1,252	**5,008**

Izvan NASLOVA 7.[46] **višegodišnjeg financijskog okvira**					
Ljudski resursi					
Ostali administrativni rashodi					
Međuzbroj izvan NASLOVA 7. višegodišnjeg financijskog okvira					

UKUPNO	1,252	1,252	1,252	1,252	**5,008**

Potrebna odobrena sredstva za ljudske resurse i ostale administrativne rashode pokrit će se odobrenim sredstvima glavne uprave koja su već dodijeljena za upravljanje djelovanjem i/ili su preraspodijeljena unutar glavne uprave te, prema potrebi, dodatnim sredstvima koja se mogu dodijeliti nadležnoj glavnoj upravi u okviru godišnjeg postupka dodjele sredstava uzimajući u obzir proračunska ograničenja.

[46] Tehnička i/ili administrativna pomoć i rashodi za potporu provedbi programa i/ili djelovanja EU-a (prijašnje linije „BA”), neizravno istraživanje, izravno istraživanje.

3.2.3.1. Procijenjene potrebe u pogledu ljudskih resursa

– ☐ Za prijedlog/inicijativu nisu potrebni ljudski resursi.

– ☑ Za prijedlog/inicijativu potrebni su sljedeći ljudski resursi:

Procjenu navesti u ekvivalentima punog radnog vremena

		Godina **2024.**	Godina **2025.**	Godina **2026.**	Godina **2027.**
20 01 02 01 (sjedište i predstavništva Komisije)		6	6	6	6
20 01 02 03 (delegacije)					
01 01 01 01 (neizravno istraživanje)					
01 01 01 11 (izravno istraživanje)					
Druge proračunske linije (navesti)					
• **Vanjsko osoblje (u ekvivalentu punog radnog vremena: EPRV)**[47]					
20 02 01 (UO, UNS, UsO iz „globalne omotnice”)		1	1	1	1
20 02 03 (UO, LO, UNS, UsO i MSD u delegacijama)					
XX 01 xx **yy zz** [48]	– u sjedištima				
	– u delegacijama				
01 01 01 02 (UO, UNS, UsO – neizravno istraživanje)					
01 01 01 12 (UO, UNS, UsO – izravno istraživanje)					
Druge proračunske linije (navesti)					
UKUPNO		**7**	**7**	**7**	**7**

XX se odnosi na odgovarajuće područje politike ili glavu proračuna.

Potrebe za ljudskim resursima pokrit će se osobljem glavne uprave kojemu je već povjereno upravljanje djelovanjem i/ili koje je preraspoređeno unutar glavne uprave te, prema potrebi, resursima koji se mogu dodijeliti nadležnoj glavnoj upravi u okviru godišnjeg postupka dodjele sredstava uzimajući u obzir proračunska ograničenja.

Opis zadaća:

Dužnosnici i privremeno osoblje 6 EPRV-a x 157 000 EUR/godišnje = 942 000 EUR	Kako je opisano u odjeljku 2.2.1.: – priprema zahtjeva za normizaciju i/ili zajedničkih specifikacija putem provedbenih akata u slučaju neuspješnog postupka normizacije, – priprema delegiranog akta [u roku od 12 mjeseci od stupanja na snagu Uredbe] kojim se utvrđuju definicije ključnih proizvoda s digitalnim elementima, – potencijalna priprema delegiranih akata za ažuriranje popisa ključnih proizvoda I. i II. razreda, utvrđivanje je li potrebno ograničenje ili izuzeće za proizvode s digitalnim elementima obuhvaćene drugim pravilima Unije kojima se utvrđuju zahtjevi za postizanje iste razine zaštite kao i ovom Uredbom, uvođenje obveze certifikacije određenih visokorizičnih proizvoda s digitalnim elementima na temelju kriterija utvrđenih ovom Uredbom, određivanje minimalnog sadržaja EU izjave o sukladnosti i dodatnih elemenata koje treba uključiti u tehničku dokumentaciju, – potencijalna priprema provedbenih akata o formatu ili elementima obveza izvješćivanja, popisu softverskog materijala, zajedničkim specifikacijama ili

[47] UO = ugovorno osoblje; LO = lokalno osoblje; UNS = upućeni nacionalni stručnjaci; UsO = ustupljeno osoblje; MSD = mladi stručnjaci u delegacijama.

[48] U okviru gornje granice za vanjsko osoblje iz odobrenih sredstava za poslovanje (prijašnje linije „BA”).

	stavljanju oznake CE, – potencijalna priprema brze intervencije za uvođenje korektivnih ili restriktivnih mjera u iznimnim okolnostima radi očuvanja dobrog funkcioniranja unutarnjeg tržišta, uključujući pripremu provedbenog akta, – organizacija i koordinacija prijavljivanja prijavljenih tijela koje provode države članice i koordinacija prijavljenih tijela, – podupiranje koordinacije tijela za nadzor tržišta država članica.
Vanjsko osoblje 1 UNS x 88 000 EUR/godišnje	Kako je opisano u odjeljku 2.2.1.: – priprema zahtjeva za normizaciju i/ili zajedničkih specifikacija putem provedbenih akata u slučaju neuspješnog postupka normizacije, – priprema delegiranog akta [u roku od 12 mjeseci od stupanja na snagu Uredbe] kojim se utvrđuju definicije ključnih proizvoda s digitalnim elementima, – potencijalna priprema delegiranih akata za ažuriranje popisa ključnih proizvoda razreda I. i II., utvrđivanje je li potrebno ograničenje ili izuzeće za proizvode s digitalnim elementima obuhvaćene drugim pravilima Unije kojima se utvrđuju zahtjevi za postizanje iste razine zaštite kao i ovom Uredbom, uvođenje obveze certifikacije određenih visokorizičnih proizvoda s digitalnim elementima na temelju kriterija utvrđenih ovom Uredbom, određivanje minimalnog sadržaja EU izjave o sukladnosti i dodatnih elemenata koje treba uključiti u tehničku dokumentaciju, – potencijalna priprema provedbenih akata o formatu ili elementima obveza izvješćivanja, popisu softverskog materijala, zajedničkim specifikacijama ili stavljanju oznake CE, – potencijalna priprema brze intervencije za uvođenje korektivnih ili restriktivnih mjera u iznimnim okolnostima radi očuvanja dobrog funkcioniranja unutarnjeg tržišta, uključujući pripremu provedbenog akta, – organizacija i koordinacija prijavljivanja prijavljenih tijela koje provode države članice i koordinacija prijavljenih tijela, – podupiranje koordinacije tijela za nadzor tržišta država članica.

3.2.4. Usklađenost s aktualnim višegodišnjim financijskim okvirom

U prijedlogu/inicijativi:

– x može se u potpunosti financirati preraspodjelom unutar relevantnog naslova višegodišnjeg financijskog okvira (VFO).

Nije potrebno reprogramiranje.

– ☐ zahtijeva upotrebu nedodijeljene razlike u okviru relevantnog naslova VFO-a i/ili upotrebu posebnih instrumenata kako su definirani u Uredbi o VFO-u.

–

– ☐ zahtijeva reviziju VFO-a.

–

3.2.5. Doprinos trećih strana

U prijedlogu/inicijativi:

– x ne predviđa se sudjelovanje trećih strana u sufinanciranju.

– ☐ predviđa se sudjelovanje trećih strana u sufinanciranju prema sljedećoj procjeni:

Odobrena sredstva u milijunima EUR (do 3 decimalna mjesta)

	Godina **N**[49]	Godina **N+1**	Godina **N+2**	Godina **N+3**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)			Ukupno
Navesti tijelo koje sudjeluje u financiranju								
UKUPNO sufinancirana odobrena sredstva								

[49] Godina N je godina početka provedbe prijedloga/inicijative. Umjesto „N” upisati predviđenu prvu godinu provedbe (na primjer: 2021.) Isto vrijedi i za ostale godine.

3.3. Procijenjeni učinak na prihode

– ☐ Prijedlog/inicijativa nema financijski učinak na prihode.

– ☐ Prijedlog/inicijativa ima sljedeći financijski učinak:

  – ☐ na vlastita sredstva

  – ☐ na ostale prihode

  – navesti jesu li prihodi namijenjeni proračunskim linijama rashoda ☐

U milijunima EUR (do 3 decimalna mjesta)

Proračunska linija prihoda:	Odobrena sredstva dostupna za tekuću financijsku godinu	Učinak prijedloga/inicijative[50]						
		Godina **N**	Godina **N+1**	Godina **N+2**	Godina **N+3**	Unijeti onoliko godina koliko je potrebno za prikaz trajanja učinka (vidjeti točku 1.6.)		
Članak …….								

Za namjenske prihode navesti odgovarajuće proračunske linije rashoda.

Ostale napomene (npr. metoda/formula za izračun učinka na prihode ili druge informacije)

[50] Kad je riječ o tradicionalnim vlastitim sredstvima (carine, pristojbe na šećer) navedeni iznosi moraju biti neto iznosi, to jest bruto iznosi nakon odbitka od 20 % na ime troškova naplate.