2024/2847

20.11.2024.

UREDBA (EU) 2024/2847 EUROPSKOG PARLAMENTA I VIJEĆA

od 23. listopada 2024.

o horizontalnim zahtjevima u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima i o izmjeni uredbi (EU) br. 168/2013 i (EU) 2019/1020 te Direktive (EU) 2020/1828 (Akt o kibernetičkoj otpornosti)

(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]),

nakon savjetovanja s Odborom regija,

u skladu s redovnim zakonodavnim postupkom ([2]),

budući da:

(1) Kibernetička sigurnost jedan je od ključnih izazova za Uniju. Broj i raznolikost povezanih uređaja eksponencijalno će rasti u nadolazećim godinama. Kibernetički napadi tema su od javnog interesa jer imaju kritičan učinak ne samo na gospodarstvo Unije nego i na demokraciju te na sigurnost i zdravlje potrošača. Stoga je potrebno osnažiti Unijin pristup kibernetičkoj sigurnosti, odgovoriti na pitanjem kibernetičke otpornosti na razini Unije te poboljšati funkcioniranje unutarnjeg tržišta utvrđivanjem jedinstvenog pravnog okvira za bitne zahtjeve u pogledu kibernetičke sigurnosti koji se odnose na stavljanje na tržište Unije proizvoda s digitalnim elementima. Trebalo bi odgovoriti na dva glavna problema koji uzrokuju dodatne troškove za korisnike i društvo: nisku razinu kibernetičke sigurnosti proizvoda s digitalnim elementima koja se odražava u raširenim ranjivostima te nedovoljnim i neredovitim sigurnosnim ažuriranjima za njihovo rješavanje, te nedovoljno razumijevanje informacija od strane korisnika i nedovoljan pristup korisnika informacijama što ih sprečava da odaberu proizvode s odgovarajućim svojstvima kibernetičke sigurnosti ili da ih upotrebljavaju na siguran način.

(2) Ovom se Uredbom nastoje utvrditi okvirni uvjeti za razvoj sigurnih proizvoda s digitalnim elementima tako što se osigurava 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 omogućuju korisnicima da pri odabiru i upotrebi proizvoda s digitalnim elementima vode računa o kibernetičkoj sigurnosti, na primjer poboljšanjem transparentnosti u pogledu razdoblja potpore za proizvode s digitalnim elementima koji se stavljaju na tržište.

(3) Relevantno pravo Unije koje je na snazi sastoji se od nekoliko skupova horizontalnih pravila kojima se iz različitih kutova odgovara na određene aspekte povezane s kibernetičkom sigurnošću, uključujući mjere za poboljšanje sigurnosti digitalnog lanca opskrbe. Međutim, postojećim pravom Unije koje se odnosi na kibernetičku sigurnost, uključujući Uredbu (EU) 2019/881 Europskog parlamenta i Vijeća ([3]) i Direktivu (EU) 2022/2555 Europskog parlamenta i Vijeća ([4]), ne uređuju se izravno obvezni zahtjevi u pogledu sigurnosti proizvoda s digitalnim elementima.

([1]) SL C 100, 16.3.2023., str. 101.
([2]) Stajalište Europskog parlamenta od 12. ožujka 2024. (još nije objavljeno u Službenom listu) i odluka Vijeća od 10. listopada 2024.
([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]) Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2) (SL L 333, 27.12.2022., str. 80.).

(4) Iako se postojeće pravo Unije primjenjuje na određene proizvode s digitalnim elementima, ne postoji horizontalni regulatorni okvir Unije kojim se utvrđuju sveobuhvatni zahtjevi u pogledu kibernetičke sigurnosti za sve proizvode s digitalnim elementima. Raznim dosad donesenim aktima i poduzetim inicijativama na razini Unije i na nacionalnoj razini samo se djelomično odgovara na utvrđene probleme i rizike povezane s kibernetičkom sigurnošću, što na unutarnjem tržištu stvara pravnu neujednačenost, povećava pravnu nesigurnost i za dobavljače i za korisnike tih proizvoda te poduzećima i organizacijama nameće nepotrebno opterećenje usklađivanja s nizom zahtjeva i obveza za slične vrste proizvoda. Kibernetička sigurnost tih proizvoda ima posebno snažnu prekograničnu dimenziju jer proizvode s digitalnim elementima proizvedene u jednoj državi članici ili trećoj zemlji često upotrebljavaju organizacije i potrošači na cjelokupnom unutarnjem tržištu. Stoga je to područje potrebno urediti na razini Unije kako bi se osigurao usklađen regulatorni okvir i pravna sigurnost za korisnike, organizacije i poduzeća, uključujući mikropoduzeća te mala i srednja poduzeća kako su definirana u Prilogu Preporuci Komisije 2003/361/EZ ([5]). Regulatorni okvir Unije trebalo bi uskladiti uvođenjem horizontalnih zahtjeva u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima. Osim toga, trebalo bi u cijeloj Uniji osigurati pravnu sigurnost za gospodarske subjekte i korisnike, kao i bolju usklađenost unutarnjeg tržišta i proporcionalnost za mikropoduzeća te mala i srednja poduzeća, čime bi se stvorili održiviji uvjeti za gospodarske subjekte koji namjeravaju ući na to tržište.

(5) Kad je riječ o mikropoduzećima te malim i srednjim poduzećima pri određivanju kategorije u koju poduzeće pripada odredbe Priloga Preporuci 2003/361/EZ trebale bi se primjenjivati u cijelosti. Stoga bi se pri izračunu broja zaposlenika i financijskih gornjih granica kojima se određuju kategorije poduzeća trebale primjenjivati i odredbe članka 6. Priloga Preporuci 2003/361/EZ o utvrđivanju podataka za poduzeće s obzirom na posebne vrste poduzeća, kao što su partnerska poduzeća ili povezana poduzeća.

(6) Komisija bi trebala pružati smjernice za pomoć gospodarskim subjektima u primjeni ove Uredbe, posebno mikropoduzećima te malim i srednjim poduzećima. Takve smjernice trebale bi, među ostalim, obuhvaćati područje primjene ove Uredbe, posebno daljinsku obradu podataka i njezine implikacije za programere besplatnog softvera otvorenog koda, primjenu kriterija koji se upotrebljavaju za utvrđivanje razdoblja potpore za proizvode s digitalnim elementima, međudjelovanje ove Uredbe i drugog prava Unije te koncept bitne izmjene.

(7) U raznim programskim i političkim dokumentima na razini Unije, kao što su Zajednička komunikacija Komisije i Visokog predstavnika Unije za vanjske poslove i sigurnosnu politiku od 16. prosinca 2020. naslovljena „Strategija EU-a za kibernetičku sigurnost za digitalno desetljeće”, zaključci Vijeća od 2. prosinca 2020. o kibernetičkoj sigurnosti povezanih uređaja i od 23. svibnja 2022. o razvoju položaja Europske unije u pogledu kiberprostora, ili Rezolucija Europskog parlamenta od 10. lipnja 2021. o strategiji EU-a za kibersigurnost za digitalno desetljeće ([6]), pozivalo se na donošenje posebnih zahtjeva Unije u pogledu kibernetičke sigurnosti digitalne ili povezane proizvode, a nekoliko trećih zemalja na vlastitu je inicijativu uvelo mjere radi odgovaranja na ovo pitanje. U završnom izvješću Konferencije o budućnosti Europe građani su pozvali na „veću ulogu EU-a u borbi protiv kibernetičkih sigurnosnih prijetnji”. Važno je uspostaviti ambiciozan regulatorni okvir kako bi Unija imala vodeću međunarodnu ulogu u području kibernetičke sigurnosti.

(8) Kako bi se povećala ukupna razina kibernetičke sigurnosti svih proizvoda s digitalnim elementima koji se stavljaju na unutarnje tržište, za te je proizvode potrebno uvesti tehnološki neutralne bitne zahtjeve u pogledu kibernetičke sigurnosti koji su orijentirani na ciljeve i primjenjuju se horizontalno.

(9) Pod određenim uvjetima svi proizvodi s digitalnim elementima koji su integrirani u veći elektronički informacijski sustav ili su povezani s njim mogu poslužiti kao vektor napada za zlonamjerne aktere. Zbog toga čak i hardver i softver koji se smatraju manje kritičnima mogu olakšati početno ugrožavanje uređaja ili mreže, omogućujući zlonamjernim akterima da ostvare povlašteni pristup sustavu ili da se lateralno kreću među sustavima. Stoga bi proizvođači trebali osigurati da su svi proizvodi s digitalnim elementima projektirani i razvijeni u skladu s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi. Ta se obveza odnosi i na 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 sučelja. S obzirom na to da se kibernetičke prijetnje mogu širiti putem raznih proizvoda s digitalnim elementima prije nego što dođu do određene mete, primjerice ulančavanjem više kodova za iskorištavanje ranjivosti, proizvođači bi također trebali osigurati kibernetičku sigurnost proizvoda s digitalnim elementima koji su samo neizravno povezani s drugim uređajima ili mrežama.

([5]) Preporuka Komisije 2003/361/EZ od 6. svibnja 2003. o definiciji mikropoduzeća te malih i srednjih poduzeća (SL L 124, 20.5.2003., str. 36.).

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

(10) Utvrđivanjem zahtjeva u pogledu kibernetičke sigurnosti za stavljanje na tržište proizvoda s digitalnim elementima nastoji se poboljšati kibernetičku sigurnost tih proizvoda i za potrošače i za poduzeća. Tim će se zahtjevima također osigurati da se kibernetička sigurnost uzima u obzir u cijelim lancima opskrbe, povećavajući sigurnost konačnih proizvoda s digitalnim elementima i njihovih komponenti. To uključuje i zahtjeve u pogledu stavljanja na tržište potrošačkih proizvoda s digitalnim elementima namijenjenih ranjivim potrošačima, kao što su igračke i sustavi za nadzor male djece. Potrošački proizvodi s digitalnim elementima koji su u ovoj Uredbi kategorizirani kao važni proizvodi s digitalnim elementima predstavljaju veći kibernetički sigurnosni rizik jer obavljaju funkciju koja sadržava znatan rizik od štetnih učinaka u smislu svojeg intenziteta i sposobnosti da našteti zdravlju, sigurnosti ili zaštiti korisnika takvih proizvoda te bi trebali biti podvrgnuti strožem postupku ocjenjivanja sukladnosti. To se odnosi na proizvode kao što su pametni kućanski proizvodi sa sigurnosnim funkcionalnostima, među ostalim i na pametne brave za vrata, sustave za nadzor male djece i alarmne sustave, povezane igračke i osobne nosive zdravstvene tehnološke proizvode. Nadalje, stroži postupci ocjenjivanja sukladnosti kojima se moraju podvrgnuti drugi proizvodi s digitalnim elementima koji su u ovoj Uredbi kategorizirani kao važni ili kritični proizvodi s digitalnim elementima pridonijet će sprečavanju mogućih negativnih učinaka iskorištavanja ranjivosti na potrošače.

(11) Svrha je ove Uredbe osigurati visoku razinu kibernetičke sigurnosti proizvoda s digitalnim elementima i njihovih integriranih rješenja za daljinsku obradu podataka. Takva rješenja za daljinsku obradu podataka trebalo bi definirati kao obradu podataka na daljinu za koju je softver projektirao i razvio proizvođač tog proizvoda s digitalnim elementima ili je projektiran i razvijen u njegovo ime, a čiji bi nedostatak onemogućio da proizvod s digitalnim elementima obavlja neku od svojih funkcija. Tim se pristupom osigurava da proizvođači takve proizvode u cijelosti prikladno zaštite, neovisno o tome obrađuju li se ili pohranjuju podaci lokalno na uređaju korisnika ili ih obrađuje ili pohranjuje proizvođač na daljinu. Istodobno, obrada ili pohrana na daljinu obuhvaćeni su područjem primjene ove Uredbe samo u mjeri u kojoj su potrebni da proizvod s digitalnim elementima obavlja svoje funkcije. Takva obrada ili pohrana na daljinu uključuje situaciju u kojoj mobilna aplikacija zahtijeva pristup aplikacijskom programskom sučelju ili bazi podataka koji se pružaju uz pomoć usluge koju je razvio proizvođač. U tom je slučaju usluga obuhvaćena područjem primjene ove Uredbe kao rješenje za daljinsku obradu podataka. Zahtjevi koji se odnose na rješenja za daljinsku obradu podataka koja su obuhvaćena područjem primjene ove Uredbe stoga ne uključuju tehničke, operativne ili organizacijske mjere kojima je cilj upravljanje rizicima za sigurnost mrežnih i informacijskih sustava proizvođača u cjelini.

(12) Rješenja u oblaku predstavljaju rješenja za daljinsku obradu podataka u smislu ove Uredbe samo ako odgovaraju definiciji utvrđenoj u ovoj Uredbi. Na primjer, funkcionalnosti omogućene oblakom koje pruža proizvođač pametnih kućanskih uređaja koje korisnicima omogućuju upravljanje uređajem na daljinu obuhvaćene su područjem primjene ove Uredbe. S druge strane, internetske stranice koje ne podržavaju funkcionalnost proizvoda s digitalnim elementima ili usluge u oblaku osmišljene i razvijene izvan odgovornosti proizvođača proizvoda s digitalnim elementima nisu obuhvaćene područjem primjene ove Uredbe. Direktiva (EU) 2022/2555 primjenjuje se na usluge računalstva u oblaku i modele usluga u oblaku kao što su softver kao usluga (SaaS), platforma kao usluga (PaaS) ili infrastruktura kao usluga (IaaS). Subjekti koji pružaju usluge računalstva u oblaku u Uniji koji pripadaju srednjim poduzećima u skladu s člankom 2. Priloga Preporuci 2003/361/EZ ili premašuju gornje granice za srednja poduzeća predviđene u stavku 1. tog članka obuhvaćeni su područjem primjene te direktive.

(13) U skladu s ciljem ove Uredbe o uklanjanju prepreka za slobodno kretanje proizvoda s digitalnim elementima, države članice ne bi trebale sprečavati, kad je riječ o pitanjima obuhvaćenima ovom Uredbom, stavljanje na raspolaganje na tržištu proizvoda s digitalnim elementima koji su u skladu s ovom Uredbom. Stoga, kad je riječ o pitanjima usklađenima s ovom Uredbom, države članice ne mogu nametnuti dodatne zahtjeve u pogledu kibernetičke sigurnosti za stavljanje na raspolaganje na tržištu proizvoda s digitalnim elementima. Međutim, svaki javni ili privatni subjekt može utvrditi dodatne zahtjeve uz one utvrđene u ovoj Uredbi za nabavu ili upotrebu proizvoda s digitalnim elementima za svoje posebne svrhe te stoga može odlučiti upotrebljavati proizvode s digitalnim elementima koji ispunjavaju strože ili detaljnije zahtjeve u pogledu kibernetičke sigurnosti od onih koji su primjenjivi za stavljanje na raspolaganje na tržištu u skladu s ovom Uredbom. Ne dovodeći u pitanje direktive 2014/24/EU ([7]) i 2014/25/EU ([8]) Europskog parlamenta i Vijeća, pri nabavi proizvoda s digitalnim elementima, koji moraju biti u skladu s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi, uključujući

([7]) Direktiva 2014/24/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o javnoj nabavi i o stavljanju izvan snage Direktive 2004/18/EZ (SL L 94, 28.3.2014., str. 65.).

([8]) Direktiva 2014/25/EU Europskog parlamenta i Vijeća od 26. veljače 2014. o nabavi subjekata koji djeluju u sektoru vodnog gospodarstva, energetskom i prometnom sektoru te sektoru poštanskih usluga i stavljanju izvan snage Direktive 2004/17/EZ (SL L 94, 28.3.2014., str. 243.).

one koji se odnose na postupanje s ranjivostima, države članice trebale bi osigurati da se takvi zahtjevi uzmu u obzir u postupku nabave i da se uzme u obzir i sposobnost proizvođača da djelotvorno primjenjuju mjere kibernetičke sigurnosti i upravljaju kibernetičkim prijetnjama. Nadalje, Direktivom (EU) 2022/2555 utvrđuju se mjere upravljanja kibernetičkim sigurnosnim rizicima za ključne i važne subjekte kako su navedeni u članku 3. te direktive koje bi mogle uključivati mjere za sigurnost lanca opskrbe kojima se zahtijeva da takvi subjekti upotrebljavaju proizvode s digitalnim elementima koji ispunjavaju strože zahtjeve u pogledu kibernetičke sigurnosti od onih utvrđenih u ovoj Uredbi. U skladu s Direktivom (EU) 2022/2555 i u skladu s njezinim načelom minimalnog usklađivanja države članice stoga mogu nametnuti dodatne zahtjeve u pogledu kibernetičke sigurnosti za upotrebu informacijske i komunikacijske tehnologije (IKT) proizvoda od strane ključnih ili važnih subjekata u skladu s tom direktivom kako bi se osigurala viša razina kibernetičke sigurnosti, pod uvjetom da su takvi zahtjevi u skladu s obvezama država članica utvrđenima u pravu Unije. Pitanja koja nisu obuhvaćena ovom Uredbom mogu uključivati netehničke čimbenike povezane s proizvodima s digitalnim elementima i njihovim proizvođačima. Države članice stoga mogu utvrditi nacionalne mjere, uključujući ograničenja za proizvode s digitalnim elementima ili dobavljače takvih proizvoda kojima se uzimaju u obzir netehnički čimbenici. Zahtijeva se da nacionalne mjere koje se odnose na takve čimbenike budu u skladu s pravom Unije.

(14) Ovom Uredbom ne bi se trebala dovoditi u pitanje odgovornost država članica za zaštitu nacionalne sigurnosti, u skladu s pravom Unije. Države članice trebale bi moći podvrgnuti dodatnim mjerama proizvode s digitalnim elementima koji se nabavljaju ili upotrebljavaju u svrhe nacionalne sigurnosti ili obrane, pod uvjetom da su takve mjere u skladu s obvezama država članica utvrđenima u pravu Unije.

(15) Ova se Uredba primjenjuje na gospodarske subjekte samo u vezi s proizvodima s digitalnim elementima koji su stavljeni na raspolaganje na tržištu i koji su stoga isporučeni za distribuciju ili upotrebu na tržištu Unije u okviru komercijalne djelatnosti. Opskrbu u okviru komercijalne djelatnosti moglo bi karakterizirati ne samo naplaćivanje određene cijene za proizvod s digitalnim elementima nego i naplaćivanje određene cijene za usluge tehničke podrške kada to ne služi samo povratu stvarnih troškova, s namjerom unovčavanja, primjerice pružanjem softverske platforme putem koje proizvođač unovčuje druge usluge, čiju upotrebu uvjetuje obradom osobnih podataka u svrhe koje nisu isključivo poboljšanje sigurnosti, kompatibilnosti ili interoperabilnosti softvera, ili prihvaćanje donacija koje premašuju troškove povezane s projektiranjem, razvojem i pružanjem proizvoda s digitalnim elementima. Prihvaćanje donacija bez namjere ostvarivanja dobiti ne bi se trebalo smatrati komercijalnom djelatnošću.

(16) Proizvodi s digitalnim elementima koji se pružaju kao dio pružanja usluge za koju se naplaćuje naknada isključivo radi povrata stvarnih troškova izravno povezanih s funkcioniranjem te usluge, kao što to može biti slučaj s određenim proizvodima s digitalnim elementima koje pružaju subjekti javne uprave, ne bi se samo na temelju tih razloga trebali smatrati komercijalnom djelatnošću za potrebe ove Uredbe. Nadalje, proizvodi s digitalnim elementima koje je subjekt javne uprave razvio ili izmijenio isključivo za vlastitu upotrebu ne bi se trebali smatrati stavljenima na raspolaganje na tržištu u smislu ove Uredbe.

(17) Softver i podaci koji se slobodno dijele i kojima korisnici mogu slobodno pristupiti, upotrebljavati ih, mijenjati i redistribuirati njih ili njihove izmijenjene verzije, mogu doprinijeti istraživanju i inovacijama na tržištu. Kako bi se poticali razvoj i korištenje besplatnog softvera otvorenog koda, posebno od strane mikropoduzeća te malih i srednjih poduzeća, uključujući start-up poduzeća, pojedince, neprofitne organizacije i akademske istraživačke organizacije, prilikom primjene ove Uredbe na proizvode s digitalnim elementima koji se smatraju besplatnim softverom otvorenog koda i isporučuju za distribuciju ili upotrebu u okviru komercijalne djelatnosti trebalo bi uzeti u obzir prirodu različitih razvojnih modela softvera koji se distribuiraju i razvijaju u okviru besplatnih licencija za softver otvorenog koda.

(18) Besplatni softver otvorenog koda tumači se kao softver čiji se izvorni kod otvoreno dijeli i u čijoj su licenci predviđena sva prava kako bi ga se učinilo slobodno dostupnim, upotrebljivim, izmjenjivim i preraspodjeljivim. Besplatni softver otvorenog koda razvija se, održava i distribuira otvoreno, uključujući putem internetskih platformi. Kad je riječ o gospodarskim subjektima koji su obuhvaćeni područjem primjene ove Uredbe, područjem primjene ove Uredbe trebao bi biti obuhvaćen samo besplatan softver otvorenog koda koji je stavljen na raspolaganje na tržištu i koji se stoga isporučuje za distribuciju ili upotrebu u okviru komercijalne djelatnosti. Same okolnosti u kojima je proizvod s digitalnim elementima razvijen, ili način financiranja njegova razvoja, ne bi stoga trebalo uzimati u obzir pri određivanju komercijalne ili nekomercijalne prirode te djelatnosti. Točnije, za potrebe ove Uredbe i u odnosu na gospodarske subjekte koji su obuhvaćeni njezinim područjem primjene, kako bi se osigurala jasna razlika između faze razvoja i faze isporuke, pružanje proizvoda s digitalnim elementima koji se smatraju besplatnim

softverom otvorenog koda koje njihovi proizvođači ne unovčuju ne bi trebalo smatrati komercijalnom djelatnošću. Nadalje, isporuku proizvoda s digitalnim elementima koji se smatraju besplatnim softverskim komponentama otvorenog koda namijenjenima tome da ih drugi proizvođači integriraju u vlastite proizvode s digitalnim elementima trebalo bi smatrati stavljanjem na raspolaganje na tržištu samo ako je izvorni proizvođač unovčio komponentu. Na primjer, sama činjenica da proizvod s digitalnim elementima sa softverom otvorenog koda prima financijsku potporu proizvođača ili da proizvođači doprinose razvoju takvog proizvoda sama po sebi ne bi trebala odrediti da je djelatnost komercijalne prirode. Osim toga, postojanje redovitih novih izdanja ne bi trebalo samo po sebi dovesti do zaključka da se proizvod s digitalnim elementima isporučuje u okviru komercijalne djelatnosti. Naposljetku, za potrebe ove Uredbe, razvoj od strane neprofitnih organizacija proizvoda s digitalnim elementima koji se smatraju besplatnim softverom otvorenog koda ne bi se trebao smatrati komercijalnom djelatnošću pod uvjetom da je organizacija ustrojena na način kojim se osigurava da se sva zarada nakon troškova upotrebljava za postizanje neprofitnih ciljeva. Ova se Uredba ne primjenjuje na fizičke ili pravne osobe koje izvornim kodom doprinose proizvodima s digitalnim elementima koji se smatraju besplatnim softverom otvorenog koda za koje nisu odgovorni.

(19) Uzimajući u obzir važnost za kibernetičku sigurnost mnogih proizvoda s digitalnim elementima koji se smatraju besplatnim softverom otvorenog koda koji se objavljuju, ali se ne stavljaju na raspolaganje na tržištu u smislu ove Uredbe, pravne osobe koje na kontinuiranoj osnovi pružaju potporu za razvoj takvih proizvoda koji su namijenjeni komercijalnim djelatnostima i koje imaju vodeću ulogu u osiguravanju održivosti tih proizvoda (upravitelji softvera otvorenog koda) trebale bi podlijegati blagim i prilagođenim regulatornim režimima. Upravitelji softvera otvorenog koda uključuju određene zaklade kao i subjekte koji razvijaju i objavljuju besplatan softver otvorenog koda u poslovnom kontekstu, što uključuje neprofitne subjekte. Regulatorni režim trebao bi voditi računa o njihovoj specifičnosti i kompatibilnosti s vrstom nametnutih obveza. Trebao bi obuhvaćati samo proizvode s digitalnim elementima koji se smatraju besplatnim softverom otvorenog koda koji su u konačnici namijenjeni komercijalnim djelatnostima, kao što su integracija u komercijalne usluge ili u unovčene proizvode s digitalnim elementima. Za potrebe tog regulatornog režima namjera integracije u unovčene proizvode s digitalnim elementima uključuje slučajeve u kojima proizvođači koji integriraju komponentu u vlastite proizvode s digitalnim elementima redovito doprinose razvoju te komponente ili pružaju redovitu financijsku pomoć kako bi osigurali kontinuitet softverskog proizvoda. Pružanje kontinuirane potpore razvoju proizvoda s digitalnim elementima uključuje, među ostalim, smještaj na poslužitelju i upravljanje platformama za suradnju u razvoju softvera, smještaj izvornog koda ili softvera na poslužitelju, upravljanje ili raspolaganje proizvodima s digitalnim elementima koji se smatraju besplatnim softverom otvorenog koda, kao i upravljanje razvojem takvih proizvoda. S obzirom na to da se blagim i prilagođenim regulatornim režimom osobe koje djeluju kao upravitelji softvera otvorenog koda ne podvrgava istim obvezama kao osobe koje djeluju kao proizvođači u skladu s ovom Uredbom, ne bi im trebalo dopustiti stavljanje oznake CE na proizvode s digitalnim elementima čiji razvoj podržavaju.

(20) Sam čin smještaja proizvoda s digitalnim elementima na otvorenim repozitorijima, među ostalim putem upravitelja paketima ili na platformama za suradnju, ne predstavlja sam po sebi stavljanje na raspolaganje na tržištu proizvoda s digitalnim elementima. Pružatelje takvih usluga trebalo bi smatrati distributerima samo ako takav softver stavljaju na raspolaganje na tržištu i stoga ga isporučuju za distribuciju ili upotrebu na tržištu Unije u okviru komercijalne djelatnosti.

(21) Kako bi se poduprla i olakšala dužna pažnja proizvođača koji u svoje proizvode s digitalnim elementima integriraju besplatne softverske komponente otvorenog koda koje ne podliježu bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi, Komisija bi trebala moći uspostaviti dobrovoljne programe potvrda o sigurnosti delegiranim aktom o dopuni ove Uredbe ili zahtijevanjem europskog programa kibernetičke sigurnosne certifikacije u skladu s člankom 48. Uredbe (EU) 2019/881 kojim se uzimaju u obzir posebnosti razvojnih modela besplatnog softvera otvorenog koda. Programe potvrda o sigurnosti trebalo bi osmisliti tako da ne samo fizičke ili pravne osobe koje razvijaju proizvod s digitalnim elementima koji se smatra besplatnim softverom otvorenog koda ili doprinose njegovu razvoju mogu pokrenuti ili financirati potvrdu o sigurnosti, nego i treće strane, kao što su proizvođači koji takve proizvode integriraju u vlastite proizvode s digitalnim elementima, korisnici ili javne uprave Unije i nacionalne javne uprave.

(22) S obzirom na ciljeve ove Uredbe u području kibernetičke sigurnosti u javnom sektoru i kako bi se poboljšala informiranost država članica o stanju u pogledu ovisnosti Unije o softverskim komponentama, a posebno o potencijalno besplatnim softverskim komponentama otvorenog koda, posebna skupina za administrativnu suradnju (skupina za ADCO) osnovana ovom Uredbom trebala bi moći odlučiti zajednički provesti procjenu ovisnosti Unije. Tijela za nadzor tržišta trebala bi moći od proizvođača kategorija proizvoda s digitalnim elementima, koje je utvrdila skupina za ADCO, zatražiti da dostave popis softverskog materijala koji su izradili u skladu s ovom Uredbom. Kako bi se zaštitila povjerljivost popisa softverskog materijala, tijela za nadzor tržišta trebala bi skupini za ADCO dostaviti relevantne informacije o ovisnostima u anonimiziranom i objedinjenom obliku.

(23) Djelotvornost provedbe ove Uredbe ovisit će i o dostupnosti odgovarajućih vještina u području kibernetičke sigurnosti. U raznim programskim i političkim dokumentima na razini Unije, uključujući Komunikaciju Komisije od 18. travnja 2023. naslovljenu „Povećanjem broja stručnjaka za kibernetičku sigurnost do veće konkurentnosti, rasta i otpornosti Unije" i zaključke Vijeća od 22. svibnja 2023. o politici Unije u području kibernetičke obrane, prepoznati su nedostatak vještina u području kibernetičke sigurnosti u Uniji i potreba za prioritetnim svladavanjem takvih izazova, i u javnom i u privatnom sektoru. Kako bi se osigurala djelotvorna provedba ove Uredbe, države članice trebale bi osigurati da su dostupna odgovarajući resursi za zapošljavanje prikladnog broja osoblja tijela za nadzor tržišta i tijela za ocjenjivanje sukladnosti potrebnog za obavljanje njihovih zadaća kako su utvrđene u ovoj Uredbi. Tim bi se mjerama trebala ojačati mobilnost radne snage u području kibernetičke sigurnosti i s time povezanih karijera. Te mjere trebale bi također pridonijeti povećanju otpornosti i uključivosti radne snage u području kibernetičke sigurnosti, među ostalim u pogledu roda. Države članice stoga bi trebale poduzeti mjere kako bi se pobrinule da te zadaće obavljaju adekvatno osposobljeni stručnjaci s potrebnim vještinama u području kibernetičke sigurnosti. Slično tome, proizvođači bi trebali osigurati da njihovo osoblje ima potrebne vještine za ispunjavanje obveza kako su utvrđene u ovoj Uredbi. Države članice i Komisija, u skladu sa svojim ovlastima i nadležnostima te posebnim zadaćama koje su im dodijeljene ovom Uredbom, trebale bi poduzeti mjere za pružanje potpore proizvođačima, a posebno mikropoduzećima te malim i srednjim poduzećima, uključujući start-up poduzeća, među ostalim i u područjima kao što je razvoj vještina, u svrhu usklađenosti sa svojim obvezama utvrđenima u ovoj Uredbi. Nadalje, budući da se Direktivom (EU) 2022/2555 od država članica zahtijeva da u okviru svojih nacionalnih strategija za kibernetičku sigurnost donesu politike kojima se promiču i razvijaju osposobljavanje u području kibernetičke sigurnosti i vještine u pogledu kibernetičke sigurnosti, države članice mogu pri donošenju takvih strategija također razmotriti hoće li odgovoriti na potrebe za vještinama u području kibernetičke sigurnosti koje proizlaze iz ove Uredbe, uključujući potrebe koje se odnose na prekvalifikaciju i usavršavanje.

(24) Siguran internet neophodan je za funkcioniranje kritičnih infrastruktura i društva u cjelini. Direktivom (EU) 2022/2555 nastoji se osigurati visoka razina kibernetičke sigurnosti usluga koje pružaju ključni i važni subjekti kako su navedeni u članku 3. te direktive, uključujući pružatelje digitalne infrastrukture koji podupiru osnovne funkcije otvorenog interneta te osiguravaju pristup internetu i pružaju internetske usluge. Stoga je važno da se proizvodi s digitalnim elementima koji su pružateljima digitalne infrastrukture potrebni 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 usklađenost sa zahtjevima koji se odnose na lance opskrbe na temelju Direktive (EU) 2022/2555 tako što se osigurava da se proizvodi s digitalnim elementima koje pružatelji digitalne infrastrukture upotrebljavaju za pružanje usluga razvijaju sigurno i da imaju pristup pravodobnim sigurnosnim ažuriranjima za takve proizvode.

(25) Uredbom (EU) 2017/745 Europskog parlamenta i Vijeća ([9]) utvrđuju se pravila za medicinske proizvode, a Uredbom (EU) 2017/746 Europskog parlamenta i Vijeća ([10]) *za in vitro* dijagnostičke medicinske proizvode. Tim se uredbama odgovara na kibernetičke sigurnosne rizike te se temelje na posebnim pristupima, o kojima govori 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 po sebi softver. Tim uredbama obuhvaćeni su i određeni neugrađeni softver te pristup koji se temelji na cijelom životnom ciklusu. Tim se zahtjevima od proizvođača zahtijeva da pri razvoju i izradi svojih proizvoda primjenjuju načelâ upravljanja rizikom i utvrđuju zahtjeve koji se odnose na mjere IT sigurnosti te odgovarajuće postupke ocjenjivanja sukladnosti. Nadalje, od prosinca 2019. na snazi su posebne smjernice za kibernetičku sigurnost medicinskih proizvoda kojima se proizvođačima medicinskih proizvoda, uključujući *in vitro* dijagnostičke proizvode, pružaju smjernice o tome kako ispuniti sve relevantne bitne zahtjeve utvrđene u Prilogu I. tim uredbama u pogledu kibernetičke sigurnosti. Stoga proizvodi na koje se primjenjuje bilo koja od tih uredbi ne bi trebali podlijegati ovoj Uredbi.

(26) Proizvodi s digitalnim elementima koji su razvijeni ili izmijenjeni isključivo u svrhe nacionalne sigurnosti ili obrane ili proizvodi koji su posebno osmišljeni za obradu klasificiranih podataka nisu obuhvaćeni područjem primjene ove Uredbe. Države članice se potiču da osiguraju istu ili višu razinu zaštite za te proizvode kao i za one koji su obuhvaćeni područjem primjene ove Uredbe.

([9]) 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.).

([10]) 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.).

(27) Uredbom (EU) 2019/2144 Europskog parlamenta i Vijeća ([11]) utvrđeni su zahtjevi za homologaciju tipa vozila i njihovih sustava i sastavnih dijelova te su pritom uvedeni određeni zahtjevi u pogledu kibernetičke sigurnosti, među ostalim u pogledu rada certificiranog sustava upravljanja kibernetičkom sigurnošću i ažuriranja softvera, koji se odnose na politike i postupke organizacijâ za upravljanje kibernetičkim sigurnosnim rizicima tijekom cijelog životnog ciklusa vozila, opreme i usluga u skladu s primjenjivim pravilnicima Ujedinjenih naroda o tehničkim specifikacijama i kibernetičkoj sigurnosti, posebice s Pravilnikom UN-a br. 155 – Jedinstvene odredbe o homologaciji vozila s obzirom na kibernetičku sigurnost i sustav za upravljanje kibernetičkom sigurnošću ([12]), te na posebne postupke ocjenjivanja sukladnosti. U području zrakoplovstva, glavni je cilj Uredbe (EU) 2018/1139 Europskog parlamenta i Vijeća ([13]) uspostaviti i održavati visoku ujednačenu razinu sigurnosti civilnog zrakoplovstva u Uniji. Tom je uredbom uspostavljen okvir za bitne zahtjeve u pogledu plovidbenosti za aeronautičke proizvode, dijelove i opremu, uključujući softver, koji uključuje obveze zaštite od prijetnji povezanih sa sigurnošću informacija. Postupkom certifikacije na temelju Uredbe (EU) 2018/1139 postiže se razina jamstva koja se nastoji postići ovom Uredbom. Stoga proizvodi s digitalnim elementima na koje se primjenjuje Uredba (EU) 2019/2144 i proizvodi certificirani u skladu s Uredbom (EU) 2018/1139 ne bi trebali podlijegati bitnim zahtjevima u pogledu kibernetičke sigurnosti i postupcima ocjenjivanja sukladnosti utvrđenima u ovoj Uredbi.

(28) Ovom se Uredbom utvrđuju horizontalna pravila o kibernetičkoj sigurnosti 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 se utvrđuju zahtjevi koji se odnose na sve ili neke rizike obuhvaćene bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi. 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 u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi može primjenjivati ograničeno ili njezina primjena može biti isključena ako je takvo ograničenje odnosno takvo isključenje primjene u skladu s općim regulatornim okvirom koji se primjenjuje na te proizvode i ako se sektorskim pravilima postiže barem razina zaštite jednaka onoj propisanoj ovom Uredbom. Komisiju bi trebalo ovlastiti za donošenje delegiranih akata radi dopune ove Uredbe utvrđivanjem takvih proizvoda i pravila. Kad je riječ o postojećem pravu Unije u odnosu na koje bi se trebalo primjenjivati takvo ograničenje odnosno takvo isključenje primjene, ova Uredba sadržava posebne odredbe kako bi se pojasnio njezin odnos s tim pravom Unije.

(29) Kako bi se osiguralo da se proizvodi s digitalnim elementima koji su stavljeni na raspolaganje na tržištu mogu djelotvorno popraviti, a njihova trajnost produljiti, trebalo bi predvidjeti izuzeće za rezervne dijelove. To bi izuzeće trebalo obuhvatiti i rezervne dijelove u svrhu popravka naslijeđenih proizvoda koji su stavljeni na raspolaganje prije datuma početka primjene ove Uredbe te rezervne dijelove koji su već prošli postupak ocjenjivanja sukladnosti u skladu s ovom Uredbom.

(30) Delegiranom uredbom Komisije (EU) 2022/30 ([14]) utvrđeno je da se na određenu radijsku opremu primjenjuje niz bitnih zahtjeva iz članka 3. stavka 3. točaka (d), (e) i (f) Direktive 2014/53/EU Europskog parlamenta i Vijeća ([15]) koji se odnose na štetu za mrežu i zlouporabu mrežnih resursa, osobne podatke i privatnost te prijevaru. Provedbenom odlukom Komisije C(2022) 5637 od 5. kolovoza 2022. o zahtjevu za normizaciju upućenom Europskom odboru za normizaciju i Europskom odboru za elektrotehničku normizaciju utvrđeni su zahtjevi za izradu posebnih normi kojima se pobliže određuje kako bi trebalo ispuniti te bitne zahtjeve. Bitni zahtjevi u pogledu kibernetičke sigurnosti utvrđeni u ovoj Uredbi uključuju sve elemente bitnih zahtjeva iz članka 3. stavka 3. točaka (d), (e) i (f) Direktive

([11]) 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.).

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

([13]) 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.).

([14]) Delegirana uredba Komisije (EU) 2022/30 od 29. listopada 2021. o dopuni Direktive 2014/53/EU Europskog parlamenta i Vijeća u pogledu primjene bitnih zahtjeva iz članka 3. stavka 3. točaka (d), (e) i (f) te direktive (SL L 7, 12.1.2022., str. 6.).

([15]) Direktiva 2014/53/EU Europskog parlamenta i Vijeća od 16. travnja 2014. o usklađivanju zakonodavstava država članica o stavljanju na raspolaganje radijske opreme na tržištu i stavljanju izvan snage Direktive 1999/5/EZ (SL L 153, 22.5.2014., str. 62.).

2014/53/EU. Nadalje, bitni zahtjevi u pogledu kibernetičke sigurnosti utvrđeni u ovoj Uredbi usklađeni su s ciljevima zahtjevâ za posebne norme uključene u taj zahtjev za normizaciju. Dakle, kada 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 C(2022)5637. Tijekom prijelaznog razdoblja za primjenu ove Uredbe Komisija bi trebala pružiti smjernice proizvođačima koji podliježu i ovoj Uredbi i Delegiranoj uredbi (EU) 2022/30 radi olakšavanja dokazivanja usklađenosti s tim dvjema uredbama.

(31) Direktiva (EU) 2024/2853 Europskog parlamenta i Vijeća ([16]) 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 nedovoljnom sigurnošću njegova proizvoda, neovisno o krivnji („objektivna odgovornost”). Ako se takvo pomanjkanje sigurnosti sastoji od nedostatka sigurnosnih ažuriranja nakon stavljanja proizvoda na tržište i to prouzroči štetu, proizvođač bi mogao snositi odgovornost. Obveze proizvođača koje se odnose na pružanje takvih sigurnosnih ažuriranja trebalo bi utvrditi ovom Uredbom.

(32) Ovom se Uredbom ne bi trebalo dovoditi u pitanje Uredbu (EU) 2016/679 Europskog parlamenta i Vijeća ([17]), uključujući odredbe koje se odnose na uspostavu mehanizama certificiranja zaštite podataka te pečata i oznaka za zaštitu podataka za potrebe dokazivanja usklađenosti postupaka obrade koje obavljaju voditelji i izvršitelji obrade s tom uredbom. Takvi bi se postupci mogli ugraditi u proizvod s digitalnim elementima. Tehnička i integrirana zaštita podataka te općenito kibernetička sigurnost ključni su elementi Uredbe (EU) 2016/679. Štiteći potrošače i organizacije od kibernetičkih sigurnosnih rizika, bitni zahtjevi u pogledu kibernetičke sigurnosti utvrđeni u ovoj Uredbi trebali bi doprinijeti i poboljšanju zaštite osobnih podataka i privatnosti pojedinaca. Trebalo bi razmotriti sinergije u području normizacije i certifikacije s obzirom na aspekte kibernetičke sigurnosti 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 izvršavanja. U tu bi svrhu nacionalna tijela za nadzor tržišta imenovana na temelju ove Uredbe trebala surađivati s tijelima koja nadziru primjenu prava Unije o zaštiti podataka. Tijela koja nadziru primjenu prava Unije o zaštiti podataka trebala bi ujedno imati pristup informacijama relevantnima za obavljanje svojih zadaća.

(33) U mjeri u kojoj su njihovi proizvodi obuhvaćeni područjem primjene ove Uredbe, pružatelji europskih lisnica za digitalni identitet iz članka 5.a stavka 2. Uredbe (EU) br. 910/2014 Europskog parlamenta i Vijeća ([18]) trebali bi biti u skladu s horizontalnim bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi i posebnim sigurnosnim zahtjevima utvrđenima u članku 5.a Uredbe (EU) br. 910/2014. Kako bi se olakšala usklađenost, pružatelji lisnica trebali bi moći certificiranjem svojih proizvoda u okviru europskog programa kibernetičke sigurnosne certifikacije koji je uspostavljen na temelju Uredbe (EU) 2019/881, i za koji je Komisija delegiranim aktima utvrdila da stvara pretpostavku sukladnosti s ovom Uredbom, dokazati usklađenost europskih lisnica za digitalni identitet sa zahtjevima utvrđenima u ovoj Uredbi odnosno Uredbi (EU) br. 910/2014, u mjeri u kojoj certifikat, ili njegovi dijelovi, obuhvaća te zahtjeve.

(34) Kako bi osigurali da su proizvodi projektirani, razvijeni i proizvedeni u skladu s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi, pri integraciji komponenti koje potječu od trećih strana u proizvode s digitalnim elementima tijekom faze projektiranja i razvoja proizvođači bi trebali postupati s dužnom pažnjom u pogledu tih komponenti, uključujući besplatne softverske komponente otvorenog koda koje nisu

([16]) Direktiva (EU) 2024/2853 Europskog parlamenta i Vijeća od 23. listopada 2024. o odgovornosti za neispravne proizvode i stavljanju izvan snage Direktive Vijeća 85/374/EEZ (SL L, 2024/2853, 18.11.2024., ELI: http://data.europa.eu/eli/dir/2024/2853/oj).

([17]) 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.).

([18]) Uredba (EU) br. 910/2014 Europskog parlamenta i Vijeća od 23. srpnja 2014. o elektroničkoj identifikaciji i uslugama povjerenja za elektroničke transakcije na unutarnjem tržištu i stavljanju izvan snage Direktive 1999/93/EZ (SL L 257, 28.8.2014., str. 73.).

stavljene na raspolaganje na tržištu. Odgovarajuća razina dužne pažnje ovisi o prirodi i razini kibernetičkog sigurnosnog rizika povezanoj s određenom komponentom te u tu svrhu treba razmotriti jednu ili više sljedećih mjera: provjeriti, kako je primjenjivo, je li proizvođač komponente dokazao sukladnost s ovom Uredbom, među ostalim provjerom ima li komponenta već oznaku CE; provjeriti je li komponenta redovito sigurnosno ažurirana, primjerice pregledom povijesti sigurnosnih ažuriranja; provjeriti da u komponenti nema ranjivosti registriranih u europskoj bazi podataka o ranjivostima uspostavljenoj u skladu s člankom 12. stavkom 2. Direktive (EU) 2022/2555 ili u drugim javno dostupnim bazama podataka o ranjivostima; ili provesti dodatna sigurnosna ispitivanja. Obveze u pogledu postupanja s ranjivostima utvrđene u ovoj Uredbi, koje proizvođači moraju ispunjavati pri stavljanju proizvoda s digitalnim elementima na tržište i tijekom razdoblja potpore, primjenjuju se na proizvode s digitalnim elementima u cijelosti, uključujući sve integrirane komponente. Ako tijekom postupanja s dužnom pažnjom proizvođač proizvoda s digitalnim elementima utvrdi ranjivost u pojedinoj komponenti, uključujući u besplatnoj komponenti otvorenog koda, trebao bi obavijestiti osobu ili subjekt koji je proizveo komponentu ili je održava, otkloniti i ispraviti ranjivost te, ako je primjenjivo, pružiti dotičnoj osobi ili dotičnom subjektu provedbu sigurnosnog popravka.

(35) Odmah nakon prijelaznog razdoblja za primjenu ove Uredbe proizvođač proizvoda s digitalnim elementima koji integrira jednu ili više komponenti koje potječu od trećih strana i koje također podliježu ovoj Uredbi, možda neće moći u okviru svoje obveze dužne pažnje provjeriti jesu li proizvođači tih komponenti dokazali sukladnost s ovom Uredbom, primjerice, provjerom toga imaju li te komponente već oznaku CE. To može biti slučaj ako su komponente integrirane prije početka primjene ove Uredbe na proizvođače tih komponenti. U tom bi slučaju proizvođač koji je integrirao takve komponente trebao postupati s dužnom pažnjom na druge načine.

(36) Proizvodi s digitalnim elementima trebali bi imati oznaku CE kao vidljivi, čitljivi i neizbrisivi 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 Uredbe i imaju oznaku CE. Nadalje, države članice ne bi trebale sprečavati izlaganje ni upotrebu proizvoda s digitalnim elementima, uključujući njegov prototip, koji nije u skladu s ovom Uredbom, na sajmovima, izložbama, predstavljanjima ili sličnim događanjima, pod uvjetom da proizvod ima vidljiv znak kojim se jasno navodi da proizvod nije u skladu s ovom Uredbom i da ne smije biti stavljen na raspolaganje na tržištu dok ne bude u skladu s njom.

(37) Kako bi se osiguralo da proizvođači mogu izdavati softver u svrhu testiranja prije podvrgavanja svojih proizvoda s digitalnim elementima ocjenjivanju sukladnosti, države članice ne bi trebale sprečavati stavljanje na raspolaganje nedovršenog softvera, kao što su alfa verzije, beta verzije ili potencijalne verzije za izdavanje, pod uvjetom da je nedovršeni softver stavljen na raspolaganje samo tijekom razdoblja potrebnog za njegovo testiranje i prikupljanje povratnih informacija. Proizvođači bi trebali osigurati da se softver koji se stavi na raspolaganje pod tim uvjetima izda tek nakon procjene rizika i da je u mjeri u kojoj je to moguće sukladan sa sigurnosnim zahtjevima utvrđenima u ovoj Uredbi koji se odnose na svojstva proizvoda s digitalnim elementima. Proizvođači bi u najvećoj mogućoj mjeri trebali provoditi i zahtjeve u pogledu postupanja s ranjivostima. Proizvođači ne bi trebali korisnike primoravati na nadogradnje na verzije izdane samo radi testiranja.

(38) Kako bi se osiguralo da proizvodi s digitalnim elementima kad su stavljeni na tržište ne predstavljaju kibernetičke sigurnosne rizike za osobe i organizacije, trebalo bi utvrditi bitne zahtjeve u pogledu kibernetičke sigurnosti za takve proizvode. Ti bitni zahtjevi u pogledu kibernetičke sigurnosti, uključujući zahtjeve u pogledu upravljanja ranjivostima, primjenjuju se na svaki pojedinačni proizvod s digitalnim elementima kada se stavlja na tržište, neovisno o tome je li proizvod s digitalnim elementima proizveden kao pojedinačna jedinica ili dio serije. Na primjer, za vrstu proizvoda svaki pojedinačni proizvod s digitalnim elementima trebao je pri stavljanju na tržište dobiti sve sigurnosne zakrpe ili ažuriranja dostupne radi odgovaranja na relevantne sigurnosne probleme. Kad se proizvodi s digitalnim elementima naknadno mijenjaju, fizičkim ili digitalnim sredstvima, na način koji proizvođač nije predvidio u prvotnoj procjeni rizika i koji može ukazivati na to da više ne ispunjavaju relevantne bitne zahtjeve u pogledu kibernetičke sigurnosti, takva izmjena trebala bi se smatrati bitnom. Na primjer, popravci softvera mogu se izjednačiti s održavanjem pod uvjetom da se njima proizvod s digitalnim elementima koji je već stavljen na tržište ne mijenja na takav način da to može utjecati na usklađenost s primjenjivim zahtjevima ili promijeniti namjenu za koju je proizvod ocijenjen.

(39) Kao i u slučaju fizičkih popravaka ili izmjena, proizvod s digitalnim elementima trebao bi se smatrati bitno izmijenjenim softverskom promjenom ako se ažuriranjem softvera izmijeni namjena tog proizvoda, a proizvođač te promjene nije predvidio u prvotnoj procjeni rizika ili ako se zbog ažuriranja softvera promijenila priroda opasnosti

ili povećala razina kibernetičkog sigurnosnog rizika te je ažurirana verzija proizvoda stavljena na raspolaganje na tržištu. Ako se sigurnosnim ažuriranjem koje je projektirano kako bi se smanjila razina kibernetičkog sigurnosnog rizika proizvoda s digitalnim elementima ne mijenja namjena proizvoda s digitalnim elementima, ono se ne smatra bitnom izmjenom. To obično uključuje situacije u kojima sigurnosno ažuriranje podrazumijeva samo manje prilagodbe izvornog koda. Na primjer, to bi mogao biti slučaj kada se sigurnosnim ažuriranjem ispravlja poznata ranjivost, među ostalim izmjenom funkcija ili performansi proizvoda s digitalnim elementima isključivo u svrhu smanjenja razine kibernetičkog sigurnosnog rizika. Slično tomu, manje ažuriranje funkcionalnosti, kao što je vizualno poboljšanje ili dodavanje novih piktograma ili jezika korisničkom sučelju, općenito se ne bi trebalo smatrati bitnom izmjenom. S druge strane, ako se ažuriranjem značajke mijenjaju izvorno predviđena funkcija ili vrsta ili performanse proizvoda s digitalnim elementima i ispunjavaju se gore navedeni kriteriji, ono bi se trebalo smatrati bitnom izmjenom jer dodavanje novih značajki obično dovodi do šire površine napada, čime se povećava kibernetički sigurnosni rizik. Na primjer, to bi mogao biti slučaj kada se aplikaciji dodaje novi ulazni element kojim se od proizvođača zahtijeva da osigura odgovarajuću potvrdu ulaznih podataka. Pri procjeni smatra li se ažuriranje značajke bitnom izmjenom nije relevantno je li riječ o zasebnom ažuriranju ili kombinaciji sa sigurnosnim ažuriranjem. Komisija bi trebala izdati smjernice o tome kako odrediti što predstavlja bitnu izmjenu.

(40) Uzimajući u obzir iterativnu prirodu razvoja softvera, proizvođači koji su naknadne verzije softverskog proizvoda stavili na tržište kao rezultat naknadne bitne izmjene tog proizvoda trebali bi moći pružati sigurnosna ažuriranja tijekom razdoblja potpore samo za posljednju verziju softverskog proizvoda koju su stavili na tržište. To bi trebali moći učiniti samo ako korisnici relevantnih prethodnih verzija proizvoda imaju besplatan pristup posljednjoj verziji proizvoda koja je stavljena na tržište i ne snose dodatne troškove za prilagodbu hardverskog ili softverskog okruženja u kojem se koriste proizvodom. To bi, na primjer, mogao biti slučaj kada se za nadogradnju operativnog sustava stolnog računala ne zahtijeva novi hardver, kao što je brža središnja procesorska jedinica ili više memorije. Međutim, proizvođač bi tijekom razdoblja potpore trebao i dalje biti u skladu s drugim zahtjevima u pogledu postupanja s ranjivostima, kao što su postojanje politike koordiniranog otkrivanja ranjivosti ili mjere uspostavljene za olakšavanje dijeljenja informacija o potencijalnim ranjivostima za sve naknadne bitno izmijenjene verzije softverskog proizvoda stavljenog na tržište. Proizvođači bi trebali moći pružati manja sigurnosna ažuriranja ili ažuriranja funkcionalnosti koja ne predstavljaju bitnu izmjenu samo za najnoviju verziju ili podverziju softverskog proizvoda koji nije bitno izmijenjen. U isto vrijeme, ako hardverski proizvod, kao što je pametni telefon, nije kompatibilan s najnovijom verzijom operativnog sustava s kojim je izvorno isporučen, proizvođač bi trebao nastaviti pružati, tijekom razdoblja potpore, sigurnosna ažuriranja barem za posljednju kompatibilnu verziju operativnog sustava.

(41) U skladu s uvriježenim konceptom bitne izmjene za proizvode uređene zakonodavstvom Unije o usklađivanju primjereno je da se za proizvod s digitalnim elementima provjeri usklađenost i, ako je primjenjivo, provede novi postupak ocjenjivanja sukladnosti ako nastupi bitna izmjena koja može utjecati na usklađenost proizvoda s digitalnim elementima s ovom Uredbom ili kad se promijeni namjena tog proizvoda. Ako je primjenjivo, ako proizvođač provodi ocjenjivanje sukladnosti koje uključuje treću stranu, treću stranu trebalo bi obavijestiti o promjeni koja bi mogla dovesti do bitne izmjene.

(42) Ako proizvod s digitalnim elementima podliježe „obnovi", „održavanju" i „popravku" kako su definirani u članku 2. točkama 18., 19. i 20. Uredbe (EU) 2024/1781 Europskog parlamenta i Vijeća ([19]), to nužno ne dovodi do bitne izmjene proizvoda, primjerice ako se ne promijene namjena i funkcionalnosti te razina rizika ostane nepromijenjena. Međutim, nadogradnja proizvoda s digitalnim elementima koju je učinio proizvođač mogla bi dovesti do promjena u projektu i razvoju tog proizvoda te bi stoga mogla utjecati na njegovu namjenu i njegovu usklađenost sa zahtjevima utvrđenima u ovoj Uredbi.

(43) Proizvodi s digitalnim elementima trebali bi se smatrati važnima ako negativni učinci iskorištavanja potencijalnih ranjivosti u proizvodima mogu biti teški zbog, među ostalim, njihove funkcionalnosti povezane s kibernetičkom sigurnošću ili funkcije koja sa sobom nosi znatan rizik od štetnih učinaka u smislu svojeg intenziteta i sposobnosti ometanja, kontrole ili nanošenja štete velikom broju drugih proizvoda s digitalnim elementima ili zdravlju, sigurnosti ili zaštiti svojih korisnika izravnom manipulacijom, kao što je funkcija središnjeg sustava, među ostalim upravljanje mrežom, kontrola konfiguracije, virtualizacija ili obrada osobnih podataka. Osobito, ranjivosti u proizvodima s digitalnim elementima koji imaju funkcionalnost povezanu s kibernetičkom sigurnošću, kao što su upravitelji pokretanja sustava, mogu dovesti do širenja sigurnosnih problema cijelim lancem opskrbe. Težina učinka

([19]) Uredba (EU) 2024/1781 Europskog parlamenta i Vijeća od 13. lipnja 2024. o uspostavi okvira za utvrđivanje zahtjeva za ekološki dizajn održivih proizvoda, izmjeni Direktive (EU) 2020/1828 i Uredbe (EU) 2023/1542 te stavljanju izvan snage Direktive 2009/125/EZ (SL L, 2024/1781, 28.6.2024., ELI: http://data.europa.eu/eli/reg/2024/1781/oj).

incidenta može se također povećati ako proizvod prvenstveno obavlja funkciju središnjeg sustava, uključujući upravljanje mrežom, kontrolu konfiguracije, virtualizaciju ili obradu osobnih podataka.

(44) Određene kategorije proizvoda s digitalnim elementima trebale bi podlijegati strožim postupcima ocjenjivanja sukladnosti, pri čemu bi se trebao zadržati proporcionalan pristup. U tu bi svrhu važne proizvode s digitalnim elementima trebalo podijeliti u dva razreda koja odražavaju razinu kibernetičkog sigurnosnog rizika povezanog s tim kategorijama proizvoda. Incident koji uključuje važne proizvode s digitalnim elementima koji pripadaju u II. razred mogao bi dovesti do većih negativnih učinaka od incidenta koji uključuje važne proizvode s digitalnim elementima koji pripadaju u I. razred, na primjer zbog prirode njihove funkcije povezane s kibernetičkom sigurnošću ili zbog obavljanja druge funkcije koja nosi znatan rizik od štetnih učinaka. Kao pokazatelj takvih većih negativnih učinaka, proizvodi s digitalnim elementima koji pripadaju u II. razred mogli bi obavljati kibernetičku sigurnosnu funkcionalnost ili drugu funkciju koja nosi znatan rizik od štetnih učinaka koji je veći nego za one navedene u I. razredu, ili ispunjavaju oba prethodno navedena kriterija. Važni proizvodi s digitalnim elementima koji pripadaju u II. razred stoga bi trebali podlijegati strožem postupku ocjenjivanja sukladnosti.

(45) Važne proizvode s digitalnim elementima iz ove Uredbe trebalo bi tumačiti kao proizvode koji imaju osnovnu funkcionalnost kategorije važnih proizvoda s digitalnim elementima koja je utvrđena u ovoj Uredbi. Na primjer, ovom se Uredbom utvrđuju kategorije važnih proizvoda s digitalnim elementima koji su definirani prema svojoj osnovnoj funkcionalnosti kao vatrozidovi ili sustavi za otkrivanje ili sprečavanje neovlaštenih upada u II. razredu. Zato vatrozidovi te sustavi za otkrivanje ili sprečavanje neovlaštenih upada podliježu obveznom ocjenjivanju sukladnosti koje provodi treća strana. To nije slučaj s drugim proizvodima s digitalnim elementima koji nisu kategorizirani kao važni proizvodi s digitalnim elementima koji mogu integrirati vatrozidove ili sustave za otkrivanje ili sprečavanje neovlaštenih upada. Komisija bi trebala donijeti provedbeni akt kojim se pobliže određuje tehnički opis kategorija važnih proizvoda s digitalnim elementima koji pripadaju I. i II. razredu, kako je utvrđeno u ovoj Uredbi.

(46) Kategorije kritičnih proizvoda s digitalnim elementima utvrđene u ovoj Uredbi imaju funkcionalnost povezanu s kibernetičkom sigurnošću i obavljaju funkciju koja nosi znatan rizik od štetnih učinaka u smislu intenziteta i sposobnosti ometanja, kontrole ili nanošenja štete velikom broju drugih proizvoda s digitalnim elementima izravnom manipulacijom. Nadalje, te kategorije proizvoda s digitalnim elementima smatraju se kritičnim ovisnostima za ključne subjekte iz članka 3. stavka 1. Direktive (EU) 2022/2555. Kategorije kritičnih proizvoda s digitalnim elementima navedene u prilogu ovoj Uredbi zbog svoje kritičnosti već se u velikoj mjeri koriste različitim oblicima certifikacije te su obuhvaćene i europskim programom kibernetičke sigurnosne certifikacije na temelju zajedničkih kriterija (EUCC) utvrđenim u Provedbenoj uredbi Komisije (EU) 2024/482 ([20]). Stoga bi, kako bi se osigurala zajednička odgovarajuća kibernetička sigurnosna zaštita kritičnih proizvoda s digitalnim elementima u Uniji, moglo biti prikladno i proporcionalno da se takve kategorije proizvoda delegiranim aktom podvrgnu obveznoj europskoj kibernetičkoj sigurnosnoj certifikaciji ako je već uspostavljen relevantni europski program kibernetičke sigurnosne certifikacije koji obuhvaća te proizvode i ako je Komisija provela procjenu mogućeg učinka predviđene obvezne certifikacije na tržište. U toj bi procjeni trebalo razmotriti i ponudu i potražnju, među ostalim postoji li dostatna potražnja za predmetnim proizvodima s digitalnim elementima iz država članica i od korisnika kako bi se zahtijevala europska kibernetička sigurnosna certifikacija, kao i svrhe u koje su proizvodi s digitalnim elementima namijenjeni, među ostalim kritične ovisnosti ključnih subjekata kako su navedeni u članku 3. stavku 1. Direktive (EU) 2022/2555 o tim proizvodima. U procjeni bi trebalo analizirati i moguće učinke obvezne certifikacije na dostupnost tih proizvoda na unutarnjem tržištu te sposobnosti i spremnost država članica za provedbu relevantnih europskih programa kibernetičke sigurnosne certifikacije.

(47) Delegiranim aktima kojima se zahtijeva obvezna europska kibernetička sigurnosna certifikacija trebalo bi utvrditi proizvode s digitalnim elementima koji imaju osnovnu funkcionalnost kategorije kritičnih proizvoda s digitalnim elementima utvrđene u ovoj Uredbi koji podliježu obveznoj certifikaciji, kao i potrebnu razinu jamstva koja bi trebala biti barem „znatna”. Potrebna razina jamstva trebala bi biti proporcionalna razini kibernetičkog sigurnosnog rizika povezanog s proizvodom s digitalnim elementima. Na primjer, ako proizvod s digitalnim elementima ima osnovnu funkcionalnost kategorije kritičnih proizvoda s digitalnim elementima utvrđene u ovoj Uredbi i namijenjen

([20]) Provedbena uredba Komisije (EU) 2024/482 od 31. siječnja 2024. o utvrđivanju pravila za primjenu Uredbe (EU) 2019/881 Europskog parlamenta i Vijeća u pogledu donošenja europskog programa kibernetičkosigurnosne certifikacije na temelju zajedničkih kriterija (EUCC) (SL L, 2024/482, 7.2.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

je za upotrebu u osjetljivom ili kritičnom okruženju, kao što su proizvodi namijenjeni za upotrebu ključnih subjekata iz članka 3. stavka 1. Direktive (EU) 2022/2555, možda će biti potrebna najviša razina jamstva.

(48) Kako bi se u Uniji osigurala zajednička odgovarajuća kibernetička sigurnosna zaštita proizvoda s digitalnim elementima koji imaju osnovnu funkcionalnost kategorije kritičnih proizvoda s digitalnim elementima utvrđene u ovoj Uredbi, Komisiju bi također trebalo ovlastiti za donošenje delegiranih akata radi izmjene ove Uredbe dodavanjem ili povlačenjem kategorija kritičnih proizvoda s digitalnim elementima za koje bi se od proizvođača moglo zahtijevati da ishode europski kibernetički sigurnosni certifikat u okviru europskog programa kibernetičke sigurnosne certifikacije na temelju Uredbe (EU) 2019/881 radi dokazivanja sukladnosti s ovom Uredbom. Tim se kategorijama može dodati nova kategorija kritičnih proizvoda s digitalnim elementima ako ključni subjekti kako su navedeni u članku 3. stavku 1. Direktive (EU) 2022/2555 kritično ovise o tim proizvodima ili, ako su pogođeni incidentima ili sadržavaju iskorištene ranjivosti, to bi moglo dovesti do poremećaja u ključnim lancima opskrbe. Pri ocjenjivanju potrebe za dodavanjem ili povlačenjem kategorija kritičnih proizvoda s digitalnim elementima delegiranim aktom Komisija bi trebala moći uzeti u obzir jesu li države članice na nacionalnoj razini utvrdile proizvode s digitalnim elementima koji imaju kritičnu ulogu za otpornost ključnih subjekata kako su navedeni u članku 3. stavku 1. Direktive (EU) 2022/2555 i koji se sve više suočavaju s kibernetičkim napadima u lancu opskrbe, s mogućim ozbiljnim negativnim učincima. Nadalje, Komisija bi trebala moći uzeti u obzir ishod koordinirane procjene sigurnosnog rizika ključnih lanaca opskrbe na razini Unije provedene u skladu s člankom 22. Direktive (EU) 2022/2555.

(49) Komisija bi pri pripremi mjera za provedbu ove Uredbe trebala osigurati strukturirano i redovito savjetovanje sa širokim krugom relevantnih dionika. To bi posebno trebao biti slučaj kada Komisija ocjenjuje potrebu za mogućim ažuriranjima popisa kategorija važnih ili kritičnih proizvoda s digitalnim elementima, pri čemu bi se trebalo savjetovati s relevantnim proizvođačima i uzeti u obzir njihova stajališta kako bi se analizirali kibernetički sigurnosni rizici te ravnoteža troškova i koristi određivanja takvih kategorija proizvoda kao važnih ili kritičnih.

(50) Ovom se Uredbom ciljano odgovara na kibernetičke sigurnosne rizike. Međutim, proizvodi s digitalnim elementima mogli bi predstavljati druge sigurnosne rizike koji nisu uvijek povezani s kibernetičkom sigurnošću, ali mogu biti posljedica povrede sigurnosti. Takvi bi rizici i dalje trebali biti uređeni relevantnim zakonodavstvom Unije o usklađivanju koje nije ova Uredba. Ako drugo zakonodavstvo Unije o usklađivanju koje nije ova Uredba nije primjenjivo, oni bi trebali podlijegati Uredbi (EU) 2023/988 Europskog parlamenta i Vijeća ([21]). Stoga, s obzirom na ciljanu prirodu ove Uredbe, kao odstupanje od članka 2. stavka 1. trećeg podstavka točke (b) Uredbe (EU) 2023/988, poglavlje III., odjeljak 1., poglavlja V. i VII., i poglavlja od IX. do XI. Uredbe (EU) 2023/988 trebali bi se primjenjivati na proizvode s digitalnim elementima u pogledu sigurnosnih rizika koji nisu obuhvaćeni ovom Uredbom ako ti proizvodi ne podliježu posebnim zahtjevima utvrđenima u zakonodavstvu Unije o usklađivanju koje nije ova Uredba u smislu članka 3. točke 27. Uredbe (EU) 2023/988.

(51) Proizvodi s digitalnim elementima koji su klasificirani kao visokorizični UI sustavi u skladu s člankom 6. Uredbe (EU) 2024/1689 Europskog parlamenta i Vijeća ([22]) koji su obuhvaćeni područjem primjene ove Uredbe trebali bi biti u skladu s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi. Ako ti visokorizični UI sustavi ispunjavaju bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u ovoj Uredbi, trebalo bi smatrati da su u skladu sa zahtjevima za kibernetičku sigurnost utvrđenima u članku 15. Uredbe (EU) 2024/1689 u mjeri u kojoj su ti zahtjevi obuhvaćeni EU izjavom o sukladnosti, ili njezinim dijelovima, izdanom na temelju ove Uredbe. U tu svrhu, procjenom kibernetičkih sigurnosnih rizika povezanih s proizvodom s digitalnim elementima koji je klasificiran kao visokorizični UI sustav u skladu s Uredbom (EU) 2024/1689 koju treba uzeti u obzir u fazama planiranja, projektiranja, razvoja, proizvodnje, isporuke i održavanja takvog proizvoda, kako se zahtijeva ovom Uredbom, trebalo bi uzeti u obzir rizike za kibernetičku otpornost UI sustava u pogledu pokušaja neovlaštenih trećih

([21]) Uredba (EU) 2023/988 Europskog parlamenta i Vijeća od 10. svibnja 2023. o općoj sigurnosti proizvoda, izmjeni Uredbe (EU) br. 1025/2012 Europskog parlamenta i Vijeća i Direktive (EU) 2020/1828 Europskog parlamenta i Vijeća te o stavljanju izvan snage Direktive 2001/95/EZ Europskog parlamenta i Vijeća i Direktive Vijeća 87/357/EEZ (SL L 135, 23.5.2023., str. 1.).

([22]) Uredba (EU) 2024/1689 Europskog parlamenta i Vijeća od 13. lipnja 2024. o utvrđivanju usklađenih pravila o umjetnoj inteligenciji i o izmjeni uredaba (EZ) br. 300/2008, (EU) br. 167/2013, (EU) br. 168/2013, (EU) 2018/858, (EU) 2018/1139 i (EU) 2019/2144 te direktiva 2014/90/EU, (EU) 2016/797 i (EU) 2020/1828 (Akt o umjetnoj inteligenciji) (SL L, 2024/1689, 12.7.2024., ELI: http://data.europa.eu/eli/reg/2024/1689/oj).

strana da izmijene njegovu upotrebu, ponašanje ili performanse, uključujući ranjivosti specifične za UI kao što su trovanje podacima ili neprijateljski napadi, kao i, prema potrebi, rizike za temeljna prava, u skladu s Uredbom (EU) 2024/1689. Kad je riječ o postupcima ocjenjivanja sukladnosti koji se odnose na bitne zahtjeve u pogledu kibernetičke sigurnosti za proizvod s digitalnim elementima koji je obuhvaćen područjem primjene ove Uredbe i koji je klasificiran kao visokorizični UI sustav, umjesto relevantnih odredbi ove Uredbe u pravilu bi se trebao primjenjivati članak 43. Uredbe (EU) 2024/1689. Međutim, to pravilo ne bi trebalo dovesti do smanjenja potrebne razine jamstva za važne ili kritične proizvode s digitalnim elementima iz ove Uredbe. Stoga bi, odstupajući od tog pravila, visokorizični UI sustavi koji su obuhvaćeni područjem primjene Uredbe (EU) 2024/1689 i također su važni ili kritični proizvodi s digitalnim elementima iz ove Uredbe te na koje se primjenjuje postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga VI. Uredbi (EU) 2024/1689 trebali podlijegati postupcima ocjenjivanja sukladnosti predviđenima u ovoj Uredbi u mjeri u kojoj se to odnosi na bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u ovoj Uredbi. U takvom bi se slučaju za sve ostale aspekte obuhvaćene Uredbom (EU) 2024/1689 trebale primjenjivati relevantne odredbe o ocjenjivanju sukladnosti na temelju unutarnje kontrole utvrđene u Prilogu VI. toj uredbi.

(52) Kako bi se poboljšala sigurnost proizvoda s digitalnim elementima koji se stavljaju na unutarnje tržište, potrebno je utvrditi bitne zahtjeve u pogledu kibernetičke sigurnosti primjenjive na takve proizvode. Tim bitnim zahtjevima u pogledu kibernetičke sigurnosti ne bi se trebale dovoditi u pitanje koordinirane procjene sigurnosnih rizika ključnih lanaca opskrbe na razini Unije iz članka 22. Direktive (EU) 2022/2555 u kojima se uzimaju u obzir tehnički i, prema potrebi, netehnički čimbenici rizika, kao što je nedopušteni utjecaj treće zemlje na dobavljače. Nadalje, njima se ne bi trebale dovoditi u pitanje ovlasti država članica da utvrde dodatne zahtjeve kojima se uzimaju u obzir netehnički čimbenici za potrebe osiguravanja visoke razine otpornosti, uključujući one definirane u Preporuci Komisije (EU) 2019/534 ([23]), u koordiniranoj procjeni rizika za kibernetičku sigurnost 5G mreža u EU-u i u paketu instrumenata EU-a za kibernetičku sigurnost 5G mreža koji je dogovorila skupina za suradnju osnovana u skladu s člankom 14. Direktive (EU) 2022/2555.

(53) Proizvođači proizvoda obuhvaćenih područjem primjene Uredbe (EU) 2023/1230 Europskog parlamenta i Vijeća ([24]) koji su i proizvodi s digitalnim elementima kako su definirani u ovoj Uredbi trebali bi biti u skladu i s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi i s bitnim zdravstvenim i sigurnosnim zahtjevima utvrđenima u Uredbi (EU) 2023/1230. Bitni zahtjevi u pogledu kibernetičke sigurnosti utvrđeni u ovoj Uredbi i određeni bitni zahtjevi utvrđeni u Uredbi (EU) 2023/1230 mogli bi se odnositi na slične kibernetičke sigurnosne rizike. Stoga bi se usklađenošću s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi mogla olakšati usklađenost s bitnim zahtjevima koji obuhvaćaju i određene kibernetičke sigurnosne rizike kako su utvrđeni u Uredbi (EU) 2023/1230, a posebno onima koji se odnose na zaštitu od zlouporabe te sigurnost i pouzdanost kontrolnih sustava iz odjeljaka 1.1.9. i 1.2.1. Priloga III. toj uredbi. Takve sinergije proizvođač mora dokazati, primjerice primjenom, ako su dostupne, usklađenih normi ili drugih tehničkih specifikacija koje obuhvaćaju relevantne bitne zahtjeve u pogledu kibernetičke sigurnosti nakon procjene rizika kojom su obuhvaćeni ti kibernetički sigurnosni rizici. Proizvođač bi također trebao slijediti primjenjive postupke ocjenjivanja sukladnosti utvrđene u ovoj Uredbi i u Uredbi (EU) 2023/1230. Komisija i europske organizacije za normizaciju trebale bi u pripremnom radu na potpori provedbi ove Uredbe i Uredbe (EU) 2023/1230 i povezanih postupaka normizacije promicati dosljednost u načinu na koji treba procjenjivati kibernetičke sigurnosne rizike i načinu na koji ti rizici trebaju biti obuhvaćeni usklađenim normama u pogledu relevantnih bitnih zahtjeva. Posebno, Komisija i europske organizacije za normizaciju trebale bi uzeti u obzir ovu Uredbu pri pripremi i razvoju usklađenih normi kako bi se olakšala provedba Uredbe (EU) 2023/1230, posebno u vezi s kibernetičkim sigurnosnim aspektima u pogledu zaštite od zlouporabe te sigurnosti i pouzdanosti kontrolnih sustava iz odjeljaka 1.1.9. i 1.2.1. Priloga III. toj uredbi. Komisija bi trebala pružiti smjernice za potporu proizvođačima koji podliježu ovoj Uredbi i koji također podliježu Uredbi (EU) 2023/1230, posebno kako bi se olakšalo dokazivanje usklađenosti s relevantnim bitnim zahtjevima utvrđenima u ovoj Uredbi i u Uredbi (EU) 2023/1230.

(54) Kako bi se osigurala sigurnost proizvoda s digitalnim elementima i u trenutku njihova stavljanja na tržište i tijekom očekivanog vremena upotrebe proizvoda s digitalnim elementima, potrebno je utvrditi bitne zahtjeve u pogledu kibernetičke sigurnosti za postupanje s ranjivostima i bitne zahtjeve u pogledu kibernetičke sigurnosti koji se odnose na svojstva proizvoda s digitalnim elementima. Iako bi proizvođači trebali postupati u skladu sa svim bitnim

([23]) Preporuka Komisije (EU) 2019/534 od 26. ožujka 2019. Kibersigurnost 5G mreža (SL L 88, 29.3.2019., str. 42.).
([24]) Uredba (EU) 2023/1230 Europskog parlamenta i Vijeća od 14. lipnja 2023. o strojevima te o stavljanju izvan snage Direktive 2006/42/EZ Europskog parlamenta i Vijeća i Direktive Vijeća 73/361/EEZ (SL L 165, 29.6.2023., str. 1.).

zahtjevima u pogledu kibernetičke sigurnosti u vezi s postupanjem s ranjivostima tijekom razdoblja potpore, trebali bi odrediti koji su drugi bitni zahtjevi u pogledu svojstava proizvoda relevantni za predmetnu vrstu proizvoda s digitalnim elementima. U tu bi svrhu proizvođači trebali procijeniti kibernetičke sigurnosne rizike povezane s proizvodom s digitalnim elementima kako bi utvrdili relevantne rizike i relevantne bitne zahtjeve u pogledu kibernetičke sigurnosti kako bi stavili na raspolaganje svoje proizvode s digitalnim elementima bez poznatih iskoristivih ranjivosti koje bi mogle utjecati na sigurnost tih proizvoda te kako bi na odgovarajući način primijenili odgovarajuće usklađene norme, zajedničke specifikacije ili europske ili međunarodne norme.

(55) Ako određeni bitni zahtjevi u pogledu kibernetičke sigurnosti nisu primjenjivi na proizvod s digitalnim elementima, proizvođač bi trebao uključiti jasno obrazloženje u procjenu kibernetičkog sigurnosnog rizika uključenu u tehničku dokumentaciju. To bi mogao biti slučaj kad bitni zahtjev u pogledu kibernetičke sigurnosti nije u skladu s prirodom proizvoda s digitalnim elementima. Na primjer, namjena proizvoda s digitalnim elementima može zahtijevati da proizvođač poštuje široko priznate norme interoperabilnosti čak i ako se njegove sigurnosne značajke više ne smatraju najsuvremenijima. Slično tome, drugim se pravom Unije od proizvođača zahtijeva da primjenjuju posebne zahtjeve interoperabilnosti. Ako bitni zahtjev u pogledu kibernetičke sigurnosti nije primjenjiv na proizvod s digitalnim elementima, ali je proizvođač utvrdio kibernetičke sigurnosne rizike u odnosu na taj bitni zahtjev u pogledu kibernetičke sigurnosti, trebao bi poduzeti mjere za uklanjanje tih rizika drugim sredstvima, primjerice ograničavanjem namjene proizvoda na pouzdana okruženja ili obavješćivanjem korisnika o tim rizicima.

(56) Jedna od najvažnijih mjera koje korisnici trebaju poduzeti kako bi zaštitili svoje proizvode s digitalnim elementima od kibernetičkih napada jest ugradnja najnovijih dostupnih sigurnosnih ažuriranja što je prije moguće. Proizvođači bi stoga trebali projektirati svoje proizvode i uspostaviti procese kojima se osigurava da proizvodi s digitalnim elementima uključuju funkcije koje omogućuju automatsko obavješćivanje, distribuciju, preuzimanje i ugradnju sigurnosnih ažuriranja, posebno u slučaju potrošačkih proizvoda. Također bi trebali pružiti mogućnost odobravanja preuzimanja i ugradnje sigurnosnih ažuriranja kao završnog koraka. Korisnici bi trebali zadržati mogućnost deaktivacije automatskih ažuriranja jasnim i jednostavnim mehanizmom koji je podržan jasnim uputama o tome kako se korisnici mogu isključiti. Zahtjevi koji se odnose na automatska ažuriranja kako su utvrđeni u prilogu ovoj Uredbi nisu primjenjivi na proizvode s digitalnim elementima koji se prvenstveno namjeravaju integrirati kao komponente u druge proizvode. Ne primjenjuju se ni na proizvode s digitalnim elementima za koje korisnici ne bi razumno očekivali automatska ažuriranja, uključujući proizvode s digitalnim elementima namijenjene za upotrebu u profesionalnim mrežama IKT-a, a posebno u kritičnim i industrijskim okruženjima u kojima bi automatsko ažuriranje moglo uzrokovati ometanje rada. Bez obzira na to je li proizvod s digitalnim elementima projektiran za primanje automatskih ažuriranja ili nije, njegov bi proizvođač trebao obavijestiti korisnike o ranjivostima i bez odgode staviti na raspolaganje sigurnosna ažuriranja. Ako proizvod s digitalnim elementima ima korisničko sučelje ili slično tehničko sredstvo koje omogućuje izravnu interakciju s korisnicima, proizvođač bi trebao upotrebljavati takve značajke kako bi obavijestio korisnike da je razdoblje potpore za njihov proizvod s digitalnim elementima završilo. Obavijesti bi trebale biti ograničene na ono što je potrebno kako bi se osigurala djelotvorno primanje tih informacija i ne bi trebale negativno utjecati na iskustvo korištenja proizvoda s digitalnim elementima.

(57) Kako bi se poboljšala transparentnost procesa postupanja s ranjivostima i osiguralo da se od korisnika ne zahtijeva ugradnja novih ažuriranja funkcionalnosti isključivo u svrhu primanja najnovijih sigurnosnih ažuriranja, proizvođači bi trebali osigurati, ako je to tehnički izvedivo, da se nova sigurnosna ažuriranja pružaju odvojeno od ažuriranja funkcionalnosti.

(58) U Zajedničkoj komunikaciji Komisije i Visokog predstavnika Unije za vanjske poslove i sigurnosnu politiku od 20. lipnja 2023. naslovljenoj „Europska strategija gospodarske sigurnosti” navodi se da Unija treba maksimalno povećati koristi svoje gospodarske otvorenosti uz istodobno smanjenje rizika od gospodarske ovisnosti o visokorizičnim dobavljačima putem zajedničkog strateškog okvira za gospodarsku sigurnost Unije. Ovisnosti o visokorizičnim dobavljačima proizvoda s digitalnim elementima mogu predstavljati strateški rizik koji treba rješavati na razini Unije, posebno ako su proizvodi s digitalnim elementima namijenjeni upotrebi od strane ključnih subjekata kako su navedeni u članku 3. stavku 1. Direktive (EU) 2022/2555. Takvi rizici mogu biti povezani, ali ne moraju biti ograničeni na nadležnost koja se primjenjuje na proizvođača, obilježja njegova korporativnog vlasništva i veze kontrole s vladom treće zemlje u kojoj ima poslovni nastan, posebno ako je treća zemlja uključena u gospodarsku špijunažu ili neodgovorno ponašanje države u kibernetičkom prostoru, a njezino zakonodavstvo dopušta proizvoljni pristup bilo kojoj vrsti operacija ili podataka društva, uključujući komercijalno osjetljive podatke, i može nametnuti obveze u obavještajne svrhe bez demokratskih provjera i ravnoteže, mehanizama nadzora, pravičnog postupka ili prava na žalbu neovisnom sudu. Pri utvrđivanju je li kibernetički sigurnosni rizik znatan u smislu ove Uredbe Komisija i tijela za nadzor tržišta, u skladu sa svojim odgovornostima utvrđenima u ovoj

Uredbi, trebala bi razmotriti i netehničke čimbenike rizika, posebno one utvrđene na temelju koordiniranih procjena sigurnosnih rizika ključnih lanaca opskrbe na razini Unije provedenih u skladu s člankom 22. Direktive (EU) 2022/2555.

(59) Radi osiguravanja sigurnosti proizvoda s digitalnim elementima nakon njihova stavljanja na tržište, proizvođači bi trebali odrediti razdoblje potpore, koje bi trebalo odražavati očekivano vrijeme upotrebe proizvoda s digitalnim elementima. Pri određivanju razdoblja potpore proizvođač bi posebno trebao uzeti u obzir razumna očekivanja korisnika, prirodu proizvoda i relevantno pravo Unije kojim se utvrđuje životni vijek proizvodâ s digitalnim elementima. Proizvođači bi također trebali moći uzeti u obzir druge relevantne čimbenike. Kriteriji bi se trebali primjenjivati na način kojim se osigurava proporcionalnost pri određivanju razdoblja potpore. Proizvođač bi tijelima za nadzor tržišta na zahtjev trebao dostaviti informacije koje su uzete u obzir pri utvrđivanju razdoblja potpore za proizvod s digitalnim elementima.

(60) Razdoblje potpore za koje proizvođač osigurava djelotvorno postupanje s ranjivostima trebalo bi biti najmanje pet godina, osim ako je životni vijek proizvoda s digitalnim elementima kraći od pet godina u kojem bi slučaju proizvođač trebao osigurati postupanje s ranjivostima tijekom tog životnog vijeka. Ako se razumno očekuje da će se proizvod s digitalnim elementima upotrebljavati dulje od pet godina, kao što je često slučaj s hardverskim komponentama kao što su matične ploče ili mikroprocesori, mrežnim uređajima kao što su ruteri, modemi ili preklopnici, kao i sa softverom, kao što su operativni sustavi ili alati za uređivanje videozapisa, proizvođači bi u skladu s time trebali osigurati dulja razdoblja potpore. Posebno, proizvodi s digitalnim elementima namijenjeni upotrebi u industrijskim okruženjima, kao što su industrijski kontrolni sustavi, često se upotrebljavaju tijekom znatno duljih razdoblja. Proizvođač bi trebao moći odrediti razdoblje potpore kraće od pet godina samo ako je to opravdano prirodom predmetnog proizvoda s digitalnim elementima i ako se očekuje da će se taj proizvod upotrebljavati manje od pet godina, a u tom bi slučaju razdoblje potpore trebalo odgovarati očekivanom vremenu upotrebe. Na primjer, životni vijek aplikacije za praćenje kontakata namijenjene upotrebi tijekom pandemije mogao bi biti ograničen na trajanje pandemije. Osim toga, neke softverske aplikacije mogu po svojoj prirodi biti stavljene na raspolaganje samo na temelju modela pretplate, posebno ako aplikacija postane nedostupna korisniku i stoga se više ne upotrebljava nakon isteka pretplate.

(61) Kad razdoblja potpore za proizvode s digitalnim elementima istekne, proizvođači bi, kako bi se osiguralo da se ranjivostima može upravljati nakon isteka razdoblja potpore, trebali razmotriti stavljanje na raspolaganje izvornog koda takvih proizvoda s digitalnim elementima drugim poduzećima koja se obvežu nastaviti pružati usluge postupanja s ranjivostima ili javnosti. Ako proizvođači stave na raspolaganje izvorni kod drugim poduzećima, trebali bi moći zaštititi vlasništvo nad proizvodom s digitalnim elementima i spriječiti širenje izvornog koda javnosti, na primjer putem ugovornih aranžmana.

(62) Kako bi se osiguralo da proizvođači diljem Unije odrede slična razdoblja potpore za usporedive proizvode s digitalnim elementima, skupina za ADCO trebala bi objaviti statističke podatke o prosječnim razdobljima potpore koja su proizvođači odredili za kategorije proizvoda s digitalnim elementima i izdati smjernice u kojima se navode odgovarajuća razdoblja potpore za takve kategorije. Osim toga, kako bi se osigurao usklađen pristup na cijelom unutarnjem tržištu, Komisija bi trebala moći donijeti delegirane akte kojima se utvrđuju minimalna razdoblja potpore za određene kategorije proizvoda ako podaci koje su dostavila tijela za nadzor tržišta upućuju na to da razdoblja potpore koja su utvrdili proizvođači sustavno nisu u skladu s kriterijima za određivanje razdoblja potpore utvrđenima u ovoj Uredbi ili da proizvođači u različitim državama članicama neopravdano određuju različita razdoblja potpore.

(63) Proizvođači bi trebali uspostaviti jedinstvenu kontaktnu točku koja korisnicima omogućuje laku komunikaciju s njima, među ostalim u svrhu izvješćivanja i primanja informacija o ranjivostima proizvoda s digitalnim elementom. Trebali bi osigurati da jedinstvena kontaktna točka bude lako dostupna korisnicima i jasno naznačiti njezinu dostupnost te ažurirati te informacije. Ako proizvođači odluče ponuditi automatizirane alate, npr. okvire za razgovor, trebali bi ponuditi i telefonski broj ili druga digitalna sredstva za kontakt, kao što su adresa e-pošte ili obrazac za kontakt. Jedinstvena kontaktna točka ne bi se trebala oslanjati isključivo na automatizirane alate.

(64) Proizvođači bi svoje proizvode s digitalnim elementima trebali staviti na raspolaganje na tržištu sa zadanom sigurnom konfiguracijom i korisnicima besplatno pružati sigurnosna ažuriranja. Proizvođači bi trebali moći odstupiti od bitnih zahtjeva u pogledu kibernetičke sigurnosti samo u odnosu na prilagođene proizvode koji su ugrađeni u određenu svrhu za određenog poslovnog korisnika i ako su i proizvođač i korisnik izričito pristali na drukčiji skup ugovornih uvjeta.

(65) Proizvođači bi putem jedinstvene platforme za izvješćivanje trebali istodobno obavijestiti tim za odgovor na računalne sigurnosne incidente (CSIRT) koji je imenovan koordinatorom i ENISA-u o aktivno iskorištenim ranjivostima sadržanima u proizvodima s digitalnim elementima, kao i o značajnim incidentima koji utječu na sigurnost tih proizvoda. Obavijesti bi se trebale dostavljati putem elektroničke krajnje točke za obavješćivanje CSIRT-a koji je imenovan koordinatorom i trebale bi biti istodobno dostupne ENISA-i.

(66) Proizvođači bi trebali obavijestiti o aktivno iskorištenim ranjivostima kako bi osigurali da CSIRT-ovi imenovani koordinatorima i ENISA imaju odgovarajući pregled takvih ranjivosti i da dobivaju informacije potrebne za ispunjavanje svojih zadaća kako su utvrđene u Direktivi (EU) 2022/2555 i povećanje ukupne razine kibernetičke sigurnosti ključnih i važnih subjekata kako su navedeni u članku 3. te direktive te kako bi se osiguralo djelotvorno funkcioniranje tijelâ za nadzor tržišta. S obzirom na to 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. ENISA bi, u dogovoru s proizvođačem, trebala objaviti popravljene ranjivosti u europskoj bazi podataka o ranjivostima koja je uspostavljena u skladu s člankom 12. stavkom 2. Direktive (EU) 2022/2555. Europska baza podataka o ranjivostima pomoći će proizvođačima u otkrivanju poznatih iskoristivih ranjivosti u njihovim proizvodima kako bi se osiguralo da se na raspolaganje na tržištu stavljaju sigurni proizvodi.

(67) Proizvođači bi ujedno trebali obavijestiti CSIRT koji je imenovan koordinatorom i ENISA-u o svakom značajnom incidentu koji utječe na sigurnost proizvoda s digitalnim elementima. Kako bi se osiguralo da korisnici mogu brzo reagirati na značajne incidente koji utječu na sigurnost njihovih proizvoda s digitalnim elementima, proizvođači bi također trebali obavijestiti njihove korisnike o svakom takvom incidentu i, ako je primjenjivo, o svim korektivnim mjerama koje korisnici mogu poduzeti za ublažavanje posljedica incidenta, primjerice objavljivanjem relevantnih informacija na svojim internetskim stranicama ili, ako proizvođač može stupiti u kontakt s korisnicima i kibernetički sigurnosni rizici to opravdavaju, izravnim obraćanjem korisnicima.

(68) Aktivno iskorištene ranjivosti odnose se na slučajeve u kojima proizvođač utvrdi da je povreda sigurnosti koja utječe na njegove korisnike ili bilo koju drugu fizičku ili pravnu osobu posljedica toga što je zlonamjerni akter iskoristio manu u jednom od proizvoda s digitalnim elementima koje je proizvođač stavio na raspolaganje na tržištu. Primjeri takvih ranjivosti mogli bi biti slabosti u funkcijama identifikacije i autentifikacije proizvoda. Ranjivosti koje se otkrivaju bez zle namjere u svrhu ispitivanja, istrage, ispravljanja ili otkrivanja u dobroj vjeri radi promicanja sigurnosti ili zaštite vlasnika sustava i njegovih korisnika ne bi trebale podlijegati obveznom obavješćivanju. Značajni incidenti koji utječu na sigurnost proizvoda s digitalnim elementima odnose se, s druge strane, na situacije u kojima kibernetički incident utječe na procese razvoja, proizvodnje ili održavanja proizvođača tako da bi mogao dovesti do povećanog kibernetičkog sigurnosnog rizika za korisnike ili druge osobe. Takav značajan incident mogao bi uključivati situaciju u kojoj je napadač uspješno ubacio zlonamjerni kod u kanal za objavljivanje putem kojeg proizvođač objavljuje sigurnosna ažuriranja korisnicima.

(69) Kako bi se osiguralo da se obavijesti mogu brzo podijeliti sa svim relevantnim CSIRT-ovima koji su imenovani koordinatorima i kako bi se proizvođačima omogućilo podnošenje jedinstvene obavijesti u svakoj fazi postupka obavješćivanja, ENISA bi trebala uspostaviti jedinstvenu platformu za izvješćivanje s nacionalnim krajnjim točkama za elektroničko obavješćivanje. ENISA bi trebala upravljati svakodnevnim radom jedinstvene platforme za izvješćivanje i održavati je. CSIRT-ovi koji su imenovani koordinatorima trebali bi obavijestiti svoja tijela za nadzor tržišta o prijavljenim ranjivostima ili incidentima. Jedinstvena platforma za izvješćivanje trebala bi biti osmišljena tako da se njome osigurava povjerljivost obavijesti, posebno u pogledu ranjivosti za koje još nije dostupno sigurnosno ažuriranje. Osim toga, ENISA bi trebala uspostaviti postupke za sigurno i povjerljivo postupanje s informacijama. Na temelju informacija koje prikupi ENISA bi trebala izraditi dvogodišnje tehničko izvješće o novim trendovima u području kibernetičkih sigurnosnih rizika proizvoda s digitalnim elementima i podnijeti ga skupini za suradnju uspostavljenoj u skladu s člankom 14. Direktive (EU) 2022/2555.

(70) U iznimnim okolnostima, a posebno na zahtjev proizvođača, CSIRT koji je imenovan koordinatorom koji je prvotno primio obavijest trebao bi moći odlučiti odgoditi njezino dijeljenje drugim relevantnim CSIRT-ovima koji su imenovani koordinatorima putem jedinstvene platforme za izvješćivanje ako to može biti opravdano razlozima povezanima s kibernetičkom sigurnošću i na razdoblje koje je prijeko potrebno. CSIRT koji je imenovan koordinatorom trebao bi odmah obavijestiti ENISA-u o odluci o odgodi dijeljenja i razlozima za nju, kao i o tome kada namjerava nastaviti daljnje dijeljenje. Komisija bi delegiranim aktom trebala izraditi specifikacije o uvjetima pod kojima bi se razlozi povezani s kibernetičkom sigurnošću mogli primjenjivati te bi u pripremi nacrta delegiranog akta trebala surađivati s mrežom CSIRT-ova uspostavljenom u skladu s člankom 15. Direktive (EU) 2022/2555 i ENISA-om. Primjeri razloga povezanih s kibernetičkom sigurnošću uključuju kontinuirani postupak koordiniranog otkrivanja ranjivosti ili situacije u kojima se očekuje da će proizvođač uskoro osigurati mjeru ublažavanja, a kibernetički sigurnosni rizici od neposrednog širenja informacija putem jedinstvene platforme za izvješćivanje

nadmašuju njegove koristi. Ako to zatraži CSIRT koji je imenovan koordinatorom, ENISA bi trebala biti u mogućnosti podržati taj CSIRT u primjeni razloga povezanih s kibernetičkom sigurnošću za odgodu širenja obavijesti, na temelju informacija koje je ENISA primila od tog CSIRT-a o odluci da uskrati obavijest zbog tih razloga povezanih s kibernetičkom sigurnošću. Nadalje, u posebno iznimnim okolnostima ENISA ne bi trebala istodobno primati sve pojedinosti obavijesti o aktivno iskorištenoj ranjivosti. To bi bio slučaj ako proizvođač u svojoj obavijesti označi da je zlonamjerni akter aktivno iskoristio prijavljenu ranjivost i da, prema dostupnim informacijama, nije iskorištena ni u jednoj državi članici koja nije država članica CSIRT-a koji je imenovan koordinatorom i kojemu je proizvođač prijavio ranjivost, ako bi svako neposredno daljnje dijeljenje prijavljene ranjivosti vjerojatno dovelo do dostave informacija čije bi otkrivanje bilo u suprotnosti s ključnim interesima te države članice ili ako prijavljena ranjivost predstavlja neposredan visok kibernetički sigurnosni rizik koji proizlazi iz daljnjeg dijeljenja. U takvim slučajevima ENISA će dobiti samo istodobni pristup informacijama o tome da je proizvođač podnio obavijest, općim informacijama o predmetnom proizvodu s digitalnim elementima, informacijama o općoj prirodi iskorištavanja i informacijama o činjenici da je proizvođač istaknuo te sigurnosne razloge te da je stoga uskraćen puni sadržaj obavijesti. Potpuna obavijest zatim bi se trebala staviti na raspolaganje ENISA-i i drugim relevantnim CSIRT-ovima koji su imenovani koordinatorima ako CSIRT koji je imenovan koordinatorom koji je prvotno primio obavijest utvrdi da ti sigurnosni razlozi, koji odražavaju posebno iznimne okolnosti utvrđene u ovoj Uredbi, više ne postoje. Ako na temelju dostupnih informacija ENISA smatra da postoji sistemski rizik koji utječe na sigurnost unutarnjeg tržišta, ENISA bi trebala preporučiti CSIRT-u primatelju da proslijedi potpunu obavijest drugim CSIRT-ovima koji su imenovani koordinatorima i samoj ENISA-i.

(71) Kad proizvođači obavijeste o aktivno iskorištenoj ranjivosti ili značajnom incidentu koji utječu na sigurnost proizvoda s digitalnim elementima, trebali bi navesti koliko smatraju da su prijavljene informacije osjetljive. CSIRT koji je imenovan koordinatorom koji je prvotno primio obavijest trebao bi te informacije uzeti u obzir pri procjeni toga je li zbog obavijesti došlo do iznimnih okolnosti koje opravdavaju odgodu dijeljenja obavijesti drugim relevantnim CSIRT-ovima koji su imenovani koordinatorima na temelju opravdanih razloga povezanih s kibernetičkom sigurnošću. Te bi informacije trebalo uzeti u obzir i pri procjeni toga je li obavijest o aktivno iskorištenoj ranjivosti dovela do posebno iznimnih okolnosti koje opravdavaju da potpuna obavijest nije istodobno stavljena na raspolaganje ENISA-i. Naposljetku, CSIRT-ovi koji su imenovani koordinatorima trebali bi moći uzeti u obzir te informacije pri utvrđivanju odgovarajućih mjera za ublažavanje rizika koji proizlaze iz takvih ranjivosti i incidenata.

(72) Kako bi se pojednostavnilo izvješćivanje o informacijama koje se zahtijevaju na temelju ove Uredbe, uzimajući u obzir druge dodatne zahtjeve u pogledu izvješćivanja utvrđene u pravu Unije, kao što su Uredba (EU) 2016/679, Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća ([25]), Direktiva 2002/58/EZ Europskog parlamenta i Vijeća ([26]) i Direktiva (EU) 2022/2555, te kako bi se smanjilo administrativno opterećenje za subjekte, države članice potiče se da razmotre uvođenje jedinstvenih ulaznih točaka na nacionalnoj razini za takve zahtjeve u pogledu izvješćivanja. Upotreba takvih nacionalnih jedinstvenih ulaznih točaka za izvješćivanja o sigurnosnim incidentima u skladu s Uredbom (EU) 2016/679 i Direktivom 2002/58/EZ ne bi trebala utjecati na primjenu odredaba Uredbe (EU) 2016/679 i Direktive 2002/58/EZ, posebno onih koje se odnose na neovisnost tijela navedenih u njima. Pri uspostavi jedinstvene platforme za izvješćivanje iz ove Uredbe ENISA bi trebala uzeti u obzir mogućnost da se nacionalne krajnje točke za elektroničko obavješćivanje iz ove Uredbe integriraju u nacionalne jedinstvene ulazne točke koje mogu uključivati i druge obavijesti koje se zahtijevaju pravom Unije.

(73) Pri uspostavi jedinstvene platforme za izvješćivanje iz ove Uredbe i kako bi iskoristila prethodno iskustvo, ENISA bi se trebala savjetovati s drugim institucijama ili agencijama Unije koje upravljaju platformama ili bazama podataka koje podliježu strogim sigurnosnim zahtjevima, kao što je Agencija Europske unije za operativno upravljanje opsežnim informacijskim sustavima u području slobode, sigurnosti i pravde (eu-LISA). ENISA bi također trebala analizirati moguće komplementarnosti s europskom bazom podataka o ranjivostima koja je uspostavljena u skladu s člankom 12. stavkom 2. Direktive (EU) 2022/2555.

(74) Proizvođači i druge fizičke i pravne osobe trebali bi moći dobrovoljno obavijestiti CSIRT koji je imenovan koordinatorom ili ENISA-u o svakoj ranjivosti proizvoda s digitalnim elementima, kibernetičkim prijetnjama koje bi

([25]) Uredba (EU) 2022/2554 Europskog parlamenta i Vijeća od 14. prosinca 2022. o digitalnoj operativnoj otpornosti za financijski sektor i o izmjeni uredbi (EZ) br. 1060/2009, (EU) br. 648/2012, (EU) br. 600/2014, (EU) br. 909/2014 i (EU) 2016/1011 (SL L 333, 27.12.2022., str. 1.).

([26]) Direktiva 2002/58/EZ Europskog parlamenta i Vijeća od 12. srpnja 2002. o obradi osobnih podataka i zaštiti privatnosti u području elektroničkih komunikacija (Direktiva o privatnosti i elektroničkim komunikacijama) (SL L 201, 31.7.2002., str. 37.).

mogle utjecati na profil rizičnosti proizvoda s digitalnim elementima, o svakom incidentu koji utječe na sigurnost proizvoda s digitalnim elementima, kao i o izbjegnutim incidentima koji su mogli dovesti do takvog incidenta.

(75) U skladu s nacionalnim pravom države članice trebale bi, u mjeri u kojoj je to moguće, nastojati odgovoriti na izazove s kojima se suočavaju oni koji istražuju ranjivosti, uključujući njihovu moguću izloženost kaznenoj odgovornosti. S obzirom na to da bi fizičke i pravne osobe koje istražuju ranjivosti u nekim državama članicama mogle biti izložene kaznenoj i građanskopravnoj odgovornosti, države članice potiču se da donesu smjernice u pogledu neprovođenja kaznenog progona istraživača u području informacijske sigurnosti i izuzeća od građanskopravne odgovornosti za njihove aktivnosti.

(76) Proizvođači proizvoda s digitalnim elementima trebali bi uspostaviti politike koordiniranog otkrivanja ranjivosti kako bi pojedincima ili subjektima olakšali njihovo prijavljivanje, bilo izravno proizvođaču ili neizravno, i kada se to traži anonimno, putem CSIRT-ova koji su određeni kao koordinatori za potrebe koordiniranog otkrivanja ranjivosti u skladu s člankom 12. stavkom 1. Direktive (EU) 2022/2555. U politici koordiniranog otkrivanja ranjivosti proizvođačâ trebalo bi utvrditi strukturirani proces prijavljivanja ranjivosti proizvođaču na način koji omogućuje proizvođaču njihovo dijagnosticiranje i otklanjanje prije otkrivanja detaljnih informacija o ranjivostima trećim stranama ili javnosti. Štoviše, proizvođači bi trebali razmotriti i objavljivanje svojih sigurnosnih politika u strojno čitljivom formatu. S obzirom na činjenicu da se informacije o iskoristivim ranjivostima proizvoda s digitalnim elementima koji se nalaze u širokoj upotrebi mogu skupo prodati na crnom tržištu, proizvođači takvih proizvoda trebali bi moći upotrebljavati, u okviru svojih politika koordiniranog otkrivanja ranjivosti, programe za poticanje pojedinaca ili subjekata na prijavljivanje ranjivosti osiguravanjem priznanja i naknada za njihov trud. To se odnosi na takozvane „programe nagrađivanja pronalaska pogrešaka”.

(77) 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 poboljšavaju njihovo razumijevanje lanca opskrbe, što donosi višestruke koristi, a posebno pomaže proizvođačima i korisnicima da prate poznate nove ranjivosti i kibernetičke sigurnosne rizike. Osobito je važno da proizvođači osiguraju da njihovi proizvodi s digitalnim elementima ne sadržavaju ranjive komponente koje su razvile treće strane. Proizvođači ne bi trebali biti obvezni objaviti popis softverskog materijala.

(78) U okviru novih složenih poslovnih modela povezanih s internetskom prodajom poduzeće koje posluje na internetu može pružati niz usluga. Ovisno o prirodi usluga koje se pružaju u vezi s određenim proizvodom s digitalnim elementima, isti subjekt može biti pripadati u različite kategorije poslovnih modela ili gospodarskih subjekata. Ako subjekt pruža samo usluge internetskog posredovanja za određeni proizvod s digitalnim elementima i samo je pružatelj internetskog tržišta kako je definirano u članku 3. točki 14. Uredbe (EU) 2023/988, ne smatra se vrstom gospodarskog subjekta kako je definiran u ovoj Uredbi. Ako je isti subjekt pružatelj internetskog tržišta i također djeluje kao gospodarski subjekt kako je definiran u ovoj Uredbi za prodaju određenih proizvoda s digitalnim elementima trebao bi podlijegati obvezama utvrđenima u ovoj Uredbi za tu vrstu gospodarskog subjekta. Na primjer, ako pružatelj internetskog tržišta također distribuira proizvod s digitalnim elementima, onda bi se, kad je riječ o prodaji tog proizvoda, smatrao distributerom. Slično tome, ako predmetni subjekt prodaje proizvode s digitalnim elementima vlastite robne marke, smatrao bi se proizvođačem i stoga bi morao biti u skladu s primjenjivim zahtjevima za proizvođače. Osim toga, neki subjekti mogu se smatrati pružateljima usluga provođenja narudžbi kako su definirani u članku 3. točki 11. Uredbe (EU) 2019/1020 Europskog parlamenta i Vijeća ([27]) ako nude takve usluge. Takvi bi se slučajevi trebali procjenjivati pojedinačno. S obzirom na istaknutu ulogu koju internetska tržišta imaju u omogućavanju elektroničke trgovine, trebala bi nastojati surađivati s tijelima za nadzor tržišta država članica kako bi pomogla osigurati da su proizvodi s digitalnim elementima kupljeni putem internetskih tržišta u skladu sa zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi.

(79) Kako bi se olakšalo ocjenjivanje sukladnosti sa zahtjevima utvrđenim u ovoj Uredbi, trebala bi postojati pretpostavka sukladnosti proizvoda s digitalnim elementima koji su sukladni s usklađenim normama kojima su bitni zahtjevi u pogledu kibernetičke sigurnosti utvrđeni u ovoj Uredbi preneseni u detaljne tehničke specifikacije i koje su

([27]) 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.).

donesene u skladu s Uredbom (EU) br. 1025/2012 Europskog parlamenta i Vijeća ([28]). Tom uredbom predviđen je postupak podnošenja prigovora na usklađene norme ako te norme ne udovoljavaju u potpunosti zahtjevima utvrđenima u ovoj Uredbi. Postupak normizacije trebao bi osigurati uravnoteženu zastupljenost interesa i djelotvorno sudjelovanje dionika civilnog društva, uključujući organizacije potrošača. Trebalo bi uzeti u obzir i međunarodne norme koje su u skladu s razinom kibernetičke sigurnosne zaštite koja se nastoji postići bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi kako bi se olakšali razvoj usklađenih normi i provedba ove Uredbe te kako bi se poduzećima, posebno mikropoduzećima te malim i srednjim poduzećima i onima koja posluju na globalnoj razini, olakšala usklađenost.

(80) Pravovremeni razvoj usklađenih normi tijekom prijelaznog razdoblja za primjenu ove Uredbe i njihova dostupnost prije datuma početka primjene ove Uredbe bit će posebno važni za njezinu djelotvornu provedbu. To posebno vrijedi za važne proizvode s digitalnim elementima koji pripadaju u razred I. Dostupnost usklađenih normi omogućit će proizvođačima takvih proizvoda da provedu ocjenjivanje sukladnosti putem postupka unutarnje kontrole i stoga mogu izbjeći uska grla i kašnjenja u aktivnostima tijela za ocjenjivanje sukladnosti.

(81) Uredbom (EU) 2019/881 uspostavljen je dobrovoljni europski okvir za kibernetičku sigurnosnu certifikaciju IKT proizvoda, IKT procesa i IKT usluga. Europski programi kibernetičke sigurnosne certifikacije pružaju zajednički okvir povjerenja za korisnike u upotrebi proizvoda s digitalnim elementima obuhvaćenih područjem primjene ove Uredbe. Ovom bi se Uredbom posljedično trebale stvoriti sinergije s Uredbom (EU) 2019/881. Kako bi se olakšalo ocjenjivanje sukladnosti sa zahtjevima utvrđenima u ovoj Uredbi, proizvodi s digitalnim elementima koji su certificirani ili za koje je izdana izjava o sukladnosti u okviru europskog programa kibernetičke sigurnosti u skladu s Uredbom (EU) 2019/881 i koji je Komisija utvrdila provedbenim aktom smatraju se usklađenima s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi u mjeri u kojoj europski kibernetički sigurnosni 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 kibernetičke sigurnosne certifikacije za proizvode s digitalnim elementima, uključujući pri izradi tekućeg programa rada Unije u skladu s Uredbom (EU) 2019/881. Ako postoji potreba za novim programom koji obuhvaća proizvode s digitalnim elementima, među ostalim kako bi se olakšala usklađenost s ovom Uredbom, Komisija može zatražiti od ENISA-e da izradi prijedloge programa u skladu s člankom 48. Uredbe (EU) 2019/881. U okviru takvih budućih europskih programa kibernetičke sigurnosne certifikacije koji bi obuhvaćali proizvode s digitalnim elementima trebalo bi uzeti u obzir bitne zahtjeve u pogledu kibernetičke sigurnosti i postupke ocjenjivanja sukladnosti kako su utvrđeni u ovoj Uredbi i olakšati usklađenost s ovom Uredbom. Za europske programe kibernetičke sigurnosne certifikacije koji stupaju na snagu prije stupanja na snagu ove Uredbe možda će biti potrebne dodatne specifikacije o detaljnim aspektima primjene pretpostavke sukladnosti. Komisiju bi trebalo ovlastiti da delegiranim aktima odredi pod kojim se uvjetima europski programi kibernetičke sigurnosne certifikacije mogu upotrebljavati za dokazivanje sukladnosti s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi. Nadalje, kako bi se izbjeglo neopravdano administrativno opterećenje, proizvođači ne bi trebali imati obvezu ocjenjivanja sukladnosti koje provodi treća strana kako je predviđeno u ovoj Uredbi za odgovarajuće zahtjeve ako je u okviru takvih europskih programa kibernetičke sigurnosne certifikacije izdan europski kibernetički sigurnosni certifikat na razini koja je barem „znatna”.

(82) Nakon stupanja na snagu Provedbene uredbe (EU) 2024/482 koja se odnosi na proizvode obuhvaćene područjem primjene ove Uredbe, kao što su hardverski sigurnosni moduli i mikroprocesori, Komisija bi trebala moći delegiranim aktom odrediti kako se EUCC-om predviđa pretpostavka sukladnosti s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi ili njezinim dijelovima. Nadalje, takvim delegiranim aktom može se odrediti na koji način certifikat izdan na temelju EUCC-a oslobađa proizvođače od obveze ocjenjivanja koje provodi treća strana kako se zahtijeva u skladu s ovom Uredbom za odgovarajuće zahtjeve.

(83) Postojeći europski okvir za normizaciju koji se temelji na načelima novog pristupa iz Rezolucije Vijeća od 7. svibnja 1985. o novom pristupu tehničkom usklađivanju i normama te na Uredbi (EU) br. 1025/2012 predstavlja standardni okvir za izradu normi kojima se predviđa pretpostavka sukladnosti s relevantnim bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi. Europske norme trebale bi biti tržišno orijentirane, uzimati u obzir javni interes i ciljeve politika koji su jasno navedeni u zahtjevu Komisije upućenom jednoj ili više europskih organizacija za normizaciju da u zadanom roku izrade usklađene norme i trebale bi se temeljiti na konsenzusu. Međutim, ako ne postoje relevantna upućivanja na usklađene norme, Komisija bi trebala moći donijeti

([28]) 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.).

provedbene akte kojima se utvrđuju zajedničke specifikacije za bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u ovoj Uredbi, pod uvjetom da se time na odgovarajući način poštuju uloga i funkcije europskih organizacija za normizaciju, kao iznimno zamjensko rješenje kojim se olakšava obveza proizvođača da postupa u skladu s tim bitnim zahtjevima u pogledu kibernetičke sigurnosti, ako je postupak normizacije blokiran ili ako postoje kašnjenja u utvrđivanju odgovarajućih usklađenih normi. Ako je takvo kašnjenje posljedica tehničke složenosti predmetne norme, Komisija bi to trebala uzeti u obzir prije razmatranja utvrđivanja zajedničkih specifikacija.

(84) Kako bi se zajedničke specifikacije koje obuhvaćaju bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u ovoj Uredbi utvrdile na najučinkovitiji način, Komisija bi u proces trebala uključiti relevantne dionike.

(85) Razumno razdoblje znači, u odnosu na objavu upućivanja na usklađene norme u *Službenom listu Europske unije* u skladu s Uredbom (EU) br. 1025/2012, razdoblje tijekom kojeg se očekuje objava upućivanja na normu, njezina ispravka ili njezine izmjene u *Službenom listu Europske unije* i koje ne bi trebalo biti dulje od godine dana nakon roka za izradu europske norme utvrđenog u skladu s Uredbom (EU) br. 1025/2012.

(86) Kako bi se olakšalo ocjenjivanje sukladnosti s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi, 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 navođenja detaljnih tehničkih specifikacija tih zahtjeva.

(87) Primjenom usklađenih normi, zajedničkih specifikacija ili europskih programa kibernetičke sigurnosne certifikacije donesenih na temelju Uredbe (EU) 2019/881 kojima se predviđa pretpostavka sukladnosti u odnosu na bitne zahtjeve u pogledu kibernetičke sigurnosti primjenjive na proizvode s digitalnim elementima olakšat će se ocjenjivanje sukladnosti koje provode proizvođači. Ako proizvođač odluči ne primijeniti takva sredstva za određene zahtjeve, u svojoj tehničkoj dokumentaciji mora navesti kako se postiže usklađenost na neki drugi način. Nadalje, primjenom usklađenih normi, zajedničkih specifikacija ili europskih programa kibernetičke sigurnosne certifikacije donesenih na temelju Uredbe (EU) 2019/881 kojima se predviđa pretpostavka sukladnosti proizvođačâ tijelima za nadzor tržišta olakšala bi se provjera usklađenosti proizvoda s digitalnim elementima. Stoga se proizvođače proizvoda s digitalnim elementima potiče na primjenu takvih usklađenih normi, zajedničkih specifikacija ili europskih programa kibernetičke sigurnosne certifikacije.

(88) Proizvođači bi trebali sastaviti EU izjavu o sukladnosti kako bi pružili informacije koje se zahtijevaju ovom Uredbom o sukladnosti proizvoda s digitalnim elementima s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi i, ako je primjenjivo, drugim relevantnim zakonodavstvom Unije o usklađivanju kojim je obuhvaćen taj proizvod s digitalnim elementima. Od proizvođača se može i drugim pravnim aktima Unije zahtijevati sastavljanje EU izjave o sukladnosti. Kako bi se osigurao djelotvoran pristup informacijama u svrhu nadzora tržišta, trebalo bi sastaviti jedinstvenu EU izjavu o sukladnosti koja se odnosi na usklađenost sa svim relevantnim pravnim aktima Unije. Kako bi se smanjilo administrativno opterećenje gospodarskih subjekata, trebalo bi omogućiti da se ta jedinstvena EU izjava o sukladnosti sastoji od dokumentacije sastavljene od relevantnih pojedinačnih izjava o sukladnosti.

(89) Oznaka CE, koja označuje sukladnost proizvoda, vidljiva je posljedica cijelog procesa koji obuhvaća ocjenjivanje sukladnosti u širem smislu. Opća načela kojima se uređuje stavljanje oznake CE utvrđena su u Uredbi (EZ) br. 765/2008 Europskog parlamenta i Vijeća ([29]). Ovom Uredbom trebalo bi utvrditi pravila za stavljanje oznake CE na proizvode s digitalnim elementima. Oznaka CE trebala bi biti jedina oznaka kojom se jamči usklađenosti proizvoda s digitalnim elementima sa zahtjevima utvrđenima u ovoj Uredbi.

(90) Kako bi se gospodarskim subjektima omogućilo da dokažu sukladnost s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi, a tijelima za nadzor tržišta da osiguraju da su proizvodi s digitalnim elementima koji su stavljeni na raspolaganje na tržištu usklađeni s tim zahtjevima, potrebno je utvrditi postupke ocjenjivanja sukladnosti. Odlukom br. 768/2008/EZ Europskog parlamenta i Vijeća ([30]) utvrđeni su moduli za

([29]) 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.).

([30]) 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.).

postupke ocjenjivanja sukladnosti razmjerno razini uključenog rizika i razini sigurnosti koja se zahtijeva. Kako bi se postigla međusektorska usklađenost i izbjegle *ad hoc* varijante, postupci ocjenjivanja sukladnosti prikladni za provjeru sukladnosti proizvoda s digitalnim elementima s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi trebali bi se temeljiti na tim modulima. U postupcima ocjenjivanja sukladnosti trebalo bi ispitati i provjeriti kako zahtjeve u pogledu proizvoda tako i zahtjeve u pogledu procesa koji se odnose cijeli životni ciklus proizvoda s digitalnim elementima, uključujući planiranje, projektiranje, razvoj ili proizvodnju, ispitivanje i održavanje proizvoda s digitalnim elementima.

(91) Ocjenjivanje sukladnosti proizvoda s digitalnim elementima koji u ovoj Uredbi nisu navedeni kao važni ili kritični proizvodi s digitalnim elementima može provoditi proizvođač na vlastitu odgovornost primjenom postupka unutarnje kontrole koji se temelji na modulu A iz Odluke br. 768/2008/EZ u skladu s ovom Uredbom. To se primjenjuje i na slučajeve u kojima proizvođač odluči da neće primjenjivati u cijelosti ili djelomično primjenjivu usklađenu normu, zajedničku specifikaciju ili europski program kibernetičke sigurnosne certifikacije. Proizvođač zadržava mogućnost odabira strožeg postupka ocjenjivanja sukladnosti koji uključuje treću stranu. U okviru postupka unutarnje kontrole za ocjenjivanje sukladnosti proizvođač osigurava i izjavljuje na vlastitu odgovornost da proizvod s digitalnim elementima i procesi proizvođača ispunjavaju primjenjive bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u ovoj Uredbi. Ako važan proizvod s digitalnim elementima pripada u I. razred, zahtijeva se dodatno jamstvo za dokazivanje sukladnosti s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima ovom Uredbom. Ako proizvođač želi provesti ocjenjivanje sukladnosti na vlastitu odgovornost (modul A), trebao bi primjenjivati usklađene norme, zajedničke specifikacije ili programe europske kibernetičke sigurnosne certifikacije donesene na temelju Uredbe (EU) 2019/881 koje je Komisija utvrdila provedbenim aktom. Ako proizvođač ne primjenjuje takve usklađene norme, zajedničke specifikacije ili europske programe kibernetičke sigurnosne certifikacije, trebao bi se podvrgnuti ocjenjivanju sukladnosti koje uključuje treću stranu (koje se temelji na modulima B i C ili modulu H). Uzimajući u obzir administrativno opterećenje proizvođača i to da kibernetička sigurnost ima važnu ulogu u fazi projektiranja i razvoja materijalnih i nematerijalnih proizvoda s digitalnim elementima, postupci ocjenjivanja sukladnosti koji se temelje na modulima B i C ili modulu H iz Odluke br. 768/2008/EZ odabrani su kao najprikladniji za ocjenjivanje usklađenosti važnih proizvoda s digitalnim elementima na proporcionalan i djelotvoran način. Proizvođač koji provodi ocjenjivanje sukladnosti treće strane može odabrati postupak koji najbolje odgovara njegovu procesu projektiranja i proizvodnje. S obzirom na još veći kibernetički sigurnosni rizik povezan s upotrebom važnih proizvoda s digitalnim elementima koji pripadaju u II. razred, ocjenjivanje sukladnosti uvijek bi trebalo uključivati treću stranu, čak i ako je proizvod u potpunosti ili djelomično usklađen s usklađenim normama, zajedničkim specifikacijama ili europskim programima kibernetičke sigurnosne certifikacije. Proizvođači važnih proizvoda s digitalnim elementima koji se smatraju besplatnim softverom otvorenog koda trebali bi moći slijediti postupak unutarnje kontrole na temelju modula A, pod uvjetom da tehničku dokumentaciju učine javno dostupnom.

(92) 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 usklađenosti proizvoda s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u ovoj Uredbi u fazama projektiranja, razvoja i proizvodnje primjenjuju relevantni moduli ocjenjivanja sukladnosti, trebalo bi se smatrati da te aktivnosti predstavljaju proizvodnju.

(93) Kad je riječ o mikropoduzećima i malim poduzećima, kako bi se osigurala proporcionalnost, primjereno je smanjiti administrativne troškove, a da se pritom ne utječe na razinu kibernetičke sigurnosne zaštite proizvoda s digitalnim elementima koji su obuhvaćeni područjem primjene ove Uredbe ili na ravnopravne uvjete među proizvođačima. Stoga je primjereno da Komisija utvrdi pojednostavnjeni obrazac tehničke dokumentacije usmjeren na potrebe mikropoduzeća i malih poduzeća. Pojednostavnjeni obrazac tehničke dokumentacije koji donosi Komisija trebao bi obuhvaćati sve primjenjive elemente povezane s tehničkom dokumentacijom utvrđenom u ovoj Uredbi i navesti kako mikropoduzeće ili malo poduzeće može sažeto dostaviti tražene elemente, kao što je opis projektiranja, razvoja i proizvodnje proizvoda s digitalnim elementima. Na taj način bi se tim obrascem doprinijelo smanjenju administrativnog opterećenja koje nastaje zbog usklađivanja tako što bi se predmetnim poduzećima pružila pravna sigurnost u pogledu opsega i detaljnosti informacija koje treba pružiti. Mikropoduzeća i mala poduzeća trebala bi moći odlučiti hoće li dostaviti primjenjive elemente povezane s tehničkom dokumentacijom putem opsežnog obrasca ili putem pojednostavnjenog obrasca koji im je dostupan.

(94) Kako bi se promicale i zaštitile inovacije, važno je da se posebno uzmu u obzir interesi proizvođača koji su mikropoduzeća ili mala ili srednja poduzeća, a posebno mikropoduzeća i mala poduzeća, uključujući start-up poduzeća. U tu bi svrhu države članice mogle osmisliti inicijative za proizvođače koji su mikropoduzeća ili mala poduzeća u vezi s, među ostalim osposobljavanjem, podizanjem svijesti, informiranjem, ispitivanjem i aktivnostima ocjenjivanja sukladnosti trećih strana, kao i stvaranjem izoliranih okruženja. Troškovi prijevoda koji se odnose na obveznu dokumentaciju, kao što su tehnička dokumentacija te informacije i upute za korisnika koje se zahtijevaju u skladu s ovom Uredbom, te komunikaciju s nadležnim tijelima, mogu predstavljati znatan trošak za proizvođače, posebno za manje proizvođače. Stoga bi države članice trebale moći smatrati da je jezik koji odrede i prihvaćaju za relevantnu dokumentaciju proizvođača i komunikaciju s proizvođačima jedan od jezika koji u velikoj mjeri razumije najveći mogući broj korisnika.

(95) Kako bi se osigurala neometana primjena ove Uredbe, države članice bi prije datuma početka primjene ove Uredbe trebale nastojati osigurati da je dostupan dovoljan broj prijavljenih tijela za ocjenjivanja sukladnosti koja provodi treća strana. Komisija bi trebala nastojati pomoći državama članicama i drugim relevantnim stranama u tom nastojanju kako bi se izbjegla uska grla i prepreke ulasku proizvođača na tržište. Ciljanim aktivnostima osposobljavanja koje provode države članice, među ostalim prema potrebi uz potporu Komisije, može se doprinijeti dostupnosti kvalificiranih stručnjaka, među ostalim za potporu aktivnostima prijavljenih tijela na temelju ove Uredbe. Nadalje, s obzirom na troškove koje može podrazumijevati ocjenjivanje sukladnosti koje provodi treća strana, trebalo bi razmotriti inicijative financiranja na razini Unije i na nacionalnoj razini kojima se nastoje smanjiti takvi troškovi za mikropoduzeća i mala poduzeća.

(96) Kako bi se osigurala proporcionalnost, tijela za ocjenjivanje sukladnosti pri određivanju naknada za postupke ocjenjivanja sukladnosti trebala bi uzeti u obzir posebne interese i potrebe mikropoduzeća te malih i srednjih poduzeća, uključujući start-up poduzeća. Posebno, tijela za ocjenjivanje sukladnosti trebala bi primjenjivati relevantni postupak ispitivanja i ispitivanja predviđena ovom Uredbom samo ako je to primjereno i u skladu s pristupom koji se temelji na procjeni rizika.

(97) Ciljevi regulatornih izoliranih okruženja trebali bi biti poticanje inovacija i konkurentnosti poduzeća uspostavom kontroliranih okruženja za testiranje prije stavljanja na tržište proizvoda s digitalnim elementima. Regulatorna izolirana okruženja trebala bi doprinijeti poboljšanju pravne sigurnosti za sve aktere obuhvaćene područjem primjene ove Uredbe te olakšati i ubrzati pristup tržištu Unije za proizvode s digitalnim elementima, posebno ako ih pružaju mikropoduzeća i mala poduzeća, uključujući start-up poduzeća.

(98) 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 su u skladu sa skupom zahtjeva, posebno u pogledu neovisnosti, stručnosti i nepostojanja sukoba interesa.

(99) 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 u ovoj Uredbi trebalo bi dopuniti akreditacijskim sustavom predviđenim u Uredbi (EZ) br. 765/2008. S obzirom na to da je akreditacija bitno sredstvo za provjeru stručnosti tijela za ocjenjivanje sukladnosti, trebala bi se upotrebljavati i u svrhu prijavljivanja.

(100) Tijela za ocjenjivanje sukladnosti koja su akreditirana i prijavljena u skladu s pravom Unije kojim se utvrđuju zahtjevi slični onima utvrđenima u ovoj Uredbi, kao što je tijelo za ocjenjivanje sukladnosti koje je prijavljeno za europski program kibernetičke sigurnosne certifikacije donesen na temelju Uredbe (EU) 2019/881 ili je prijavljeno na temelju Delegirane uredbe (EU) 2022/30, trebalo bi ponovno ocijeniti i prijaviti u skladu s ovom Uredbom. Međutim, relevantna tijela mogu definirati sinergije u pogledu svih zahtjeva koji se preklapaju kako bi se spriječilo nepotrebno financijsko i administrativno opterećenje te osigurao neometan i pravodoban postupak prijavljivanja.

(101) Nacionalna javna tijela u cijeloj Uniji trebala bi transparentnu akreditaciju predviđenu Uredbom (EZ) br. 765/2008, kojom se osigurava potrebna razina povjerenja u certifikate o sukladnosti, smatrati preferiranim sredstvom dokazivanja tehničke stručnosti tijela za ocjenjivanje sukladnosti. Međutim, nacionalna tijela mogu smatrati da raspolažu primjerenim sredstvima da sami provedu 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 dokaznu dokumentaciju o usklađenosti evaluiranih tijela za ocjenjivanje sukladnosti s relevantnim regulatornim zahtjevima.

(102) Tijela za ocjenjivanje sukladnosti često podugovaraju dio svojih aktivnosti povezanih s ocjenjivanjem sukladnosti ili ih prenose na društvo kćer. Kako bi se zaštitila razina zaštite koja se zahtijeva za stavljanje na tržište proizvoda s digitalnim elementima, ključno je da podugovaratelji i društva kćeri koji ocjenjuju sukladnost ispunjavaju jednake zahtjeve kao prijavljena tijela u odnosu na ocjenjivanje sukladnosti.

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

(104) S obzirom na to 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 predvidjeti razdoblje u kojem se sve sumnje ili pitanja koja se odnose na stručnost tijela za ocjenjivanje sukladnosti mogu razjasniti prije nego što počnu djelovati kao prijavljena tijela.

(105) U interesu konkurentnosti ključno je da prijavljena tijela primjenjuju postupke ocjenjivanja sukladnosti bez stvaranja nepotrebnog opterećenja za gospodarske subjekte. Iz istog razloga i radi osiguravanja jednakog postupanja prema gospodarskim subjektima treba osigurati dosljednost pri tehničkoj primjeni postupaka ocjenjivanja sukladnosti. Primjerena koordinacija i suradnja prijavljenih tijela trebali bi biti najbolji načini da se to postigne.

(106) Nadzor tržišta ključan je instrument za osiguravanje pravilne i ujednačene primjene prava Unije. Stoga je primjereno uspostaviti pravni okvir na temelju kojeg se nadzor tržišta može provoditi na odgovarajući način. Na proizvode s digitalnim elementima koji su obuhvaćeni područjem primjene ove Uredbe primjenjuju se pravila o nadzoru tržišta Unije i kontroli proizvoda koji ulaze na tržište Unije predviđena Uredbom (EU) 2019/1020.

(107) U skladu s Uredbom (EU) 2019/1020 tijelo za nadzor tržišta provodi nadzor tržišta na državnom području države članice koja ga imenuje. Ova Uredba ne bi trebala spriječiti države članice da odaberu nadležna tijela za obavljanje zadaća nadzora tržišta. Svaka država članica trebala bi na svojem državnom području imenovati jedno ili više tijela za nadzor tržišta. Države članice trebale bi moći izabrati da kao tijelo za nadzor tržišta imenuju bilo koje postojeće ili novo tijelo, uključujući nadležna tijela koja su imenovana ili uspostavljena u skladu s člankom 8. Direktive (EU) 2022/2555, nacionalna tijela za kibernetičku sigurnosnu certifikaciju imenovana u skladu s člankom 58. Uredbe (EU) 2019/881 ili tijela za nadzor tržišta imenovana za potrebe Direktive 2014/53/EU. Gospodarski subjekti trebali bi u potpunosti surađivati s tijelima za nadzor tržišta i drugim nadležnim tijelima. Svaka država članica trebala bi obavijestiti Komisiju i ostale države članice o svojim tijelima za nadzor tržišta i područjima nadležnosti svakog od tih tijela te bi trebala osigurati potrebne resurse i vještine za obavljanje zadaća nadzora tržišta koje se odnose na ovu Uredbu. U skladu s člankom 10. stavcima 2. i 3. Uredbe (EU) 2019/1020 svaka država članica trebala bi odrediti 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.

(108) Radi ujednačene primjene ove Uredbe trebalo bi uspostaviti posebnu skupinu za ADCO za kibernetičku otpornost proizvoda s digitalnim elementima u skladu s člankom 30. stavkom 2. Uredbe (EU) 2019/1020. Skupina za ADCO trebala bi biti sastavljena od predstavnika imenovanih tijela za nadzor tržišta i, ako je primjereno, 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 u skladu s člankom 29. Uredbe (EU) 2019/1020 i sastoji se od predstavnika svake države članice, uključujući predstavnika svakog jedinstvenog ureda za vezu iz članka 10. te Uredbe i, prema potrebi, nacionalnog stručnjaka, predsjednikâ skupina za ADCO i predstavnikâ Komisije. Komisija bi trebala sudjelovati na sastancima Mreže Unije za sukladnost proizvoda, njezinih podskupina i skupine za ADCO. Ona bi trebala i pomagati skupini za ADCO preko izvršnog tajništva koje pruža tehničku i logističku potporu. Skupina za ADCO može pozvati i neovisne stručnjake da sudjeluju i da se povežu s drugim skupinama za ADCO, kao što je ona uspostavljena Direktivom 2014/53/EU.

(109) Tijela za nadzor tržišta, putem skupine za ADCO uspostavljene ovom Uredbom, trebala bi blisko surađivati i trebala bi moći izraditi dokumente sa smjernicama za olakšavanje aktivnosti nadzora tržišta na nacionalnoj razini, primjerice razvojem najbolje prakse i pokazatelja za djelotvornu provjeru usklađenosti proizvoda s digitalnim elementima s ovom Uredbom.

(110) Kako bi se osigurale pravodobne, proporcionalne i djelotvorne mjere povezane s proizvodima s digitalnim elementima koji predstavljaju znatan kibernetički sigurnosni 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, ako je potrebno djeluju u ranijoj fazi. Ako se države članice i Komisija slažu o opravdanosti mjere koju je poduzela država članica, daljnje sudjelovanje Komisije ne bi trebalo biti potrebno, osim ako se neusklađenost može pripisati nedostacima usklađene norme.

(111) U određenim slučajevima proizvod s digitalnim elementima koji je usklađen s ovom Uredbom može ipak predstavljati znatan kibernetički sigurnosni rizik ili 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 kako su navedeni u članku 3. stavku 1. Direktive (EU) 2022/2555 ili rizik za druge aspekte zaštite javnog interesa. Stoga je potrebno uspostaviti pravila koja osiguravaju ublažavanje tih rizika. Tijela za nadzor tržišta posljedično bi trebala poduzeti mjere kako bi se od gospodarskog subjekta zahtijevalo da osigura 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 s digitalnim elementima na takav način, država članica trebala bi bez odgode obavijestiti Komisiju i ostale države članice o privremenim mjerama, navodeći razloge i obrazloženje odluke. Ako tijelo za nadzor tržišta donese takve mjere u odnosu na proizvode s digitalnim elementima 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 ili nije. Komisija bi svoju odluku trebala uputiti svim državama članicama te je odmah dostaviti svim državama članicama i relevantnom gospodarskom subjektu odnosno relevantnim gospodarskim subjektima. Ako se mjera smatra opravdanom, Komisija bi također trebala razmotriti donošenje prijedlogâ za reviziju relevantnog prava Unije.

(112) Za proizvode s digitalnim elementima koji predstavljaju znatan kibernetički sigurnosni rizik i ako postoji razlog za vjerovati da oni nisu u skladu s ovom Uredbom ili za proizvode koji su u skladu s ovom Uredbom, ali predstavljaju druge važne rizike, kao što su rizici za zdravlje ili sigurnost osoba, za ispunjavanje obveza na temelju prava Unije ili nacionalnog prava za zaštitu temeljnih prava ili za dostupnost, autentičnost, cjelovitost ili povjerljivost usluga koje pomoću elektroničkog informacijskog sustava nude ključni subjekti kako su navedeni u članku 3. stavku 1. Direktive (EU) 2022/2555, Komisija bi trebala moći zatražiti od ENISA-e da provede evaluaciju. Na temelju te evaluacije Komisija bi trebala moći provedbenim aktima donijeti korektivne ili restriktivne mjere na razini Unije, uključujući zahtijevanje povlačenja s tržišta predmetnih proizvoda s digitalnim elementima ili njihova opoziva u razumnom roku, razmjerno vrsti rizika. Komisija bi trebala moći pribjeći takvoj intervenciji samo u iznimnim okolnostima koje opravdavaju brzu intervenciju radi očuvanja pravilnog funkcioniranja unutarnjeg tržišta i samo ako tijela za nadzor tržišta nisu poduzela djelotvorne mjere za ispravljanje situacije. Takve iznimne okolnosti mogu biti izvanredne situacije u kojima na primjer proizvođač omogući široku dostupnost neusklađenog proizvoda s digitalnim elementima u nekoliko država članica, koji usto u ključnim sektorima rabe subjekti obuhvaćeni područjem primjene Direktive (EU) 2022/2555, pri čemu sadržava poznate ranjivosti koje zlonamjerni akteri iskorištavaju i za koje proizvođač ne pruža dostupne zakrpe. Komisija bi trebala moći intervenirati u takvim izvanrednim situacijama samo dok traju iznimne okolnosti i ako neusklađenost s ovom Uredbom ili važni rizici koje proizvod predstavlja potraju.

(113) Ako postoje naznake neusklađenost s ovom Uredbom u nekoliko država članica, tijela za nadzor tržišta trebala bi moći provoditi zajedničke aktivnosti s drugim tijelima radi provjere usklađenosti i utvrđivanja kibernetičkih sigurnosnih rizika proizvoda s digitalnim elementima.

(114) Istodobne koordinirane kontrolne mjere („opsežne provjere”) posebne su mjere izvršavanja 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 s digitalnim elementima često predstavljaju kibernetičke sigurnosne rizike. Nadalje, pri određivanju kategorija proizvoda koje treba podvrgnuti opsežnim provjerama, tijela za nadzor tržišta trebala bi uzeti u obzir i okolnosti koje se odnose na netehničke čimbenike rizika. U tu bi svrhu tijela za nadzor tržišta trebala moći uzeti u obzir rezultate koordiniranih procjena sigurnosnih rizika ključnih lanaca opskrbe na razini Unije provedenih u skladu s člankom 22. Direktive (EU) 2022/2555, uključujući okolnosti koje se odnose na netehničke čimbenike rizika. ENISA bi tijelima za nadzor tržišta trebala podnijeti prijedloge kategorija proizvoda s digitalnim elementima za koje bi se mogle organizirati opsežne provjere, na temelju, među ostalim, obavijesti o ranjivostima proizvoda i incidentima koje primi.

(115) S obzirom na svoju stručnost i ovlasti ENISA bi trebala moći pružati potporu procesu provedbe ove Uredbe. ENISA bi posebno trebala moći predlagati zajedničke aktivnosti koje bi provodila tijela za nadzor tržišta na temelju naznaka ili informacija povezanih s potencijalnom neusklađenošću proizvodâ s digitalnim elementima s ovom Uredbom u nekoliko država članica ili utvrditi kategorije proizvoda za koje bi trebalo organizirati opsežne provjere. U iznimnim okolnostima, ako je potrebna brza intervencija radi očuvanja pravilnog funkcioniranja unutarnjeg tržišta, ENISA bi, na zahtjev Komisije, trebala moći provesti evaluacije u pogledu određenih proizvoda s digitalnim elementima koji predstavljaju znatan kibernetički sigurnosni rizik.

(116) Ovom se Uredbom ENISA-i dodjeljuju određene zadaće za koje su potrebni odgovarajući resursi, kako u pogledu stručnosti tako i ljudskih resursa, kako bi se ENISA-i omogućilo da djelotvorno izvršava te zadaće. Komisija će pri pripremi nacrta općeg proračuna Unije predložiti potrebna proračunska sredstva za plan radnih mjesta ENISA-e u skladu s postupkom utvrđenim u članku 29. Uredbe (EU) 2019/881. Tijekom tog procesa Komisija će razmotriti ukupne resurse ENISA-e kako bi joj se omogućilo da ispuni svoje zadaće, uključujući one koje su ENISA-i dodijeljene na temelju ove Uredbe.

(117) Kako bi se osiguralo da se regulatorni okvir može prilagođavati ako je to potrebno, Komisiji bi trebalo delegirati ovlast za donošenje akata u skladu s člankom 290. Ugovora o funkcioniranju Europske unije (UFEU) u vezi s ažuriranjem priloga ovoj Uredbi u kojem se navode važni proizvodi s digitalnim elementima. 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, navodeći, ako je primjenjivo, je li potrebno ograničenje područja primjene ove Uredbe ili isključenje iz područja primjene ove Uredbe te opseg tog ograničenja. Ovlast za donošenje akata u skladu s tim člankom Komisiji bi trebalo delegirati i u vezi s potencijalnim uvođenjem obveze certifikacije u okviru europskog programa kibernetičke sigurnosne certifikacije kritičnih proizvoda s digitalnim elementima utvrđenih u prilogu ovoj Uredbi, kao i za ažuriranje popisa kritičnih proizvoda s digitalnim elementima na temelju kriterija kritičnosti utvrđenih u ovoj Uredbi, te za utvrđivanje europskih programa kibernetičke sigurnosne certifikacije donesenih na temelju Uredbe (EU) 2019/881 koji se mogu upotrijebiti za dokazivanje sukladnosti s bitnim zahtjevima u pogledu kibernetičke sigurnosti ili njihovim dijelovima kako su utvrđeni u prilogu ovoj Uredbi. Komisiji bi trebalo delegirati i ovlast za donošenje akata kako bi se odredilo minimalno razdoblje potpore za određene kategorije proizvoda ako podaci o nadzoru tržišta pokazuju da su razdoblja potpore neprimjerena te kako bi se odredili uvjeti za primjenu razloga povezanih s kibernetičkom sigurnošću u vezi s odgodom širenja obavijesti o aktivno iskorištenim ranjivostima. Nadalje, Komisiji bi trebalo delegirati ovlast za donošenje akata radi uspostave dobrovoljnih programa za sigurnosne potvrde o ocjenjivanju sukladnosti proizvoda s digitalnim elementima koji se smatraju besplatnim softverom otvorenog koda sa svim ili određenim bitnim zahtjevima u pogledu kibernetičke sigurnosti ili drugim obvezama utvrđenima 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. ([31]). 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. Ovlast za donošenje delegiranih akata u skladu s ovom Uredbom trebala bi se dodijeliti Komisiji na razdoblje od pet godina počevši od 10. prosinca 2024. Komisija bi trebala izraditi izvješće o delegiranju ovlasti najkasnije devet mjeseci prije kraja razdoblja od pet godina. Delegiranje ovlasti prešutno bi se trebalo produljiti za razdoblja jednakog trajanja, osim ako se Europski parlament ili Vijeće tom produljenju usprotive najkasnije tri mjeseca prije kraja svakog razdoblja.

(118) Radi osiguranja jedinstvenih uvjeta za provedbu ove Uredbe, provedbene ovlasti trebalo bi dodijeliti Komisiji za određivanje tehničkog opisa kategorija važnih proizvoda s digitalnim elementima utvrđenih u prilogu ovoj Uredbi, određivanje formata i elemenata popisa softverskog materijala, pobliže određivanje formata i postupka podnošenja obavijesti o aktivno iskorištenim ranjivostima i značajnim incidentima koji utječu na sigurnost proizvoda s digitalnim elementima koje podnose proizvođači, utvrđivanje zajedničkih specifikacija koje obuhvaćaju tehničke zahtjeve kojima se osigurava sredstvo za usklađivanje s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u prilogu ovoj Uredbi, utvrđivanje tehničkih specifikacija za oznake, piktograme i sve druge oznake povezane sa sigurnošću proizvoda s digitalnim elementima, njihova razdoblja potpore te mehanizama za promicanje njihove upotrebe i podizanje javne svijesti o sigurnosti proizvoda s digitalnim elementima, utvrđivanje pojednostavnjenog obrasca dokumentacije namijenjenog potrebama mikropoduzeća i malih poduzeća te

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

odlučivanje o korektivnim ili restriktivnim mjerama na razini Unije u iznimnim okolnostima koje opravdavaju brzu intervenciju radi očuvanja pravilnog funkcioniranja unutarnjeg tržišta. Te bi ovlasti trebalo izvršavati u skladu s Uredbom (EU) br. 182/2011 Europskog parlamenta i Vijeća ([32]).

(119) Kako bi se osigurala konstruktivna suradnja koja se temelji na povjerenju između 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 pribavljenih pri obavljanju svojih zadaća.

(120) Kako bi se osiguralo djelotvorno 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 nacionalnom pravu 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 je li proizvođač mikropoduzeće ili malo ili srednje poduzeće, uključujući start-up poduzeće i jesu li ista ili druga tijela za nadzor tržišta već izrekla upravne novčane kazne istom gospodarskom subjektu za slična kršenja. Takve bi okolnosti mogle biti otegotne, u situacijama u kojima isti gospodarski subjekt nastavlja s kršenjem na državnim područjima država članica koje nisu država članica 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 kršenja 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 kršenja trebala bi osigurati poštovanje načela proporcionalnosti. S obzirom na to da se upravne novčane kazne zbog nepoštovanja roka od 24 sata za rano upozorenje o aktivno iskorištenim ranjivostima ili značajnim incidentima koji utječu na sigurnost proizvoda s digitalnim elementima ne primjenjuju na mikropoduzeća ili mala poduzeća, kao ni na upravitelje softvera otvorenog koda za bilo koje kršenje ove Uredbe te podložno načelu da bi sankcije trebale biti učinkovite, proporcionalne i odvraćajuće, države članice tim subjektima ne bi trebale nametati druge vrste novčanih kazni.

(121) Ako su upravne novčane kazne izrečene osobi koja nije 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 moći utvrditi i trebaju li i do koje mjere primjenjivati upravne novčane kazne za javna tijela.

(122) Države članice trebale bi, uzimajući u obzir nacionalne okolnosti, ispitati mogućnost upotrebe prihoda od sankcija predviđenih u ovoj Uredbi ili njihova financijskog ekvivalenta za potporu kibernetičkim sigurnosnim politikama i povećanje razine kibernetičke sigurnosti u Uniji, među ostalim povećanjem broja kvalificiranih stručnjaka za kibernetičku sigurnost, jačanjem izgradnje kapaciteta mikropoduzeća te malih i srednjih poduzeća te poboljšanjem javne svijesti o kibernetičkim prijetnjama.

(123) U svojim odnosima s trećim zemljama Unija nastoji promicati međunarodnu trgovinu reguliranim proizvodima. Može se primijeniti širok raspon mjera kako bi se olakšala trgovina, 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 u pogledu ocjenjivanja sukladnosti. Ti se sporazumi temelje na uzajamnom prihvaćanju 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 trećih zemalja. Sporazumi o uzajamnom priznavanju sklapaju se u više posebnih sektora koji se mogu razlikovati od jedne do druge treće zemlje. 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 uređuje ovom Uredbom u skladu s člankom 218. UFEUA-a. Važna je i suradnja s partnerskim trećim zemljama radi povećanja kibernetičke otpornosti na globalnoj razini jer će to dugoročno doprinijeti učvršćivanju okvira kibernetičke sigurnosti unutar i izvan Unije.

([32]) 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., ELI: http://data.europa.eu/eli/reg/2011/182/oj).

(124) Potrošači bi trebali biti ovlašteni ostvarivati svoja prava u odnosu na obveze nametnute gospodarskim subjektima na temelju ove Uredbe putem predstavničkih tužbi u skladu s Direktivom (EU) 2020/1828 Europskog parlamenta i Vijeća ([33]). U tu bi svrhu ovom Uredbom trebalo predvidjeti da je Direktiva (EU) 2020/1828 primjenjiva na predstavničke tužbe koje se odnose na kršenja ove Uredbe koje štete ili mogu naštetiti kolektivnim interesima potrošača. Prilog I. toj direktivi trebalo bi stoga na odgovarajući način izmijeniti. Države članice trebale bi osigurati da se te izmjene uzmu u obzir u mjerama za prenošenje donesenima u skladu s tom direktivom, iako donošenje nacionalnih mjera za prenošenje u tom pogledu nije uvjet za primjenjivost te direktive na te predstavničke tužbe. Primjenjivost te direktive na predstavničke tužbe podnesene zbog kršenja odredaba ove Uredbe od strane gospodarskih subjekata koje štete ili mogu naštetiti kolektivnim interesima potrošača, trebala bi početi od 11. prosinca 2027.

(125) Komisija bi periodično trebala evaluirati i preispitivati ovu Uredbu, uz savjetovanje s relevantnim dionicima, posebno radi utvrđivanja potrebe izmjene u svjetlu promjene društvenih, političkih, tehnoloških i tržišnih uvjeta. Ovom Uredbom olakšat će se usklađenost s obvezama u pogledu sigurnosti lanca opskrbe subjektima obuhvaćenima područjem primjene Uredbe (EU) 2022/2554 i Direktive (EU) 2022/2555 koji upotrebljavaju proizvode s digitalnim elementima. Komisija bi u okviru tog periodičnog preispitivanja trebala evaluirati kombinirane učinke okvira Unije za kibernetičku sigurnost.

(126) Gospodarskim subjektima trebalo bi dati dovoljno vremena za prilagodbu zahtjevima utvrđenima u ovoj Uredbi. Ova bi se Uredba trebala primjenjivati od 11. prosinca 2027., uz iznimku obveza u pogledu izvješćivanja povezanih s aktivno iskorištenim ranjivostima i značajnim incidentima koji utječu na sigurnost proizvoda s digitalnim elementima, koje bi se trebale primjenjivati od 11. rujna 2026. i odredaba o prijavljivanju tijelâ za ocjenjivanje sukladnosti, koje bi se trebale primjenjivati od 11. lipnja 2026.

(127) Važno je pružiti potporu mikropoduzećima te malim i srednjim poduzećima, među ostalim start-up poduzećima, u provedbi ove Uredbe i minimizirati rizike za provedbu koji proizlaze iz nedostatka znanja i stručnosti na tržištu i kako bi se proizvođačima olakšalo ispunjavanje njihovih obveza utvrđenih u ovoj Uredbi. Programom Digitalna Europa i drugim relevantnim programima Unije pruža se financijska i tehnička potpora koja tim poduzećima omogućuje da doprinesu rastu gospodarstva Unije i jačanju zajedničke razine kibernetičke sigurnosti u Uniji. Europski stručni centar za industriju, tehnologiju i istraživanja u području kibernetičke sigurnosti i nacionalni koordinacijski centri te europski centri za digitalne inovacije koje su Komisija i države članice uspostavile na razini Unije ili na nacionalnoj razini mogli bi također podupirati i poduzeća i organizacije javnog sektora te bi mogli doprinijeti provedbi ove Uredbe. U okviru svojih zadaća i područja nadležnosti mogli bi pružati tehničku i znanstvenu potporu mikropoduzećima te malim i srednjim poduzećima, primjerice za aktivnosti ispitivanja i ocjenjivanje sukladnosti koje provodi treća strana. Njima bi se također moglo poticati uvođenje alata za olakšavanje provedbe ove Uredbe.

(128) Nadalje, države članice trebale bi razmotriti poduzimanje dopunskih mjera čiji je cilj pružanje smjernica i potpore mikropoduzećima te malim i srednjim poduzećima, kao što je uspostava regulatornih izoliranih okruženja i namjenskih kanala za komunikaciju. Kako bi se ojačala razina kibernetičke sigurnosti u Uniji, države članice mogu razmotriti i pružanje potpore za razvoj kapaciteta i vještina povezanih s kibernetičkom sigurnošću proizvoda s digitalnim elementima, poboljšanje kibernetičke otpornosti gospodarskih subjekata, posebno mikropoduzeća te malih i srednjih poduzeća, te poticanje javne svijesti o kibernetičkoj sigurnosti proizvoda s digitalnim elementima.

(129) 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.

(130) Provedeno je savjetovanje s Europskim nadzornikom za zaštitu podataka u skladu s člankom 42. stavkom 1. Uredbe (EU) 2018/1725 Europskog parlamenta i Vijeća ([34]) te je on dao mišljenje 9. studenoga 2022. ([35]),

([33]) Direktiva (EU) 2020/1828 Europskog parlamenta i Vijeća od 25. studenoga 2020. o predstavničkim tužbama za zaštitu kolektivnih interesa potrošačâ i stavljanju izvan snage Direktive 2009/22/EZ (SL L 409, 4.12.2020., str. 1.).

([34]) 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.).

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

DONIJELI SU OVU UREDBU:

POGLAVLJE I.

OPĆE ODREDBE

Članak 1.

Predmet

Ovom se Uredbom utvrđuju:

(a) pravila za stavljanje na raspolaganje na tržištu proizvoda s digitalnim elementima kako bi se osigurala kibernetička sigurnost takvih proizvoda;

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

(c) bitni zahtjevi u pogledu kibernetičke sigurnosti za procese postupanja s ranjivostima koje su proizvođači uspostavili kako bi osigurali kibernetičku sigurnost proizvoda s digitalnim elementima tijekom vremena za koje se očekuje da će proizvodi biti u upotrebi i obveze gospodarskih subjekata u pogledu tih procesa;

(d) pravila o nadzoru tržišta, među ostalim o praćenju, te o izvršavanju pravila i zahtjeva iz ovog članka.

Članak 2.

Područje primjene

1. Ova se Uredba primjenjuje na proizvode s digitalnim elementima koji se stavljaju na raspolaganje na tržištu čija namjena ili razumno predvidljiva upotreba 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 pravni 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. Ova se Uredba ne primjenjuje na opremu koja je obuhvaćena područjem primjene Direktive 2014/90/EU Europskog parlamenta i Vijeća ([36]).

5. Kad je riječ o proizvodima s digitalnim elementima obuhvaćenima drugim pravilima Unije kojima se utvrđuju zahtjevi koji se odnose na sve ili neke rizike obuhvaćene bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I., primjena ove Uredbe može se ograničiti ili isključiti:

(a) ako je takvo ograničenje ili isključenje 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 ili viša razina zaštite.

Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 61. radi dopune ove Uredbe utvrđivanjem potrebe za takvim ograničenjem ili isključenjem, predmetnih proizvoda i pravila i, prema potrebi, opsega ograničenja.

([36]) Direktiva 2014/90/EU Europskog parlamenta i Vijeća od 23. srpnja 2014. o pomorskoj opremi i stavljanju izvan snage Direktive Vijeća 96/98/EZ (SL L 257, 28.8.2014., str. 146.).

6. Ova se Uredba ne primjenjuje na rezervne dijelove koji se stavljaju na raspolaganje na tržištu kako bi zamijenili istovjetne komponente u proizvodima s digitalnim elementima i koji su proizvedeni u skladu s istim specifikacijama kao sastavni dijelovi koje bi trebali zamijeniti.

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

8. Obveze utvrđene u ovoj Uredbi ne podrazumijevaju pružanje informacija čije bi otkrivanje bilo u suprotnosti s ključnim interesima nacionalne sigurnosti, javne sigurnosti ili obrane država članica.

Članak 3.

Definicije

Za potrebe ove Uredbe primjenjuju se sljedeće definicije:

1. „proizvod s digitalnim elementima” znači 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 obrada podataka na daljinu putem softvera koji je projektirao i razvio proizvođač ili koji je projektiran i razvijen pod odgovornošću proizvođača, a bez koje proizvod s digitalnim elementima ne bi mogao obavljati neku od svojih funkcija;

3. „kibernetička sigurnost” znači kibernetička sigurnost kako je definirana u članku 2. točki 1. Uredbe (EU) 2019/881;

4. „softver” znači dio elektroničkog informacijskog sustava koji se sastoji od računalnog koda;

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

6. „komponenta” znači softver ili hardver namijenjen za integraciju u elektronički informacijski sustav;

7. „elektronički informacijski sustav” znači sustav, uključujući električnu ili elektroničku opremu, koji može obrađivati, pohranjivati ili prenositi digitalne podatke;

8. „logička veza” znači virtualni prikaz podatkovne veze izvedene u obliku softverskog sučelja;

9. „fizička veza” znači veza između elektroničkih informacijskih sustava ili komponenata izvedena fizičkim sredstvima, uključujući električna, optička ili mehanička sučelja, žice ili radijske valove;

10. „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;

11. „krajnja točka” znači svaki uređaj koji je priključen na mrežu i služi kao ulazna točka u tu mrežu;

12. „gospodarski subjekt” znači proizvođač, ovlašteni zastupnik, uvoznik, distributer ili druga fizička ili pravna osoba koja podliježe obvezama u vezi s proizvodnjom proizvoda s digitalnim elementima ili u vezi sa stavljanjem na raspolaganje na tržištu proizvoda s digitalnim elementima u skladu s ovom Uredbom;

13. „proizvođač” znači 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, monetizaciju ili besplatno;

14. „upravitelj softvera otvorenog koda” znači pravna osoba, koja nije proizvođač, čija je svrha ili cilj sustavno pružati kontinuiranu potporu za razvoj određenih proizvoda s digitalnim elementima, koji se smatraju besplatnim softverom otvorenog koda i namijenjeni su komercijalnim djelatnostima, te koja osigurava održivost tih proizvoda;

15. „ovlašteni zastupnik” znači fizička ili pravna osoba koja ima poslovni nastan u Uniji i koja je dobila pisano ovlaštenje od proizvođača da u njegovo ime obavlja određene zadaće;

16. „uvoznik” znači fizička ili pravna osoba koja ima poslovni nastan u Uniji koja stavlja na tržište proizvod s digitalnim elementima s imenom ili žigom fizičke ili pravne osobe koja ima poslovni nastan izvan Unije;

17. „distributer” znači 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;

18. „potrošač” znači fizička osoba koja djeluje u svrhe koje prelaze okvire njezine trgovačke, poslovne, obrtničke ili profesionalne djelatnosti;

19. „mikropoduzeća”, „mala poduzeća” i „srednja poduzeća” znači mikropoduzeća, mala poduzeća i srednja poduzeća kako su definirana u Prilogu Preporuci 2003/361/EZ;

20. „razdoblje potpore” znači razdoblje tijekom kojeg proizvođač mora osigurati da se s ranjivostima proizvoda s digitalnim elementima postupa djelotvorno i u skladu s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu II. Priloga I.;

21. „stavljanje na tržište” znači prvo stavljanje proizvoda s digitalnim elementima na raspolaganje na tržištu Unije;

22. „stavljanje na raspolaganje na tržištu” znači isporuka proizvoda s digitalnim elementima za distribuciju ili upotrebu na tržištu Unije u okviru trgovačke djelatnosti uz naplatu ili besplatno;

23. „namjena” znači upotreba za koju je proizvođač namijenio proizvod s digitalnim elementima, uključujući specifični kontekst i uvjete upotrebe, kako je određena u informacijama koje je proizvođač naveo u uputama za upotrebu, promotivnim ili prodajnim materijalima i izjavama te u tehničkoj dokumentaciji;

24. „razumno predvidljiva upotreba” znači upotreba koja nije nužno namjena koju je proizvođač naveo u uputama za upotrebu, promotivnim ili prodajnim materijalima, izjavama i tehničkoj dokumentaciji, ali do koje vjerojatno može doći iz razumno predvidljivog ljudskog ponašanja, tehničkih operacija ili interakcija;

25. „razumno predvidljiva kriva upotreba” znači upotreba 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;

26. „tijelo koje provodi prijavljivanje” znači nacionalno tijelo odgovorno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje, imenovanje, prijavljivanje i praćenje tijelâ za ocjenjivanje sukladnosti;

27. „ocjenjivanje sukladnosti” znači postupak kojim se provjerava jesu li ispunjeni bitni zahtjevi u pogledu kibernetičke sigurnosti utvrđeni u Prilogu I.;

28. „tijelo za ocjenjivanje sukladnosti” znači tijelo za ocjenjivanje sukladnosti kako je definirano u članku 2. točki 13. Uredbe (EZ) br. 765/2008.

29. „prijavljeno tijelo” znači tijelo za ocjenjivanje sukladnosti imenovano u skladu s člankom 43. i drugim relevantnim zakonodavstvom Unije o usklađivanju;

30. „bitna izmjena” znači promjena proizvoda s digitalnim elementima nakon njegova stavljanja na tržište koja utječe na sukladnost proizvoda s digitalnim elementima s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu I. Priloga I. ili koja prouzroči promjenu namjene prema kojoj je proizvod s digitalnim elementima bio ocijenjen;

31. „oznaka CE” znači oznaka kojom proizvođač označuje da su proizvod s digitalnim elementima i procesi koje je proizvođač uspostavio sukladni s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. i drugog primjenjivog zakonodavstva Unije o usklađivanju kojim se propisuje označivanje tom oznakom;

32. „zakonodavstvo Unije o usklađivanju” znači zakonodavstvo Unije navedeno u Prilogu I. Uredbi (EU) 2019/1020 i svako drugo zakonodavstvo Unije kojim se usklađuju uvjeti za stavljanje na tržište proizvoda na koje se primjenjuje ova Uredba;

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

34. „međunarodna norma” znači međunarodna norma kako je definirana u članku 2. točki 1. podtočki (a) Uredbe (EU) br. 1025/2012;

35. „europska norma” znači europska norma kako je definirana u članku 2. točki 1. podtočki (b) Uredbe (EU) br. 1025/2012;

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

37. „kibernetički sigurnosni rizik” znači mogućnost gubitka ili poremećaja uzrokovana incidentom i treba je izražavati kao kombinaciju razmjera takvog gubitka ili poremećaja i vjerojatnosti pojave incidenta;

38. „znatan kibernetički sigurnosni rizik” znači kibernetički sigurnosni rizik za koji se na temelju njegovih tehničkih karakteristika može pretpostaviti da ima veliku vjerojatnost izazivanja incidenta koji bi mogao prouzročiti teške štetne posljedice, među ostalim znatan materijalni ili nematerijalni gubitak ili poremećaj;

39. „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;

40. „ranjivost” znači slabost, osjetljivost ili nedostatak proizvoda s digitalnim elementima koje se može iskoristiti kibernetičkom prijetnjom;

41. „iskoristiva ranjivost” znači ranjivost koju bi protivnik mogao djelotvorno iskoristiti u praktičnim operativnim uvjetima;

42. „aktivno iskorištena ranjivost” znači ranjivost za koju postoje pouzdani dokazi da ju je neki zlonamjerni akter iskoristio u sustavu bez dopuštenja vlasnika sustava;

43. „incident” znači incident kako je definiran u članku 6. točki 6. Direktive (EU) 2022/2555;

44. „incident koji utječe na sigurnost proizvoda s digitalnim elementima” znači incident koji negativno utječe ili može negativno utjecati na sposobnost proizvoda s digitalnim elementima da zaštiti dostupnost, autentičnost, cjelovitost ili povjerljivost podataka ili funkcija;

45. „izbjegnuti incident” znači izbjegnuti incident kako je definiran u članku 6. točki 5. Direktive (EU) 2022/2555;

46. „kibernetička prijetnja” znači kibernetička prijetnja kako je definirana u članku 2. točki 8. Uredbe (EU) 2019/881;

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

48. „besplatni softver otvorenog koda” znači softver čiji se izvorni kod otvoreno dijeli i koji je stavljen na raspolaganje na temelju besplatne licencije otvorenog koda kojom se pružaju sva prava kako bi ga se učinilo slobodno dostupnim, upotrebljivim, promjenjivim i preraspodjeljivim;

49. „opoziv” znači opoziv kako je definiran u članku 3. točki 22. Uredbe (EU) 2019/1020;

50. „povlačenje” znači povlačenje kako je definirano u članku 3. točki 23. Uredbe (EU) 2019/1020;

51. „CSIRT koji je imenovan koordinatorom” znači CSIRT koji je imenovan koordinatorom u skladu s člankom 12. stavkom 1. Direktive (EU) 2022/2555.

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. Na sajmovima, izložbama, predstavljanjima ili sličnim događanjima države članice ne sprečavaju izlaganje ni upotrebu proizvoda s digitalnim elementima koji nije u skladu s ovom Uredbom, među ostalim njegovih prototipova, pod uvjetom da proizvod ima vidljiv znak koji jasno upućuje na to da proizvod nije u skladu s ovom Uredbom i da ne smije biti stavljen na raspolaganje na tržištu dok ne bude u skladu s njom.

3. Države članice ne sprečavaju stavljanje na raspolaganje na tržištu 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 on ima vidljiv znak koji jasno upućuje na to da taj softver nije u skladu s ovom Uredbom i da neće biti stavljen na raspolaganju na tržištu u druge svrhe osim u svrhu ispitivanja.

4. Stavak 3. ne primjenjuje na sigurnosne komponente kako su navedene u zakonodavstvu Unije o usklađivanju koje nije ova Uredba.

Članak 5.

Nabava ili upotreba proizvoda s digitalnim elementima

1. Ovom se Uredbom ne sprečavaju države članice da na proizvode s digitalnim elementima primjenjuju dodatne kibernetičke sigurnosne zahtjeve za nabavu ili upotrebu tih proizvoda u posebne svrhe, među ostalim ako se ti proizvodi nabavljaju ili upotrebljavaju u svrhe nacionalne sigurnosti ili obrane, pod uvjetom da su takvi zahtjevi u skladu s obvezama država članica utvrđenima u pravu Unije te da su potrebni i razmjerni za postizanje tih svrha.

2. Ne dovodeći u pitanje direktive 2014/24/EU i 2014/25/EU, ako se nabavljaju proizvodi s digitalnim elementima koji su obuhvaćeni područjem primjene ove Uredbe, države članice osiguravaju da se u postupku nabave uzima u obzir usklađenost s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. ovoj Uredbi, uključujući sposobnost proizvođača da djelotvorno postupaju s ranjivostima.

Članak 6.

Zahtjevi za proizvode s digitalnim elementima

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

(a) ispunjavaju bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu I. Priloga I. pod uvjetom da su ispravno instalirani i održavani, da se upotrebljavaju u skladu sa svojom namjenom ili pod uvjetima koji se mogu razumno predvidjeti i da su, ako je primjenjivo, ugrađena potrebna sigurnosna ažuriranja; i

(b) da su procesi koje je uspostavio proizvođač u skladu s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu II. Priloga I.

Članak 7.

Važni proizvodi s digitalnim elementima

1. Proizvodi s digitalnim elementima koji imaju osnovnu funkcionalnost kategorije proizvoda utvrđene u Prilogu III. smatraju se važnim proizvodima s digitalnim elementima i podliježu postupcima ocjenjivanja sukladnosti iz članka 32. stavaka 2. i 3. Integracija proizvoda s digitalnim elementima koji ima osnovnu funkcionalnost kategorije proizvoda utvrđene u Prilogu III. sama po sebi ne znači da proizvod u koji je integriran podliježe postupcima ocjenjivanja sukladnosti iz članka 32. stavaka 2. i 3.

2. Kategorije proizvoda s digitalnim elementima iz stavka 1. ovog članka, podijeljene u razrede I. i II. kako je utvrđeno u Prilogu III., moraju ispunjavati barem jedan od sljedećih kriterija:

(a) proizvod s digitalnim elementima prvenstveno obavlja funkcije kritične za kibernetičku sigurnost drugih proizvoda, mreža ili usluga, među ostalim osiguravanje autentifikacije i pristupa, sprečavanje i otkrivanje neovlaštenog ulaska, sigurnost krajnjih točaka ili zaštita mreže;

(b) proizvod s digitalnim elementima obavlja funkciju koja nosi znatan rizik od štetnih učinaka u smislu svojeg intenziteta i sposobnosti ometanja, kontrole ili nanošenja štete velikom broju drugih proizvoda ili zdravlju, sigurnosti ili zaštiti svojih korisnika izravnom manipulacijom, kao što je funkcija središnjeg sustava, među ostalim upravljanje mrežom, kontrola konfiguracije, virtualizacija ili obrada osobnih podataka.

3. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 61. radi izmjene Priloga III. uvrštavanjem u popis nove kategorije u svaki razred kategorija proizvoda s digitalnim elementima i određivanjem njezine definicije, premještanjem kategorije proizvoda iz jednog razreda u drugi ili povlačenjem postojeće kategorije s tog popisa. Komisija pri procjeni potrebe za izmjenom popisa utvrđenog u Prilogu III. uzima u obzir kibernetičke sigurnosne funkcionalnosti ili funkciju i razinu kibernetičkog sigurnosnog rizika koji predstavljaju proizvodi s digitalnim elementima kako je utvrđeno kriterijima iz stavka 2. ovog članka.

Delegiranim aktima iz prvog podstavka ovog stavka, prema potrebi, predviđa se minimalno prijelazno razdoblje od 12 mjeseci, posebno ako je nova kategorija važnih proizvoda s digitalnim elementima dodana I. ili II. razredu ili se premješta iz I. razreda u II. kako je utvrđeno u Prilogu III., prije početka primjene relevantnih postupaka ocjenjivanja sukladnosti kako su navedeni u članku 32. stavcima 2. i 3., osim ako je kraće prijelazno razdoblje opravdano iz krajnje hitnih razloga.

4. Do 11. prosinca 2025. Komisija donosi provedbeni akt kojim se utvrđuje tehnički opis kategorija proizvoda s digitalnim elementima I. i II. razreda kako su utvrđeni u Prilogu III. i tehnički opis kategorija proizvoda s digitalnim elementima kako su utvrđeni u Prilogu IV. Taj provedbeni akt donosi se u skladu s postupkom ispitivanja iz članka 62. stavka 2.

Članak 8.

Kritični proizvodi s digitalnim elementima

1. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 61. radi dopune ove Uredbe kako bi utvrdila za koje se proizvode s digitalnim elementima koji imaju osnovnu funkcionalnost kategorije proizvoda utvrđene u Prilogu IV. ovoj Uredbi mora ishoditi europski kibernetički sigurnosni certifikat s barem „znatnom" razinom jamstva u okviru europskog programa kibernetičke sigurnosne certifikacije donesenog na temelju Uredbe (EU) 2019/881, kako bi se dokazala usklađenost s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. ovoj Uredbi ili njegovim dijelovima, pod uvjetom da je europski program kibernetičke sigurnosne certifikacije koji obuhvaća te kategorije proizvoda s digitalnim elementima donesen u skladu s Uredbom (EU) 2019/881 i da je dostupan proizvođačima. U tim delegiranim aktima utvrđuje se potrebna razina jamstva koja je razmjerna razini kibernetičkog sigurnosnog rizika povezanog s proizvodima s digitalnim elementima i uzima se u obzir njihova namjena, među ostalim kritična ovisnost ključnih subjekata kako su navedeni u članku 3. stavku 1. Direktive (EU) 2022/2555 o tim proizvodima.

Prije donošenja takvih delegiranih akata Komisija provodi procjenu mogućeg učinka predviđenih mjera na tržište i provodi savjetovanja s relevantnim dionicima, među ostalim s Europskom skupinom za kibernetičko sigurnosnu certifikaciju osnovanom Uredbom (EU) 2019/881. Pri ocjenjivanju se uzimaju u obzir spremnost i razina kapaciteta država članica za provedbu relevantnog europskog programa kibernetičke sigurnosne certifikacije. Ako nisu doneseni delegirani akti iz prvog podstavka ovog stavka, proizvodi s digitalnim elementima koji imaju osnovnu funkcionalnost kategorije proizvoda kako je utvrđeno u Prilogu IV. podliježu postupcima ocjenjivanja sukladnosti iz članka 32. stavka 3.

Delegiranim aktima iz prvog podstavka predviđa se minimalno prijelazno razdoblje od šest mjeseci, osim ako je kraće prijelazno razdoblje opravdano iz krajnje hitnih razloga.

2. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 61. radi izmjene Priloga IV. dodavanjem ili povlačenjem kategorija kritičnih proizvoda s digitalnim elementima. Pri utvrđivanju takvih kategorija kritičnih proizvoda s digitalnim elementima i potrebne razine jamstva, u skladu sa stavkom 1. ovog članka, Komisija uzima u obzir kriterije iz članka 7. stavka 2. i osigurava da kategorije proizvoda s digitalnim elementima ispunjavaju barem jedan od sljedećih kriterija:

(a) postoji kritična ovisnost kritičnih subjekata kako su navedeni u članku 3. Direktive (EU) 2022/2555 o kategoriji proizvoda s digitalnim elementima;

(b) incidenti i iskorištene ranjivosti povezane s kategorijom proizvoda s digitalnim elementima mogli bi dovesti do ozbiljnih poremećaja u ključnim lancima opskrbe na unutarnjem tržištu.

Prije donošenja takvih delegiranih akata Komisija provodi procjenu iste vrste kao što je ona navedena u stavku 1.

Delegiranim aktima iz prvog podstavka predviđa se minimalno prijelazno razdoblje od šest mjeseci, osim ako je kraće prijelazno razdoblje opravdano iz krajnje hitnih razloga.

Članak 9.

Savjetovanje s dionicima

1. Pri pripremi mjera za provedbu ove Uredbe Komisija se savjetuje s relevantnim dionicima, kao što su relevantna tijela država članica, poduzeća iz privatnog sektora, uključujući mikropoduzeća te mala i srednja poduzeća, zajednice koje primjenjuju softver otvorenog koda, udruge potrošača, akademska zajednica i relevantne agencije i tijela Unije te stručne skupine osnovane na razini Unije, i uzima u obzir njihova stajališta. Posebno, Komisija se na strukturiran način, prema potrebi, savjetuje s tim dionicima i traži njihova stajališta pri:

(a) pripremi smjernica iz članka 26.;

(b) pripremi tehničkih opisa kategorija proizvoda utvrđenih u Prilogu III. u skladu s člankom 7. stavkom 4., procjeni potrebe za mogućim ažuriranjem popisa kategorija proizvoda u skladu s člankom 7. stavkom 3. i člankom 8. stavkom 2. ili procjeni mogućeg učinka na tržište iz članka 8. stavka 1., ne dovodeći u pitanje članak 61.;

(c) poduzimanju pripremnih radnji za evaluaciju i preispitivanje ove Uredbe.

2. Komisija organizira redovita savjetovanja i informativne sastanke, najmanje jednom godišnje, kako bi prikupila stajališta dionika iz stavka 1. o provedbi ove Uredbe.

Članak 10.

Poboljšanje vještina u digitalnom okruženju otpornom na kibernetičke prijetnje

Za potrebe ove Uredbe i kako bi se odgovorilo na potrebe stručnjaka u potporu provedbi ove Uredbe, države članice, prema potrebi uz potporu Komisije, Europskog stručnog centra u području kibernetičke sigurnosti i ENISA-e, uz potpuno poštovanje odgovornosti država članica u području obrazovanja, promiču mjere i strategije za:

(a) razvoj vještina u području kibernetičke sigurnosti i stvaranje organizacijskih i tehnoloških alate kako bi se osigurala odgovarajuća dostupnost kvalificiranih stručnjaka radi potpore aktivnostima tijelâ za nadzor tržišta i tijelâ za ocjenjivanje sukladnosti;

(b) povećanje suradnje između privatnog sektora, gospodarskih subjekata, među ostalim prekvalifikacijom ili usavršavanjem zaposlenika proizvođača, potrošača, pružatelja usluga osposobljavanja te javnih uprava, kako bi se time proširile mogućnosti da se mladi zaposle na radnim mjestima u sektoru kibernetičke sigurnosti.

Članak 11.

Opća sigurnost proizvoda

Odstupajući od članka 2. stavka 1. trećeg podstavka točke (b) Uredbe (EU) 2023/988, poglavlje III. odjeljak 1., poglavlja V. i VII. te poglavlja od IX. do XI. te uredbe primjenjuju se na proizvode s digitalnim elementima u pogledu aspekata i rizika ili kategorija rizika koji nisu obuhvaćeni ovom Uredbom ako ti proizvodi ne podliježu posebnim sigurnosnim zahtjevima utvrđenima u drugom „zakonodavstvu Unije o usklađivanju" kako je definirano u članku 3. točki 27. Uredbe (EU) 2023/988.

Članak 12.

Visokorizični UI sustavi

1. Ne dovodeći u pitanje zahtjeve koji se odnose na točnost i otpornost utvrđene u članku 15. Uredbe (EU) 2024/1689, proizvodi s digitalnim elementima koji su obuhvaćeni područjem primjene ove Uredbe i koji su klasificirani kao visokorizični UI sustavi na temelju članak 6. te uredbe smatraju se sukladnima sa zahtjevima za kibernetičku sigurnost utvrđenima u članku 15. te uredbe ako:

(a) ti proizvodi ispunjavaju bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu I. Priloga I.;

(b) procesi koje je uspostavio proizvođač ispunjavaju bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu II. Priloga I.; i

(c) postizanje razine kibernetičke sigurnosne zaštite koja se zahtijeva u skladu s člankom 15. Uredbe (EU) 2024/1689 dokazano je EU izjavom o sukladnosti izdanom na temelju ove Uredbe.

2. Za proizvode s digitalnim elementima i kibernetičke sigurnosne zahtjeve iz stavka 1. ovoga članka primjenjuje se odgovarajući postupak ocjenjivanja sukladnosti predviđen u članku 43. Uredbe (EU) 2024/1689. Za potrebe tog ocjenjivanja prijavljena tijela koja su nadležna kontrolirati sukladnost visokorizičnih UI sustava na temelju Uredbe (EU) 2024/1689 nadležna su kontrolirati i sukladnost visokorizičnih UI sustava obuhvaćenih područjem primjene ove Uredbe sa zahtjevima utvrđenim u Prilogu I. ovoj Uredbi, pod uvjetom da je u kontekstu postupka prijavljivanja na temelju Uredbe (EU) 2024/1689 ocijenjeno ispunjavaju li ta prijavljena tijela zahtjeve utvrđene u članku 39. ove Uredbe.

3. Odstupajući od stavka 2. ovog članka, važni proizvodi s digitalnim elementima navedeni u Prilogu III. ovoj Uredbi koji podliježu postupcima ocjenjivanja sukladnosti iz članka 32. stavka 2. točaka (a) i (b) i članka 32. stavka 3. ove Uredbe i kritični proizvodi s digitalnim elementima navedeni u Prilogu IV. ovoj Uredbi za koje se mora ishoditi europski kibernetički sigurnosni certifikat u skladu s člankom 8. stavkom 1. ove Uredbe ili, ako se to ne zahtijeva, koji podliježu postupcima ocjenjivanja sukladnosti iz članka 32. stavka 3. ove Uredbe te su klasificirani kao visokorizični UI sustavi u skladu s člankom 6. Uredbe (EU) 2024/1689 i na koje se primjenjuje postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole iz Priloga VI. Uredbi (EU) 2024/1689 podliježu postupcima ocjenjivanja sukladnosti predviđenima u ovoj Uredbi u mjeri u kojoj su na njih odnose bitni zahtjevi u pogledu kibernetičke sigurnosti utvrđeni u ovoj Uredbi.

4. Proizvođači proizvoda s digitalnim elementima iz stavka 1. ovog članka mogu sudjelovati u regulatornim izoliranim okruženjima za umjetnu inteligenciju iz članka 57. Uredbe (EU) 2024/1689.

POGLAVLJE II.

OBVEZE GOSPODARSKIH SUBJEKATA I ODREDBE U POGLEDU BESPLATNOG SOFTVERA OTVORENOG koda

Članak 13.

Obveze proizvođača

1. Pri stavljanju proizvoda s digitalnim elementima na tržište proizvođači osiguravaju da je on projektiran, razvijen i proizveden u skladu s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu I. Priloga I.

2. U svrhu ispunjavanja obveze iz stavka 1. proizvođači procjenjuju kibernetičke sigurnosne 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 te procjene radi smanjenja kibernetičkih sigurnosnih rizika, sprečavanja incidenata i smanjivanja njihovih posljedica, među ostalim na zdravlje i sigurnost korisnika.

3. Procjena kibernetičkog sigurnosnog rizika dokumentira se i ažurira prema potrebi tijekom razdoblja potpore koje se utvrđuje u skladu sa stavkom 8. ovog članka. Ta procjena kibernetičkog sigurnosnog rizika obuhvaća barem analizu kibernetičkih sigurnosnih rizika na temelju namjene i razumno predvidljive upotrebe, kao i uvjeta upotrebe proizvoda s digitalnim elementima, kao što su operativno okruženje ili sredstva koja treba zaštititi, uzimajući u obzir očekivano trajanje upotrebe proizvoda. U procjeni kibernetičkog sigurnosnog rizika navodi se jesu li i, ako jesu, na koji način, sigurnosni zahtjevi utvrđeni u dijelu I. točki 2. Priloga I. primjenjivi na relevantni proizvod s digitalnim elementima te kako se ti zahtjevi provode na temelju procjene kibernetičkog sigurnosnog rizika. U njoj se također navodi kako proizvođač treba primijeniti dio I. točku 1. Priloga I. i zahtjeve u pogledu postupanja s ranjivostima utvrđene u dijelu II. Priloga I.

4. Pri stavljanju na tržište proizvoda s digitalnim elementima proizvođač u tehničku dokumentaciju koja se zahtijeva u skladu s člankom 31. i Prilogom VII. uključuje procjenu kibernetičkih sigurnosnih rizika iz stavka 3. ovoga članka. Za proizvode s digitalnim elementima iz članka 12. koji podliježu i drugim pravnim aktima Unije procjena kibernetičkih sigurnosnih rizika može biti dio procjene rizika koja se zahtijeva tim pravnim aktima Unije. Ako određeni bitni zahtjevi u pogledu kibernetičke sigurnosti nisu primjenjivi na proizvod s digitalnim elementima, proizvođač u tu tehničku dokumentaciju uključuje jasno obrazloženje.

5. 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 na način da te komponente ne ugrožavaju kibernetičku sigurnost proizvoda s digitalnim elementima, među ostalim i ako se integriraju komponente besplatnog softvera otvorenog koda koje nisu bile stavljene na raspolaganje na tržište tijekom komercijalne aktivnosti.

6. 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 proizvodi ili održava tu komponentu te otklanjaju i saniraju tu ranjivost u skladu sa zahtjevima u pogledu postupanja s ranjivostima utvrđenima u dijelu II. Priloga I. Ako su proizvođači razvili izmjenu softvera ili hardvera kako bi otklonili ranjivost te komponente, relevantni kod ili relevantnu dokumentaciju dijele s osobom ili subjektom koji proizvodi ili održava tu komponentu, prema potrebi u strojno čitljivom formatu.

7. Proizvođači moraju sustavno dokumentirati, na način koji je razmjeran vrsti i kibernetičkim sigurnosnim rizicima, relevantne aspekte kibernetičke sigurnosti povezane s proizvodima s digitalnim elementima, uključujući ranjivosti za koje su doznali i sve relevantne informacije koje pružaju treće strane te, ako je primjenjivo, ažurira procjenu kibernetičkog sigurnosnog rizika proizvodâ.

8. Pri stavljanju na tržište proizvoda s digitalnim elementima i tijekom razdoblja potpore, proizvođači osiguravaju da se s ranjivostima tog proizvoda, uključujući njegove komponente, postupa djelotvorno i u skladu s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu II. Priloga I.

Proizvođači određuju razdoblje potpore tako da ono odražava razdoblje tijekom kojeg se očekuje da će proizvod biti u upotrebi, posebno uzimajući u obzir razumna očekivanja korisnika, prirodu proizvoda, uključujući njegovu namjenu, kao i mjerodavno pravo Unije kojim se utvrđuje vijek trajanja proizvodâ s digitalnim elementima. Pri određivanju razdoblja potpore proizvođači mogu uzeti u obzir i razdoblja potpore za proizvode s digitalnim elementima koji nude sličnu funkcionalnost koje su na tržište stavili drugi proizvođači, dostupnost operativnog okruženja, razdoblja potpore za integrirane komponente koje pružaju osnovne funkcije i potječu od trećih strana, kao i relevantne smjernice posebne skupine za administrativnu suradnju (skupina za ADCO), osnovane u skladu s člankom 52. stavkom 15., i Komisije. Pitanja koja treba uzeti u obzir kako bi se odredilo razdoblje potpore razmatraju se na način kojim se osigurava proporcionalnost.

Ne dovodeći u pitanje drugi podstavak, razdoblje potpore traje najmanje pet godina. Ako se očekuje da će proizvod s digitalnim elementima biti u upotrebi u razdoblju kraćem od pet godina, razdoblje potpore odgovara očekivanom vremenu upotrebe.

Uzimajući u obzir preporuke skupine za ADCO, kako je navedeno u članku 52. stavku 16., Komisija može donijeti delegirane akte u skladu s člankom 61. radi dopune ove Uredbe utvrđivanjem minimalnog razdoblja potpore za određene kategorije proizvoda ako podaci o nadzoru tržišta upućuju na neodgovarajuća razdoblja potpore.

Proizvođači uključuju informacije koje su uzete u obzir za utvrđivanje razdoblja potpore za proizvod s digitalnim elementima u tehničku dokumentaciju, kako je utvrđeno u Prilogu VII.

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

9. Proizvođači osiguravaju da svako sigurnosno ažuriranje, kako je navedeno u dijelu II. točki 8. Priloga I., koje je stavljeno na raspolaganje korisnicima tijekom razdoblja potpore, po izdavanju ostane dostupno najmanje 10 godina ili tijekom preostalog razdoblja potpore, ovisno o tome što je dulje.

10. Ako je proizvođač na tržište stavio naknadne bitno izmijenjene verzije softverskog proizvoda, taj proizvođač može osigurati sukladnost s bitnim zahtjevom u pogledu kibernetičke sigurnosti utvrđenim u dijelu II. točki 2. Priloga I. samo za posljednju verziju koju je stavio na tržište, pod uvjetom da korisnici verzija koje su prethodno stavljene na tržište imaju besplatan pristup posljednjoj verziji koja je stavljena na tržište i da ne moraju snositi dodatne troškove prilagodbe hardverskog i softverskog okruženja unutar kojeg se upotrebljavala izvorna verziju tog proizvoda.

11. Proizvođači mogu održavati javne arhive softvera kako bi se poboljšao pristup korisnika ranijim verzijama. U tim se slučajevima korisnike jasno i na lako dostupan način obavješćuje o rizicima povezanima s upotrebom nepodržanog softvera.

12. Prije stavljanja na tržište proizvoda s digitalnim elementima proizvođači moraju sastaviti tehničku dokumentaciju iz članka 31.

Oni provode ili daju provesti odabrane postupke ocjenjivanja sukladnosti kako su navedeni u članku 32.

Ako je tim postupkom ocjenjivanja sukladnosti dokazana sukladnost proizvoda s digitalnim elementima s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu I. Priloga I. i sukladnost procesa koje je proizvođač uspostavio s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu II. Priloga I., proizvođači sastavljaju EU izjavu o sukladnosti u skladu s člankom 28. i stavljaju na proizvod oznaku CE u skladu s člankom 30.

13. Proizvođači najmanje 10 godina nakon što je proizvod s digitalnim elementima stavljen na tržište ili tijekom razdoblja potpore, ovisno o tome što je dulje, drže na raspolaganju tijelima za nadzor tržišta tehničku dokumentaciju i EU izjavu o sukladnosti.

14. Proizvođači osiguravaju uspostavu postupaka za očuvanje sukladnosti serijski proizvedenih proizvoda s digitalnim elementima s ovom Uredbom. Proizvođači na primjeren način uzimaju u obzir promjene povezane s razvojem i proizvodnim procesom ili s projektiranjem ili karakteristikama proizvoda s digitalnim elementima te promjene usklađenih normi, europskih programa kibernetičke sigurnosne certifikacije ili zajedničkih specifikacija iz članka 27. na temelju kojih je izjavljena ili čijom je primjenom provjerena sukladnost proizvoda s digitalnim elementima.

15. Proizvođači osiguravaju da njihovi proizvodi s digitalnim elementima nose broj tipa, šarže ili serije ili bilo koji drugi element koji omogućuje njihovu identifikaciju ili, ako to nije moguće, da su te informacije navedene na pakiranju ili u dokumentima priloženima proizvodu s digitalnim elementima.

16. Proizvođači na proizvodu s digitalnim elementima, na pakiranju ili u dokumentu priloženom uz proizvod s digitalnim elementima navode ime, registrirano trgovačko ime ili registrirani žig proizvođača te poštansku adresu, e-adresu ili druge podatke za digitalni kontakt te, ako je primjenjivo, internetske stranice preko kojih se može stupiti u kontakt s proizvođačem. Te se informacije također uključuju u informacije i upute za korisnike iz Priloga II. Podaci za kontakt moraju biti na jeziku koji korisnici i tijela za nadzor tržišta mogu bez poteškoća razumjeti.

17. Za potrebe ove Uredbe proizvođači određuju jedinstvenu kontaktnu točku koja korisnicima omogućuje izravnu i brzu komunikaciju s njima, među ostalim kako bi se olakšalo izvješćivanje o ranjivostima proizvoda s digitalnim elementima.

Proizvođači osiguravaju da korisnici mogu lako identificirati jedinstvenu kontaktnu točku. U informacije i upute za korisnike iz Priloga II. proizvođači uključuju i informacije o jedinstvenoj kontaktnoj točki.

Jedinstvena kontaktna točka omogućuje korisnicima da odaberu preferirano sredstvo komunikacije i ne ograničava takva sredstva na automatizirane alate.

18. Proizvođači osiguravaju da su uz proizvode s digitalnim elementima priložene informacije i upute za korisnike utvrđene u Prilogu II. u papirnatom ili elektroničkom obliku. Takve informacije i upute pružaju se na jeziku koji korisnici i tijela za nadzor tržišta mogu bez poteškoća razumjeti. Moraju biti jasne, razumljive i čitljive. Moraju omogućiti sigurnu ugradnju, rad i upotrebu proizvoda s digitalnim elementima. Proizvođači najmanje 10 godina nakon što je proizvod s digitalnim elementima stavljen na tržište ili tijekom razdoblja potpore, ovisno o tome što je dulje, drže na raspolaganju korisnicima i tijelima za nadzor tržišta informacije i upute za korisnike utvrđene u Prilogu II. Ako se takve informacije i upute pružaju na internetu, proizvođači osiguravaju da su one pristupačne, prilagođene korisnicima i dostupne na internetu barem 10 godina nakon što je proizvod s digitalnim elementima stavljen na tržište ili tijekom razdoblja potpore, ovisno o tome što je dulje.

19. Proizvođači osiguravaju da je datum završetka razdoblja potpore iz stavka 8. u trenutku kupnje jasno i razumljivo naveden na lako pristupačan način i, ako je primjenjivo, na proizvodu s digitalnim elementima, njegovu pakiranju ili digitalno, pri čemu se moraju navesti barem mjesec i godina.

Ako je to tehnički izvedivo s obzirom na prirodu proizvoda s digitalnim elementima, proizvođači korisnicima prikazuju obavijest kojom ih obavješćuju da je razdoblje potpore za njihov proizvod s digitalnim elementima isteklo.

20. Proizvođači uz proizvod s digitalnim elementima prilažu primjerak EU izjave o sukladnosti ili pojednostavnjenu EU izjavu o sukladnosti. Ako je priložena pojednostavnjena EU izjava o sukladnosti, u njoj se navodi točna internetska adresa na kojoj se može pristupiti cjelovitoj EU izjavi o sukladnosti.

21. Od stavljanja na tržište i tijekom razdoblja potpore proizvođači koji znaju ili imaju razloga vjerovati da proizvod s digitalnim elementima ili procesi koje je proizvođač uspostavio nisu sukladni s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. odmah poduzimaju potrebne korektivne mjere kako bi se ponovno uspostavila sukladnost tog proizvoda s digitalnim elementima ili procesa proizvođača ili kako bi se proizvod prema potrebi povukao ili opozvao.

22. Na obrazložen zahtjev tijela za nadzor tržišta proizvođači tom tijelu dostavljaju, na jeziku koje to tijelo može bez poteškoća razumjeti te u papirnatom ili elektroničkom obliku, sve informacije i svu dokumentaciju potrebne za dokazivanje sukladnosti proizvoda s digitalnim elementima i procesa koje je proizvođač uspostavio s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima Prilogu I. Na zahtjev tog tijela proizvođači s njim surađuju u pogledu svake mjere koja je poduzeta kako bi se otklonili kibernetički sigurnosni rizici proizvoda s digitalnim elementima koji su stavili na tržište.

23. Proizvođač koji se ne može uskladiti s ovom Uredbom jer prestaje s radom obavješćuje, prije prestanka rada, relevantna tijela za nadzor tržišta te, na bilo koji raspoloživ način i u mjeri u kojoj je to moguće, korisnike relevantnih proizvoda s digitalnim elementima koji su stavljeni na tržište o predstojećem prestanku rada.

24. Komisija može provedbenim aktima i uzimajući u obzir europske i međunarodne norme i najbolje prakse odrediti format i elemente popisa softverskog materijala navedene u dijelu II. točki 1. Priloga I. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 62. stavka 2.

25. Kako bi se procijenila ovisnost država članica i Unije u cjelini o softverskim komponentama, a posebno o komponentama koje se smatraju besplatnim softverom otvorenog koda, skupina za ADCO može za određene kategorije proizvoda s digitalnim elementima odlučiti provesti procjenu ovisnosti na razini Unije. U tu svrhu tijela za nadzor tržišta mogu od proizvođača takvih kategorija proizvoda s digitalnim elementima zatražiti da dostave relevantne popise softverskog materijala kako je navedeno u dijelu II. točki 1. Priloga I. Na temelju takvih informacija tijela za nadzor tržišta mogu ADCO-u dostaviti anonimizirane i objedinjene informacije o ovisnostima o softveru. Skupina za ADCO podnosi izvješće o rezultatima procjene ovisnosti skupini za suradnju osnovanoj na temelju članka 14. Direktive (EU) 2022/2555.

Članak 14.

Obveze proizvođačâ u pogledu izvješćivanja

1. Proizvođač o svakoj aktivno iskorištenoj ranjivosti proizvoda s digitalnim elementima za koju dozna mora istodobno obavijestiti CSIRT koji je imenovan koordinatorom, u skladu sa stavkom 7. ovog članka, i ENISA-u. Proizvođač o toj aktivno iskorištenoj ranjivosti obavješćuje putem jedinstvene platforme za izvješćivanje uspostavljene u skladu s člankom 16.

2. Za potrebe obavješćivanja iz stavka 1. proizvođač dostavlja:

(a) rano upozorenje o aktivno iskorištenoj ranjivosti, bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata nakon što proizvođač dozna za tu ranjivost, navodeći, ako je primjenjivo, države članice za koje proizvođač zna da je na njihovu državnom području njegov proizvod s digitalnim elementima stavljen na raspolaganje;

(b) osim ako su relevantne informacije već dostavljene, obavijest o ranjivosti, bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata nakon što proizvođač dozna za aktivno iskorištenu ranjivost, u kojoj se navode opće informacije, ako su dostupne, o predmetnom proizvodu s digitalnim elementima, općoj prirodi predmetnog iskorištavanja i predmetne ranjivosti, kao i o svim poduzetim korektivnim mjerama ili mjerama ublažavanja i korektivnim mjerama ili mjerama ublažavanja koje korisnici mogu poduzeti, te u kojoj se također navodi, ako je primjenjivo, u kojoj mjeri proizvođač prijavljene informacije smatra osjetljivima;

(c) osim ako su relevantne informacije već dostavljene, završno izvješće, najkasnije 14 dana nakon što budu dostupne korektivne mjere ili mjere ublažavanja, koje sadržava barem sljedeće:

i. opis ranjivosti, uključujući njezinu ozbiljnost i učinak;

ii. informacije o svakom zlonamjernom akteru koji je iskorištavao ili iskorištava ranjivost, ako su dostupne;

iii. pojedinosti o sigurnosnom ažuriranju ili drugim korektivnim mjerama koje su dostupne za otklanjanje ranjivosti.

3. Proizvođač o svakom značajnom incidentu koji utječe na sigurnost proizvoda s digitalnim elementima za koji dozna mora istodobno obavijestiti CSIRT koji je imenovan koordinatorom, u skladu sa stavkom 7. ovog članka, i ENISA-u. Proizvođač o tom incidentu obavješćuje putem jedinstvene platforme za izvješćivanje uspostavljene u skladu s člankom 16.

4. Za potrebe obavješćivanja iz stavka 3. proizvođač dostavlja:

(a) rano upozorenje o značajnom incidentu koji utječe na sigurnost proizvoda s digitalnim elementima, bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata nakon što proizvođač dozna za taj incident, navodeći sumnja li se da je incident uzrokovan nezakonitim ili zlonamjernim djelovanjem te, ako je primjenjivo, države članice za koje proizvođač zna da je na njihovu državnom području njegov proizvod s digitalnim elementima stavljen na raspolaganje;

(b) osim ako su relevantne informacije već dostavljene, obavijest o incidentu, bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata nakon što proizvođač dozna za taj incident, u kojoj se navode opće informacije, ako su dostupne, o prirodi incidenta, početnoj procjeni incidenta, kao i o svim poduzetim korektivnim mjerama ili mjerama ublažavanja i korektivnim mjerama ili mjerama ublažavanja koje korisnici mogu poduzeti, te u kojoj se također navodi, ako je primjenjivo, u kojoj mjeri proizvođač prijavljene informacije smatra osjetljivima;

(c) osim ako su relevantne informacije već dostavljene, završno izvješće u roku mjesec dana nakon podnošenja obavijesti o incidentu iz točke (b), koje sadržava barem sljedeće:

i. detaljan opis incidenta, uključujući njegov značaj i učinak;

ii. vrstu prijetnje odnosno temeljnog uzroka koji su vjerojatno doveli do incidenta;

iii. provedene i tekuće mjere ublažavanja.

5. Za potrebe stavka 3. incident koji utječe na sigurnost proizvoda s digitalnim elementima smatra se značajnim ako:

(a) negativno utječe ili može negativno utjecati na sposobnost proizvoda s digitalnim elementima da zaštiti dostupnost, autentičnost, cjelovitost ili povjerljivost osjetljivih ili važnih podataka ili funkcija; ili

(b) doveo je ili može dovesti do uvođenja ili izvršenja zlonamjernog koda u proizvodu s digitalnim elementima ili u mrežnim i informacijskim sustavima korisnika proizvoda s digitalnim elementima.

6. Ako je to potrebno, CSIRT koji je imenovan koordinatorom koji je prvotno primio obavijest može zatražiti od proizvođača da dostave privremeno izvješće o relevantnim ažuriranjima statusa o aktivno iskorištenoj ranjivosti ili značajnom incidentu koji utječe na sigurnost proizvoda s digitalnim elementima.

7. Obavijesti iz stavaka 1. i 3. ovog članka podnose se putem jedinstvene platforme za izvješćivanje iz članka 16., s pomoću jedne od krajnjih točaka za elektroničko obavješćivanje iz članka 16. stavka 1. Obavijest se podnosi putem krajnje točke za elektroničko obavješćivanje CSIRT-a koji je imenovan koordinatorom države članice u kojoj proizvođač ima glavni poslovni nastan u Uniji i istodobno je dostupna ENISA-i.

Za potrebe ove Uredbe smatra se da proizvođač glavni poslovni nastan u Uniji ima u onoj državi članici u kojoj se pretežno donose odluke povezane s kibernetičkom sigurnosti njegovih proizvoda s digitalnim elementima. Ako se takva država članica ne može utvrditi, smatra se da se glavni poslovni nastan nalazi u državi članici u kojoj predmetni proizvođač ima poslovnu jedinicu s najvećim brojem zaposlenika u Uniji.

Ako proizvođač nema glavni poslovni nastan u Uniji, obavijesti iz stavaka 1. i 3. podnosi s pomoću krajnje točke za elektroničko obavješćivanje CSIRT-a koji je imenovan koordinatorom u državi članici utvrđenoj u skladu sa sljedećim redoslijedom i na temelju informacija dostupnih proizvođaču:

(a) državi članici u kojoj poslovni nastan ima ovlašteni zastupnik koji djeluje u ime proizvođača za najveći broj proizvoda s digitalnim elementima tog proizvođača;

(b) državi članici u kojoj poslovni nastan ima uvoznik koji stavlja na tržište najveći broj proizvoda s digitalnim elementima tog proizvođača;

(c) državi članici u kojoj poslovni nastan ima distributer koji stavlja na raspolaganje na tržištu najveći broj proizvoda s digitalnim elementima tog proizvođača;

(d) državi članici u kojoj se nalazi najveći broj korisnika proizvodâ s digitalnim elementima tog proizvođača.

U pogledu trećeg podstavka točke (d), proizvođač obavijesti povezane sa svakom naknadnom aktivno iskorištenom ranjivošću ili značajnom incidentom koji utječe na sigurnost proizvoda s digitalnim elementima može podnijeti onom CSIRT-u koji je imenovan koordinatorom kojemu je prvotno podnio obavijest.

8. Nakon što dozna za aktivno iskorištenu ranjivost ili ozbiljan incident koji utječe na sigurnost proizvoda s digitalnim elementima, proizvođač mora obavijestiti pogođene korisnike proizvoda s digitalnim elementima i, prema potrebi, sve korisnike o toj ranjivosti ili tom incidentu i, ako je to potrebno, o svim mjerama ublažavanja rizika i korektivnim mjerama koje korisnici mogu poduzeti kako bi ublažili učinak te ranjivosti ili tog incidenta, prema potrebi u strukturiranom strojno čitljivom formatu koji je lako automatski obraditi. Ako proizvođač pravodobno ne obavijesti korisnike proizvoda s digitalnim elementima, obaviješteni CSIRT-ovi koji su imenovani koordinatorima mogu pružiti takve informacije korisnicima kada se to smatra razmjernim i potrebnim za sprečavanje ili ublažavanje učinka te ranjivosti ili tog incidenta.

9. Do 11. prosinca 2025. Komisija donosi delegirane akte u skladu s člankom 61. ove Uredbe radi dopune ove Uredbe utvrđivanjem uvjeta za primjenu razloga povezanih s kibernetičkom sigurnošću na odgodu širenja obavijesti iz članka 16. stavka 2. ove Uredbe. Komisija pri pripremi nacrta tih delegiranih akata surađuje s mrežom CSIRT-ova uspostavljenom u skladu s člankom 15. Direktive (EU) 2022/2555 i ENISA-om.

10. Komisija može provedbenim aktima pobliže odrediti format i postupke dostavljanja obavijesti iz ovog članka te iz članaka 15. i 16. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 62. stavka 2. Komisija pri pripremi tih nacrta provedbenih akata surađuje s mrežom CSIRT-ova i ENISA-om.

Članak 15.

Dobrovoljno izvješćivanje

1. Proizvođači i druge fizičke ili pravne osobe mogu o svakoj ranjivosti proizvoda s digitalnim elementima te o kibernetičkim prijetnjama koje bi mogle utjecati na profil rizičnosti proizvoda s digitalnim elementima na dobrovoljnoj osnovi obavijestiti CSIRT koji je imenovan koordinatorom ili ENISA-u.

2. Proizvođači i druge fizičke ili pravne osobe mogu o svakom incidentu koji utječe na sigurnost proizvoda s digitalnim elementima te o izbjegnutim incidentima koji su mogli dovesti do takvog incidenta na dobrovoljnoj osnovi obavijestiti CSIRT koji je imenovan koordinatorom ili ENISA-u.

3. CSIRT koji je imenovan koordinatorom ili ENISA obrađuju obavijesti iz stavka 1. i stavka 2. ovog članka u skladu s postupkom utvrđenim u članku 16.

CSIRT koji je imenovan koordinatorom može dati prednost obradi obveznih obavijesti nad obradom dobrovoljnih obavijesti.

4. Ako fizička ili pravna osoba koja nije proizvođač obavijesti o aktivno iskorištenoj ranjivosti ili značajnom incidentu koji utječe na sigurnost proizvoda s digitalnim elementima u skladu sa stavkom 1. ili stavkom 2., CSIRT koji je imenovan koordinatorom o tome bez nepotrebne odgode obavješćuje proizvođača.

5. CSIRT-ovi imenovani koordinatorima i ENISA osiguravaju povjerljivost i odgovarajuću zaštitu informacija koje je dostavila fizička ili pravna osoba koja obavješćuje. Ne dovodeći u pitanje sprečavanje, istragu, otkrivanje i progon kaznenih djela, dobrovoljno izvješćivanje ne smije dovesti do nametanja dodanih obveza fizičkoj ili pravnoj osobi koja obavješćuje kojima ne bi podlijegala da nije podnijela obavijest.

Članak 16.

Uspostava jedinstvene platforme za izvješćivanje

1. Za potrebe obavješćivanja iz članka 14. stavaka 1. i 3. i članka 15. stavaka 1. i 2. te kako bi se pojednostavnile obveze proizvođača u pogledu izvješćivanja, ENISA uspostavlja jedinstvenu platformu za izvješćivanje. ENISA upravlja svakodnevnim radom jedinstvene platforme za izvješćivanje i održava je. Arhitektura jedinstvene platforme za izvješćivanje omogućuje državama članicama i ENISA-i da uspostave vlastite krajnje točke za elektroničko obavješćivanje.

2. Po primitku obavijesti, CSIRT koji je imenovan koordinatorom koji je prvotno primio obavijest bez odgode putem jedinstvene platforme za izvješćivanje dijeli obavijest s CSIRT-ovima koji su imenovani koordinatorima na državnim područjima za koja je proizvođač naveo da je proizvod s digitalnim elementima na njima stavljen na raspolaganje.

U iznimnim okolnostima, a posebno na zahtjev proizvođača i s obzirom na stupanj osjetljivosti prijavljenih informacija koji je proizvođač naveo u skladu s člankom 14. stavkom 2. točkom (a) ove Uredbe, dijeljenje obavijesti može se odgoditi na temelju opravdanih razloga povezanih s kibernetičkom sigurnošću na razdoblje koje je nužno, među ostalim ako ranjivost podliježe postupku koordiniranog otkrivanja ranjivosti iz članka 12. stavka 1. Direktive (EU) 2022/2555. Ako CSIRT odluči uskratiti obavijest, odmah obavješćuje ENISA-u o toj odluci i dostavlja obrazloženje za uskraćivanje obavijesti, kao i naznaku o tome kada će podijeliti obavijest u skladu s postupkom dijeljenja utvrđenim u ovom stavku. ENISA može podržati CSIRT pogledu primjene razloga povezanih s kibernetičkom sigurnošću u vezi s odgodom dijeljenja obavijesti.

U posebno iznimnim okolnostima, ako proizvođač u obavijesti iz članka 14. stavka 2. točke (b) navede:

(a) da je zlonamjerni akter aktivno iskoristio prijavljenu ranjivost i da, prema dostupnim informacijama, nije iskorištena ni u jednoj državi članici osim u onoj CSIRT-a koji je imenovan koordinatorom i kojemu je proizvođač prijavio ranjivost;

(b) da bi svako neposredno daljnje dijeljenje prijavljene ranjivosti vjerojatno dovelo do dostave informacija čije bi otkrivanje bilo u suprotnosti s ključnim interesima te države članice; ili

(c) prijavljena ranjivost predstavlja neposredan visok kibernetički sigurnosni rizik koji proizlazi iz daljnjeg dijeljenja;

dok se s predmetnim CSIRT-ovima i ENISA-i ne podijeli potpuna obavijest, ENISA-i se istodobno stavljaju na raspolaganje samo informacija da je proizvođač podnio obavijest, opće informacije o proizvodu, informacije o općoj prirodi iskorištavanja i informacija o tome da su istaknuti razlozi povezani sa sigurnošću. Ako na temelju tih informacija ENISA smatra da postoji sistemski rizik koji utječe na sigurnost unutarnjeg tržišta, ENISA preporučuje CSIRT-u primatelju da potpunu obavijest podijeli s drugim CSIRT-ovima koji su imenovani koordinatorima i samoj ENISA-i.

3. Nakon primitka obavijesti o aktivno iskorištenoj ranjivosti proizvoda s digitalnim elementima ili o značajnom incidentu koji utječe na sigurnost proizvoda s digitalnim elementima, CSIRT-ovi koji su imenovani koordinatorima tijelima za nadzor tržišta svojih država članica pružaju prijavljene informacije koje su tijelima za nadzor tržišta potrebne za ispunjavanje njihovih obveza na temelju ove Uredbe.

4. ENISA poduzima odgovarajuće i razmjerne tehničke, operativne i organizacijske mjere za upravljanje rizicima kojima su izložene sigurnost jedinstvene platforme za izvješćivanje i informacije koje se dostavljaju ili šire putem jedinstvene platforme za izvješćivanje. ENISA bez nepotrebne odgode obavješćuje mrežu CSIRT-ova i Komisiju o svakom sigurnosnom incidentu koji utječe na jedinstvenu platformu za izvješćivanje.

5. ENISA u suradnji s mrežom CSIRT-ova pruža i implementira specifikacije o tehničkim, operativnim i organizacijskim mjerama u pogledu uspostave, održavanja i sigurnog rada jedinstvene platforme za izvješćivanje iz stavka 1., uključujući barem sigurnosne aranžmane povezane s uspostavom, radom i održavanjem jedinstvene platforme za izvješćivanje, kao i s krajnjim točkama za elektroničko obavješćivanje koje su uspostavili CSIRT-ovi koji su imenovani koordinatorima, na nacionalnoj razini, i ENISA, na razini Unije, uključujući postupovne aspekte kako bi se osiguralo da se, ako za prijavljenu ranjivost nema dostupnih korektivnih mjera ili mjera ublažavanja, informacije o toj ranjivosti razmjenjuju u skladu sa strogim sigurnosnim protokolima i prema načelu nužnog pristupa.

6. Ako je CSIRT koji je imenovan koordinatorom obaviješten o aktivno iskorištenoj ranjivosti u okviru postupka koordiniranog otkrivanja ranjivosti iz članka 12. stavka 1. Direktive (EU) 2022/2555, CSIRT koji je imenovan koordinatorom i koji je prvotno primio obavijest može odgoditi dijeljenje relevantne obavijesti putem jedinstvene platforme za izvješćivanje na temelju opravdanih razloga povezanih s kibernetičkom sigurnošću na razdoblje koje nije dulje nego što je nužno i sve dok strane uključene u koordinirano otkrivanje ranjivosti ne daju suglasnost za otkrivanje. Taj zahtjev ne sprečava proizvođače da na dobrovoljnoj osnovi obavijeste o takvoj ranjivosti u skladu s postupkom utvrđenim u ovom članku.

Članak 17.

Ostale odredbe povezane s izvješćivanjem

1. ENISA Europskoj mreži organizacija za vezu za kibernetičke krize (EU-CyCLONe), uspostavljenoj člankom 16. Direktive (EU) 2022/2555, može dostaviti informacije prijavljene u skladu s člankom 14. stavcima 1. i 3. te člankom 15. stavcima 1. i 2. ove Uredbe, ako su takve informacije važne za koordinirano upravljanje velikim kibernetičkim sigurnosnim incidentima i krizama na operativnoj razini. Za potrebe utvrđivanja te relevantnosti ENISA može uzeti u obzir tehničke analize koje provodi mreža CSIRT-ova, ako su dostupne.

2. Ako je za sprečavanje ili ublažavanje značajnog incidenta koji utječe na sigurnost proizvoda s digitalnim elementima ili za rješavanje incidenta koji je u tijeku potrebno osvješćivanje javnosti, ili ako je otkrivanje incidenta u javnom interesu na neki drugi način, CSIRT koji je imenovan koordinatorom relevantne države članice može, nakon savjetovanja s predmetnim proizvođačem i prema potrebi u suradnji s ENISA-om, obavijestiti javnost o incidentu ili zatražiti od proizvođača da to učini.

3. Na temelju obavijesti primljenih u skladu s člankom 14. stavcima 1. i 3. te člankom 15. stavcima 1. i 2. ENISA svaka 24 mjeseca izrađuje tehničko izvješće o novim trendovima u području kibernetičkih sigurnosnih rizika proizvoda s digitalnim elementima i dostavlja ga skupini za suradnju uspostavljenoj u skladu s člankom 14. Direktive (EU) 2022/2555. Prvo takvo izvješće dostavlja se u roku od 24 mjeseca od datuma početka primjene obveza utvrđenih u članku 14. stavcima 1. i 3. ENISA uključuje relevantne informacije iz svojih tehničkih izvješća u svoje izvješće o stanju kibernetičke sigurnosti u Uniji u skladu s člankom 18. Direktive (EU) 2022/2555.

4. Fizička ili pravna osoba koja obavješćuje u skladu s člankom 14. stavcima 1. i 3. ili člankom 15. stavcima 1. i 2. ne podliježe samo zbog obavješćivanja povećanoj odgovornosti.

5. Nakon što bude dostupno sigurnosno ažuriranje ili neki drugi oblik korektivne mjere ili mjere ublažavanja, ENISA, u dogovoru s proizvođačem predmetnog proizvoda s digitalnim elementima, tu javno poznatu ranjivost prijavljenu u skladu s člankom 14. stavkom 1. ili člankom 15. stavkom 1. ove Uredbe dodaje u europsku bazu podataka o ranjivostima uspostavljenu u skladu s člankom 12. stavkom 2. Direktive (EU) 2022/2555.

6. CSIRT-ovi koji su imenovani koordinatorima pružaju podršku proizvođačima u vezi s obvezama u pogledu izvješćivanja na temelju članka 14., a posebno proizvođačima koji se smatraju mikropoduzećima ili malim ili srednjim poduzećima.

Članak 18.

Ovlašteni zastupnici

1. Proizvođač može na temelju pisanog ovlaštenja imenovati ovlaštenog zastupnika.

2. Obveze utvrđene u članku 13. stavcima od 1. do 11., članku 13. stavku 12. prvom podstavku te članku 13. stavku 14. nisu dio ovlaštenja ovlaštenog zastupnika.

3. Ovlašteni zastupnik obavlja zadaće navedene u ovlaštenju koje mu je dao proizvođač. Ovlašteni zastupnik tijelima za nadzor tržišta na zahtjev dostavlja presliku ovlaštenja. Ovlaštenjem se ovlaštenom zastupniku omogućuje da čini barem sljedeće:

(a) da drži EU izjavu o sukladnosti iz članka 28. i tehničku dokumentaciju iz članka 31. na raspolaganju tijelima za nadzor tržišta najmanje 10 godina nakon što je proizvod s digitalnim elementima stavljen na tržište ili tijekom razdoblja potpore, ovisno o tome što je dulje;

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

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

Članak 19.

Obveze uvoznika

1. Uvoznici stavljaju na tržište samo proizvode s digitalnim elementima koji su usklađeni s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu I. Priloga I. i ako su procesi koje je proizvođač uspostavio usklađeni s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu II. Priloga I.

2. Prije stavljanja proizvoda s digitalnim elementima na tržište uvoznici osiguravaju:

(a) da je proizvođač proveo odgovarajuće postupke ocjenjivanja sukladnosti kako su navedeni u članku 32.;

(b) da je proizvođač sastavio tehničku dokumentaciju;

(c) da proizvod s digitalnim elementima nosi oznaku CE iz članka 30. i da mu je priložena EU izjava o sukladnosti iz članka 13. stavka 20. te informacije i upute za korisnika kako je utvrđeno u Prilogu II., na jeziku koji korisnici i tijela za nadzor tržišta mogu bez poteškoća razumjeti;

(d) da proizvođač ispunjava zahtjeve utvrđene u članku 13. stavcima 15., 16. i 19.

Za potrebe ovog stavka uvoznici moraju moći dostaviti potrebne dokumente kojima se dokazuje ispunjavanje zahtjeva utvrđenih u ovom članku.

3. Ako uvoznik smatra ili ima razloga vjerovati da proizvod s digitalnim elementima ili procesi koje je proizvođač uspostavio nisu sukladni s ovom Uredbom, ne smije staviti taj proizvod na tržište dok se ne postigne sukladnost tog proizvoda ili procesa koje je proizvođač uspostavio s ovom Uredbom. Nadalje, ako proizvod s digitalnim elementima predstavlja znatan kibernetički sigurnosni rizik, uvoznik o tome obavješćuje proizvođača i tijela za nadzor tržišta.

Ako uvoznik ima razloga vjerovati da proizvod s digitalnim elementima može predstavljati znatan kibernetički sigurnosni rizik s obzirom na netehničke čimbenike rizika, uvoznik o tome obavješćuje tijela za nadzor tržišta. Po primitku takvih informacija tijela za nadzor tržišta slijede postupke iz članka 54. stavka 2.

4. Uvoznici na proizvodu s digitalnim elementima, na pakiranju ili u dokumentu priloženom uz proizvod s digitalnim elementima navode svoje ime, registrirano trgovačko ime ili registrirani žig, poštansku adresu, e-adresu ili druge podatke za digitalni kontakt te, ako je primjenjivo, internetske stranice preko kojih se može stupiti u kontakt s njima. Podaci za kontakt moraju biti na jeziku koji korisnici i tijela za nadzor tržišta razumiju bez poteškoća.

5. Uvoznici koji znaju ili imaju razloga vjerovati da proizvod s digitalnim elementima koji su stavili na tržište nije sukladan s ovom Uredbom odmah poduzimaju potrebne korektivne mjere kako bi osigurali da se postigne sukladnost proizvoda s digitalnim elementima s ovom Uredbom ili, prema potrebi, povukli ili opozvali proizvod.

Nakon što doznaju za ranjivosti proizvoda s digitalnim elementima uvoznici o njoj bez nepotrebne odgode obavješćuju proizvođača. Nadalje, ako proizvod s digitalnim elementima predstavlja znatan kibernetički sigurnosni rizik, uvoznici o tome odmah 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.

6. Uvoznici najmanje 10 godina od stavljanja proizvoda s digitalnim elementima na tržište ili tijekom razdoblja potpore, ovisno o tome što je dulje, drže primjerak EU izjave o sukladnosti na raspolaganju tijelima za nadzor tržišta i osiguravaju da tehnička dokumentacija može biti dostupna tim tijelima na zahtjev.

7. Na obrazložen zahtjev tijela za nadzor tržišta uvoznici tom tijelu dostavljaju, u papirnatom ili elektroničkom obliku, sve informacije i svu dokumentaciju potrebne za dokazivanje sukladnosti proizvoda s digitalnim elementima s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu I. Priloga I. te procesa koje je proizvođač uspostavio s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu II. Priloga I. na jeziku koje to tijelo može bez

poteškoća razumjeti. Na zahtjev tog tijela oni s njim surađuju u pogledu svake mjere koja je poduzeta kako bi se uklonili kibernetički sigurnosni rizici koje predstavlja proizvod s digitalnim elementima koji su stavili na tržište.

8. Ako uvoznik proizvoda s digitalnim elementima dozna da je proizvođač tog proizvoda prestao s radom i zato ne može ispuniti obveze utvrđene u ovoj Uredbi, 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 20.

Obveze distributera

1. Pri stavljanju proizvoda s digitalnim elementima na raspolaganje na tržištu distributeri postupaju s dužnom pažnjom u pogledu zahtjeva utvrđenih u ovoj Uredbi.

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

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

(b) jesu li proizvođač i uvoznik ispunili obveze utvrđene u članku 13. stavcima 15., 16., 18., 19. i 20. i članku 19. stavku 4. te jesu li distributeru dostavili sve potrebne dokumente;

3. Ako distributer smatra ili ima razloga vjerovati, na temelju informacija koje posjeduje, da proizvod s digitalnim elementima ili procesi koje je proizvođač uspostavio nisu sukladni s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I., distributer ne smije staviti na raspolaganje na tržištu proizvod s digitalnim elementima dok se ne postigne sukladnosti tog proizvoda ili procesa koje je proizvođač uspostavio s ovom Uredbom. Nadalje, ako proizvod s digitalnim elementima predstavlja znatan kibernetički sigurnosni rizik, distributer o tome bez nepotrebne odgode obavješćuje proizvođača i tijela za nadzor tržišta.

4. Distributeri koji znaju ili imaju razloga vjerovati, na temelju informacija koje posjeduju, da proizvod s digitalnim elementima koji su stavili na raspolaganje na tržištu ili procesi koje je proizvođač uspostavio nisu sukladni s ovom Uredbom osiguravaju poduzimanje korektivnih mjera koje su potrebne da se ponovno uspostavi sukladnosti tog proizvoda s digitalnim elementima ili procesa koje je proizvođač uspostavio ili da se proizvod prema potrebi povuče ili opozove.

Nakon što doznaju za ranjivosti proizvoda s digitalnim elementima distributeri o njoj bez nepotrebne odgode obavješćuju proizvođača. Nadalje, ako proizvod s digitalnim elementima predstavlja znatan kibernetički sigurnosni rizik, distributeri o tome odmah 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 dostavljaju, u papirnatom ili elektroničkom obliku, sve informacije i svu dokumentaciju potrebne za dokazivanje sukladnosti proizvoda s digitalnim elementima i procesa koje je proizvođač uspostavio s ovom Uredbom, na jeziku koje to tijelo može bez poteškoća razumjeti. Na zahtjev tog tijela distributeri s njim surađuju u pogledu svake mjere koja je poduzeta radi uklanjanja kibernetičkih sigurnosnih rizika koje predstavljaju proizvodi s digitalnim elementima koje su stavili na raspolaganje na tržištu.

6. Ako distributer proizvoda s digitalnim elementima dozna, na temelju informacija koje posjeduje, da je proizvođač tog proizvoda prestao s radom i zato ne može ispuniti obveze utvrđene u ovoj Uredbi, distributer o toj situaciji obavješćuje, bez nepotrebne odgode, relevantna 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 21.

Slučajevi u kojem se obveze proizvođača primjenjuju na uvoznike i distributere

Uvoznik ili distributer smatra se proizvođačem za potrebe ove Uredbe te podliježe člancima 13. i 14. 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 22.

Drugi slučajevi u kojima se primjenjuju obveze proizvođača

1. Fizička ili pravna osoba, koja nije proizvođač, uvoznik ili distributer, koja učini bitnu izmjenu proizvoda s digitalnim elementima i stavi taj proizvod na raspolaganje na tržištu smatra se proizvođačem za potrebe ove Uredbe.

2. Osoba iz stavka 1. ovog članka podliježe obvezama utvrđenima u člancima 13. i 14. za dio proizvoda s digitalnim elementima na koji utječe bitna izmjena ili, ako bitna izmjena utječe na kibernetičku sigurnost proizvoda s digitalnim elementima u cjelini, za cijeli proizvod.

Članak 23.

Identifikacija gospodarskih subjekata

1. Gospodarski subjekti tijelima za nadzor tržišta na zahtjev pružaju sljedeće informacije:

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

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

2. Gospodarski subjekti moraju moći predočiti informacije iz stavka 1. 10 godina nakon što im je proizvod s digitalnim elementima isporučen i 10 godina nakon što su isporučili proizvod s digitalnim elementima.

Članak 24.

Obveze upravitelja softvera otvorenog koda

1. Upravitelji softvera otvorenog koda uspostavljaju i na provjerljiv način dokumentiraju kibernetičku sigurnosnu politiku kako bi se potaknuo razvoj sigurnog proizvoda s digitalnim elementima te kako bi razvojni programeri tog proizvoda djelotvorno postupali s ranjivostima. Tom se politikom također potiče razvojne programere tog proizvoda da dobrovoljno prijavljuju ranjivosti kako je utvrđeno u članku 15. te se uzima u obzir posebna priroda upravitelja softvera otvorenog koda te pravni i organizacijski aranžmani kojima podliježe. Ta politika posebno uključuje aspekte povezane s dokumentiranjem, rješavanjem i otklanjanjem ranjivosti te se njome promiče dijeljenje informacija o otkrivenim ranjivostima unutar zajednice otvorenog koda.

2. Upravitelji softvera otvorenog koda surađuju s tijelima za nadzor tržišta, na njihov zahtjev, kako bi se ublažili kibernetički sigurnosni rizici koje predstavlja proizvod s digitalnim elementima koji se smatra besplatnim softverom otvorenog koda.

Na obrazložen zahtjev tijela za nadzor tržišta upravitelji softvera otvorenog koda dostavljaju tom tijelu, na jeziku koji to tijelo može bez poteškoća razumjeti, dokumentaciju iz stavka 1., u papirnatom ili elektroničkom obliku.

3. Obveze utvrđene u članku 14. stavku 1. primjenjuju se na upravitelje softvera otvorenog koda u mjeri u kojoj su uključeni u razvoj proizvoda s digitalnim elementima. Obveze utvrđene u članku 14. stavcima 3. i 8. primjenjuju se na upravitelje softvera otvorenog koda u mjeri u kojoj značajni incidenti koji utječu na sigurnost proizvoda s digitalnim elementima utječu na mrežne i informacijske sustave koje upravitelji softvera otvorenog koda pružaju za razvoj takvih proizvoda.

Članak 25.

Potvrda o sigurnosti besplatnog softvera otvorenog koda

Kako bi se olakšala izvršenje obveze dužne pažnje utvrđene u članku 13. stavku 5., posebno u pogledu proizvođača koji u svoje proizvode s digitalnim elementima integriraju besplatne softverske komponente otvorenog koda, Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 61. radi dopune ove Uredbe uspostavom dobrovoljnih programa potvrda o sigurnosti kojima se razvojnim programerima ili korisnicima proizvoda s digitalnim elementima koji se smatraju besplatnim softverom otvorenog koda te ostalim trećim stranama omogućuje ocjenjivanje sukladnosti takvih proizvoda sa svim ili određenim bitnim zahtjevima u pogledu kibernetičke sigurnosti ili drugim obvezama utvrđenima u ovoj Uredbi.

Članak 26.

Smjernice

1. Kako bi se olakšala provedba i osigurala dosljednost takve provedbe, Komisija objavljuje smjernice kako bi pomogla gospodarskim subjektima u primjeni ove Uredbe, s posebnim naglaskom na olakšavanje usklađenosti mikropoduzeća, malih poduzeća i srednjih poduzeća.

2. Ako namjerava pružiti smjernice kako je navedeno u stavku 1., Komisija obuhvaća barem sljedeće aspekte:

(a) područje primjene ove Uredbe, s posebnim naglaskom na rješenja za daljinsku obradu podataka te besplatan softver otvorenog koda;

(b) primjenu razdobljâ potpore u odnosu na određene kategorije proizvoda s digitalnim elementima;

(c) smjernice usmjerene na proizvođače na koje se primjenjuje ova Uredba i na koje se također primjenjuje zakonodavstvo Unije o usklađivanju koje nije ova Uredba ili drugi povezani pravni akti Unije;

(d) pojam bitne izmjene.

Komisija također vodi jednostavno dostupan popis delegiranih i provedbenih akata donesenih u skladu s ovom Uredbom.

3. Pri izradi smjernica u skladu s ovim člankom Komisija se savjetuje s relevantnim dionicima.

POGLAVLJE III.

SUKLADNOST PROIZVODA S DIGITALNIM ELEMENTIMA

Članak 27.

Pretpostavka sukladnosti

1. Za proizvode s digitalnim elementima i procese 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 u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. obuhvaćenima tim normama ili njihovim dijelovima.

Komisija u skladu s člankom 10. stavkom 1. Uredbe (EU) br. 1025/2012 od jedne ili više europskih organizacija za normizaciju zahtijeva da izrade usklađene norme za bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u Prilogu I. ovoj Uredbi. Prilikom pripreme zahtjeva za normizaciju za ovu Uredbu Komisija nastoji uzeti u obzir europske i međunarodne norme za kibernetičku sigurnost, postojeće i one čiji je razvoj u tijeku, kako bi se pojednostavio razvoj usklađenih normi, u skladu s Uredbom (EU) br. 1025/2012.

2. Komisija može donijeti provedbene akte kojima se utvrđuju zajedničke specifikacije koje obuhvaćaju tehničke zahtjeve kojima se osigurava sredstvo za usklađivanje s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. za proizvode s digitalnim elementima obuhvaćene područjem primjene ove Uredbe.

Ti se provedbeni akti donose samo ako su ispunjeni sljedeći uvjeti:

(a) Komisija je u skladu s člankom 10. stavkom 1. Uredbe (EU) br. 1025/2012, od jedne europske organizacije za normizaciju ili više njih zatražila da izrade usklađenu normu za bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u Prilogu I. i:

   i. zahtjev nije prihvaćen;

   ii. usklađene norme koje se odnose na taj zahtjev nisu izrađene u roku utvrđenom u skladu s člankom 10. stavkom 1. Uredbe (EU) br. 1025/2012; ili

   iii. usklađene norme nisu u skladu sa zahtjevom; i

(b) u *Službenom listu Europske unije* nije objavljeno upućivanje na usklađene norme koje obuhvaćaju relevantne bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u Prilogu I. ovoj Uredbi u skladu s Uredbom (EU) br. 1025/2012 i ne očekuje se objava takvog upućivanja u razumnom roku.

Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 62. stavka 2.

3. Prije nego što izradi nacrt provedbenog akta iz stavka 2. ovog članka, Komisija obavješćuje odbor iz članka 22. Uredbe (EU) br. 1025/2012 kako smatra da su uvjeti iz stavka 2. ovog članka ispunjeni.

4. Pri izradi nacrta provedbenog akta iz stavka 2. Komisija uzima u obzir stajališta relevantnih tijela te se propisno savjetuje sa svim relevantnim dionicima.

5. Za proizvode s digitalnim elementima i procese koje je proizvođač uspostavio i koji su u skladu sa zajedničkim specifikacijama uvedenima provedbenim aktima iz stavka 2. ovog članka ili njihovim dijelovima pretpostavlja se da su u skladu s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. koji su obuhvaćeni tim zajedničkim specifikacijama ili njihovim dijelovima.

6. Ako europska organizacija za normizaciju donese usklađenu normu i predloži je Komisiji radi objave upućivanja na tu organizaciju u *Službenom listu Europske unije*, Komisija ocjenjuje usklađenu normu u skladu s Uredbom (EU) br. 1025/2012. Ako se u *Službenom listu Europske unije* objavi upućivanje na usklađenu normu, Komisija stavlja izvan snage provedbene akte iz stavka 2. ovog članka ili dijelove tih provedbenih akata koji obuhvaćaju iste bitne zahtjeve u pogledu kibernetičke sigurnosti na koje se odnosi predmetna usklađena norma.

7. Ako država članica smatra da zajednička specifikacija ne ispunjava u potpunosti bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u Prilogu I., o tome obavješćuje Komisiju u detaljnom objašnjenju. Komisija ocjenjuje to detaljno objašnjenje i, prema potrebi, može izmijeniti provedbeni akt kojim se uvodi predmetna zajednička specifikacija.

8. Za proizvode s digitalnim elementima i procese koje je proizvođač uspostavio za koje su izdani EU izjava o sukladnosti ili certifikat u okviru europskog programa kibernetičke sigurnosne certifikacije donesenog u skladu s Uredbom (EU) 2019/881 pretpostavlja se da su sukladni s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. u mjeri u kojoj EU izjava o sukladnosti ili europski kibernetički sigurnosni certifikat, ili njihovi dijelovi, obuhvaćaju te zahtjeve.

9. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 61. ove Uredbe radi dopune ove Uredbe određivanjem europskih programa kibernetičke sigurnosne certifikacije donesenih na temelju Uredbe (EU) 2019/881 koji se mogu upotrijebiti za dokazivanje sukladnosti proizvoda s digitalnim elementima s bitnim zahtjevima u pogledu kibernetičke sigurnosti ili njihovim dijelovima utvrđenima u Prilogu I. ovoj Uredbi. Nadalje, izdavanje europskog kibernetičkog sigurnosnog certifikata izdanog u okviru takvih programa na barem „znatnoj" razini jamstva, oslobađa proizvođače obveze ocjenjivanja sukladnosti koje provodi treća strana za odgovarajuće zahtjeve, kako je utvrđeno u članku 32. stavku 2. točkama (a) i (b) i članku 32. stavku 3. točkama (a) i (b) ove Uredbe.

Članak 28.

EU izjava o sukladnosti

1. EU izjavu o sukladnosti sastavljaju proizvođači u skladu s člankom 13. stavkom 12. i u njoj se navodi da je dokazano ispunjavanje primjenjivih bitnih zahtjeva u pogledu kibernetičke sigurnosti utvrđenih u Prilogu I.

2. EU izjava o sukladnosti ima strukturu predloška utvrđenu u Prilogu V. i sadržava elemente određene u odgovarajućim postupcima ocjenjivanja sukladnosti utvrđenima u Prilogu VIII. Takva se izjava ažurira prema potrebi. 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.

Pojednostavljena EU izjava o sukladnosti iz članka 13. stavka 20. ima strukturu predloška utvrđenu u Prilogu VI. 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 pravnih akata Unije kojima se zahtijeva EU izjava o sukladnosti, u vezi sa svim takvim pravnim aktima Unije sastavlja se samo jedna EU izjava o sukladnosti. U toj izjavi navodi se o kojim je pravnim aktima Unije riječ, uključujući upućivanja na njihove objave.

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

5. Kako bi se uzele u obzir tehnološke promjene, Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 61. radi dopune ove Uredbe dodavanjem elemenata minimalnom sadržaju EU izjave o sukladnosti utvrđene u Prilogu V.

Članak 29.

Opća načela za oznaku CE

Na oznaku CE primjenjuju se opća načela utvrđena u članku 30. Uredbe (EZ) br. 765/2008.

Članak 30.

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 28. 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 28. ili na popratne internetske stranice softverskog proizvoda. U potonjem slučaju relevantni dio internetskih stranica mora biti lako i izravno dostupan potrošačima.

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 kibernetički sigurnosni rizik ili posebnu upotrebu 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 32.

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 upotrebe te oznake. Ako proizvod s digitalnim elementima podliježe zakonodavstvu Unije o usklađivanju koje nije ova Uredba, a kojim se također propisuje stavljanje oznake CE, na oznaci CE navodi se da proizvod ispunjava i zahtjeve utvrđene u takvom drugom zakonodavstvu Unije o usklađivanju.

6. Komisija može delegiranim aktima utvrditi tehničke specifikacije za oznake, piktograme ili bilo koje druge oznake povezane sa sigurnošću proizvoda s digitalnim elementima, njihova razdoblja potpore te mehanizme za promicanje njihove upotrebe i podizanje razine svijesti u javnosti o sigurnosti proizvoda s digitalnim elementima. Pri pripremi nacrta provedbenih akata Komisija se savjetuje s relevantnim dionicima i, ako je to već utvrđeno u skladu s člankom 52. stavkom 15., sa skupinom za ADCO. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 62. stavka 2.

Članak 31.

Tehnička dokumentacija

1. Tehnička dokumentacija sadržava sve relevantne podatke ili pojedinosti o načinima na koje proizvođač osigurava usklađenost proizvoda s digitalnim elementima i procesa koje je uspostavio s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. Ona sadržava barem elemente utvrđene u Prilogu VII.

2. Tehnička dokumentacija sastavlja se prije stavljanja na tržište proizvoda s digitalnim elementima i redovito se ažurira, prema potrebi, najmanje tijekom razdoblja potpore.

3. Za proizvode s digitalnim elementima iz članka 12. koji podliježu i drugim pravnim aktima Unije kojima se predviđa tehnička dokumentacija sastavlja se jedinstvena tehnička dokumentacija koja sadržava informacije iz Priloga VII. i informacije koje se zahtijevaju tim pravnim 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 jeziku koji je prihvatljiv tom tijelu.

5. Komisija je ovlaštena za donošenje delegiranih akata u skladu s člankom 61. radi dopune ove Uredbe dodavanjem elemenata koje treba uključiti u tehničku dokumentaciju iz Priloga VII. kako bi se uzele u obzir tehnološke promjene i iskustva u procesu provedbe ove Uredbe. U tu svrhu Komisija nastoji osigurati da je administrativno opterećenje za mikropoduzeća te mala i srednja poduzeća proporcionalno.

Članak 32.

Postupci ocjenjivanja sukladnosti proizvoda s digitalnim elementima

1. Proizvođač provodi ocjenjivanje sukladnosti proizvoda s digitalnim elementima i procesa koje je uspostavio kako bi utvrdio jesu li ispunjeni bitni zahtjevi u pogledu kibernetičke sigurnosti utvrđeni u Prilogu I. Proizvođač sukladnost s bitnim zahtjevima u pogledu kibernetičke sigurnosti dokazuje primjenom bilo kojeg od sljedećih postupaka:

(a) postupak unutarnje kontrole (na temelju modula A) utvrđen u Prilogu VIII.;

(b) postupak EU ispitivanja tipa (na temelju modula B) utvrđen u Prilogu VIII., nakon čega slijedi provjera sukladnosti s EU tipom koja se temelji na unutarnjoj kontroli proizvodnje (na temelju modula C) utvrđenoj u Prilogu VIII.;

(c) ocjenjivanje sukladnosti na temelju potpunog osiguranja kvalitete (na temelju modula H) utvrđeno u Prilogu VIII.; ili

(d) ako je dostupan i primjenjiv, europski program kibernetičke sigurnosne certifikacije u skladu s člankom 27. stavkom 9.

2. Ako proizvođač pri ocjenjivanju sukladnosti važnog proizvoda s digitalnim elementima koji se ubraja u I. razred kako je utvrđeno u Prilogu III. i procesa koje je njegov proizvođač uspostavio s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. nije primijenio ili je samo djelomično primijenio usklađene norme, zajedničke specifikacije ili europske programe kibernetičke sigurnosne certifikacije na barem „znatnoj" razini jamstva iz članka 27. ili ako takve usklađene norme, zajedničke specifikacije ili europski programi kibernetičke sigurnosne certifikacije ne postoje, predmetni proizvod s digitalnim elementima i procesi koje je proizvođač uspostavio podvrgavaju se, s obzirom na te bitne zahtjeve u pogledu kibernetičke sigurnosti, bilo kojem od sljedećih postupaka:

(a) postupak EU ispitivanja tipa (na temelju modula B) utvrđen u Prilogu VIII., nakon čega slijedi provjera sukladnosti s EU tipom koja se temelji na unutarnjoj kontroli proizvodnje (na temelju modula C) utvrđenoj u Prilogu VIII.; ili

(b) ocjenjivanje sukladnosti na temelju potpunog osiguranja kvalitete (na temelju modula H) utvrđeno u Prilogu VIII.

3. Ako je proizvod važan proizvod s digitalnim elementima koji se ubraja u II. razred kako je utvrđeno u Prilogu III., proizvođač sukladnost s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. dokazuje primjenom bilo kojeg od sljedećih postupaka:

(a) postupak EU ispitivanja tipa (na temelju modula B) utvrđen u Prilogu VIII., nakon čega slijedi provjera sukladnosti s EU tipom koja se temelji na unutarnjoj kontroli proizvodnje (na temelju modula C) utvrđen u Prilogu VIII.

(b) ocjenjivanje sukladnosti na temelju potpunog osiguranja kvalitete (na temelju modula H) utvrđeno u Priloga VIII. ili

(c) ako je dostupan i primjenjiv, europski program kibernetičke sigurnosne certifikacije u skladu s člankom 27. stavkom 9. ove Uredbe na barem „znatnoj" razini jamstva u skladu s Uredbom (EU) 2019/881.

4. Za kritične proizvode s digitalnim elementima navedene u Prilogu IV. sukladnost s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. dokazuje se primjenom jednog od sljedećih postupaka:

(a) europski program kibernetičke sigurnosne certifikacije u skladu s člankom 8. stavkom 1.; ili

(b) ako uvjeti iz članka 8. stavka 1. nisu ispunjeni, bilo koji od postupaka iz stavka 3. ovog članka.

5. Proizvođači proizvoda s digitalnim elementima koji se smatraju besplatnim softverom otvorenog koda, koji pripadaju kategorijama utvrđenima u Prilogu III., moraju biti u stanju dokazati sukladnost s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. primjenom jednog od postupaka iz stavka 1. ovog članka, pod uvjetom da je tehnička dokumentacija iz članka 31. stavljena na raspolaganje javnosti u trenutku stavljanja tih proizvoda na tržište.

6. Posebni interesi i potrebe mikropoduzeća te malih i srednjih poduzeća, uključujući novoosnovana poduzeća, uzimaju se u obzir pri određivanju naknada za postupke ocjenjivanja sukladnosti i te se naknade smanjuju razmjerno njihovim posebnim interesima i potrebama.

Članak 33.

Mjere potpore za mikropoduzeća te mala i srednja poduzeća, uključujući novoosnovana poduzeća

1. Države članice, prema potrebi, poduzimaju sljedeće mjere prilagođene potrebama mikropoduzeća i malih poduzeća:

(a) organiziraju posebne aktivnosti podizanja razine svijesti i aktivnosti osposobljavanja o primjeni ove Uredbe;

(b) uspostavljaju poseban kanal za komunikaciju s mikropoduzećima i malim poduzećima te, prema potrebi, s lokalnim javnim tijelima radi pružanja savjeta i odgovaranja na upite o provedbi ove Uredbe;

(c) podupiru aktivnosti ispitivanja i ocjenjivanja sukladnosti, uključujući, prema potrebi, potporu Europskog stručnog centra u području kibernetičke sigurnosti.

2. Države članice mogu, prema potrebi, uspostaviti regulatorna izolirana okruženja za kibernetičku otpornost. Takva regulatorna izolirana okruženja osiguravaju kontrolirana okruženja za ispitivanje inovativnih proizvoda s digitalnim elementima kako bi se olakšali njihov razvoj, projektiranje, validacija i testiranje u svrhu usklađivanja s ovom Uredbom tijekom ograničenog razdoblja prije stavljanja na tržište. Komisija i, prema potrebi, ENISA mogu pružati tehničku potporu, savjete i alate za uspostavu i rad regulatornih izoliranih okruženja. Regulatorna izolirana okruženja uspostavljaju se pod izravnim nadzorom tijela za nadzor tržišta te uz njihove smjernice i potporu. Države članice obavješćuju Komisiju i druga tijela za nadzor tržišta o uspostavi regulatornog izoliranog okruženja preko skupine za ADCO. Regulatorna izolirana okruženja ne utječu na nadzorne i korektivne ovlasti nadležnih tijela. Države članice osiguravaju otvoren, pravedan i transparentan pristup regulatornim izoliranim okruženjima, a u prvom redu olakšavaju pristup mikropoduzećima i malim poduzećima, uključujući novoosnovana poduzeća.

3. U skladu s člankom 26. Komisija mikropoduzećima te malim i srednjim poduzećima pruža smjernice u vezi s provedbom ove Uredbe.

4. Komisija informira o dostupnoj financijskoj potpori u regulatornom okviru postojećih programa Unije, posebno kako bi se smanjio financijski teret za mikropoduzeća i mala poduzeća.

5. Mikropoduzeća i mala poduzeća mogu dostaviti sve elemente tehničke dokumentacije navedene u Prilogu VII. u pojednostavnjenom formatu. U tu svrhu Komisija provedbenim aktima utvrđuje pojednostavnjeni obrazac tehničke dokumentacije namijenjen potrebama mikropoduzeća i malih poduzeća, uključujući način na koji se moraju osigurati elementi utvrđeni u Prilogu VII. Ako mikropoduzeće ili malo poduzeće odluči na pojednostavnjen način dostaviti informacije utvrđene u Prilogu VII., koristi se obrascem iz ovog stavka. Prijavljena tijela prihvaćaju taj obrazac za potrebe ocjenjivanja sukladnosti.

Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 62. stavka 2.

Članak 34.

Sporazumi o uzajamnom priznavanju

Uzimajući u obzir razinu tehničkog razvoja i pristup ocjenjivanju sukladnosti treće zemlje, Unija može sklopiti sporazume o uzajamnom priznavanju s trećim zemljama, u skladu s člankom 218. UFEU-a, radi promicanja i olakšavanja međunarodne trgovine.

POGLAVLJE IV.

PRIJAVLJIVANJE TIJELA ZA OCJENJIVANJE SUKLADNOSTI

Članak 35.

Prijavljivanje

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

2. Države članice nastoje do 11. prosinca 2026. osigurati da u Uniji postoji dovoljan broj prijavljenih tijela za ocjenjivanje sukladnosti kako bi se izbjegla uska grla i prepreke ulasku na tržište.

Članak 36.

Tijela koja provode prijavljivanje

1. Svaka država članice imenuje tijelo koje provodi prijavljivanje odgovorno za utvrđivanje i provedbu postupaka potrebnih za ocjenjivanje, imenovanje i prijavljivanje tijelâ za ocjenjivanje sukladnosti te njihovo praćenje, uključujući usklađenost s člankom 41.

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.

3. Ako tijelo koje provodi prijavljivanje delegira ili na neki drugi način povjeri ocjenjivanje, prijavljivanje ili praćenje iz stavka 1. ovog članka tijelu koje nije javno tijelo, to tijelo mora biti pravni subjekt i, *mutatis mutandis*, biti u skladu s člankom 37. Nadalje, navedeno tijelo mora uspostaviti mehanizme kojima se obuhvaćaju odgovornosti koje proizlaze iz njegovih aktivnosti.

4. Tijelo koje provodi prijavljivanje preuzima punu odgovornost za zadaće koje obavlja tijelo iz stavka 3.

Članak 37.

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 kompetentne 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 38.

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 objavljuje informacije iz stavka 1.

Članak 39.

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 koju ocjenjuje ili proizvodu s digitalnim elementima koji ocjenjuje.

Tijelo koje je član poslovnog udruženja ili strukovne udruge koje predstavlja poduzeća uključena u projektiranje, razvoj, proizvodnju, dobavu, sastavljanje, upotrebu ili održavanje proizvoda s digitalnim elementima koje ocjenjuje može se smatrati takvim tijelom za ocjenjivanje sukladnosti koje ima svojstvo treće strane 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, uvoznik, distributer, instalater, kupac, vlasnik, korisnik ili održavatelj proizvoda s digitalnim elementima koji ocjenjuju kao ni ovlašteni zastupnik bilo koje od tih strana. Time se ne sprečava upotreba ocijenjenih proizvoda koji su potrebni za rad tijela za ocjenjivanje sukladnosti niti upotreba takvih proizvoda 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, uvozu, distribuciji, stavljanju na tržište, instaliranju, upotrebi ili održavanju proizvoda s digitalnim elementima koje ocjenjuju 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 osiguravaju 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 VIII. 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 sa stručnim znanjem te dovoljnim i odgovarajućim iskustvom za obavljanje zadaća ocjenjivanja sukladnosti;

(b) opisima postupaka u skladu s kojima se mora provesti ocjenjivanje sukladnosti, čime se osigurava transparentnost i mogućnost ponavljanja tih postupaka. Mora imati 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.

Tijelo za ocjenjivanje sukladnosti raspolaže sredstvima potrebnima za primjereno obavljanje tehničkih i administrativnih zadaća povezanih s aktivnostima ocjenjivanja sukladnosti te ima pristup 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 u pogledu ocjenjivanja koja provodi i odgovarajuće ovlaštenje za ta ocjenjivanja;

(c) odgovarajuće poznavanje i razumijevanje bitnih zahtjeva u pogledu kibernetičke sigurnosti utvrđenih u Prilogu I., važećih usklađenih normi i zajedničkih specifikacija te relevantnih odredaba zakonodavstva Unije o usklađivanju kao i njegovih provedbenih akata;

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

8. Mora biti osigurana nepristranost tijela za ocjenjivanje sukladnosti, njihova najvišeg rukovodstva i osoblja zaduženog za ocjenjivanje.

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

9. Tijela za ocjenjivanje sukladnosti sklapaju ugovor o osiguranju od odgovornosti osim ako je odgovornost preuzela njihova 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 informacije prikupljene pri provođenju svojih zadaća na temelju Priloga VIII. ili bilo koje odredbe nacionalnog prava kojim ga se provodi, osim u odnosu na tijela za nadzor tržišta države članice u kojoj se provode njegove aktivnosti. Vlasnička prava moraju biti zaštićena. Tijelo za ocjenjivanje sukladnosti mora ima uspostavljene dokumentirane postupke kojima se osigurava usklađenost s ovim stavkom.

11. Tijela za ocjenjivanje sukladnosti sudjeluju u odgovarajućim aktivnostima normizacije i aktivnostima koordinacijske skupine prijavljenog tijela osnovane na temelju članka 51. 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, razmjernih i razumnih uvjeta, izbjegavajući pritom nepotrebno opterećenje za gospodarske subjekte, posebno uzimajući u obzir interese mikropoduzeća te malih i srednjih poduzeća u vezi s naknadama.

Članak 40.

Pretpostavka sukladnosti prijavljenih tijela

Ako tijelo za ocjenjivanje sukladnosti dokaže sukladnost s kriterijima utvrđenim u relevantnim usklađenim normama ili dijelovima usklađenih normi na koje su upućivanja objavljena u *Službenom listu Europske unije*, pretpostavlja se da ispunjava zahtjeve utvrđene u članku 39. u mjeri u kojoj primjenjive usklađene norme obuhvaćaju te zahtjeve.

Članak 41.

Društva kćeri prijavljenih tijela i njihovi podizvođači

1. Ako prijavljeno tijelo povjeri određene zadaće povezane s ocjenjivanjem sukladnosti podizvođačima ili ih prenese društvu kćeri, osigurava da taj podizvođač ili to društvo kći ispunjava zahtjeve utvrđene u članku 39. i o tome obavješćuje tijelo koje provodi prijavljivanje.

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

3. Aktivnosti se mogu povjeriti podizvođaču ili ih može provoditi društvo kći samo uz suglasnost proizvođača.

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

Članak 42.

Zahtjev za prijavu

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

2. Zahtjevu za prijavu prilaže se opis aktivnosti ocjenjivanja sukladnosti, postupka ocjenjivanja sukladnosti ili više njih te proizvoda s digitalnim dokumentima ili više njih za koje to tijelo tvrdi da je nadležno te, ako je primjenjivo, potvrda o akreditaciji koju je izdalo nacionalno akreditacijsko tijelo i kojom se potvrđuje da tijelo za ocjenjivanje sukladnosti ispunjava zahtjeve utvrđene u članku 39.

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 utvrđenima u članku 39.

Članak 43.

Postupak prijavljivanja

1. Tijela koja provode prijavljivanje prijavljuju samo tijela za ocjenjivanje sukladnosti koja ispunjavaju zahtjeve iz članka 39.

2. Tijelo koje provodi prijavljivanje prijavljuje Komisiji i drugim državama članicama putem informacijskog sustava prijavljenih i imenovanih tijela prema novom pristupu koji je razvila i vodi Komisija.

3. Prijava sadržava sve pojedinosti o aktivnostima ocjenjivanja sukladnosti, modulu ili modulima za ocjenjivanje sukladnosti te predmetnom proizvodu s digitalnim elementima ili više njih i odgovarajućoj potvrdi o stručnosti.

4. Ako se prijavljivanje ne temelji na potvrdi o akreditaciji iz članka 42. 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 utvrđene u članku 39.

5. Predmetno tijelo može obavljati aktivnosti prijavljenog tijela samo ako Komisija i druge države članice ne podnesu prigovor u roku od dva tjedna od prijave u slučajevima kad se upotrebljava potvrda o akreditaciji ili u roku od dva mjeseca od prijave u slučajevima kad se akreditacija ne upotrebljava.

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 44.

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 pravnih 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 45.

Promjene u vezi s prijavama

1. Ako tijelo koje provodi prijavljivanje utvrdi ili bude obaviješteno da prijavljeno tijelo više ne ispunjava zahtjeve utvrđene u članku 39. ili da ne ispunjava svoje 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 ostale 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 odgovornim tijelima koja provode prijavljivanje i tijelima za nadzor tržišta na njihov zahtjev.

Članak 46.

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 47.

Operativne obveze prijavljenih tijela

1. Prijavljena tijela provode ocjenjivanja sukladnosti u skladu s postupcima ocjenjivanja sukladnosti iz članka 32. i Priloga VIII.

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, posebno u pogledu mikropoduzeća te malih i srednjih poduzeća, sektoru u kojem ona posluju, njihovoj strukturi, njihovu stupnju složenosti i razini kibernetičkog sigurnosnog rizika proizvoda s digitalnim elementima i tehnologije o kojoj je riječ i masovnoj ili serijskoj prirodi proizvodnog procesa.

3. Međutim, prijavljena tijela poštuju stupanj strogosti i razinu zaštite koji su potrebni za sukladnost proizvoda s digitalnim elementima s ovom Uredbom.

4. Ako prijavljeno tijelo utvrdi da proizvođač ne ispunjava zahtjeve utvrđene u Prilogu I. ili u odgovarajućim usklađenim normama ili zajedničkim specifikacijama iz članka 27., 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 utvrdi da proizvod s digitalnim elementima više nije u skladu sa zahtjevima utvrđenima u ovoj Uredbi, ono zahtijeva od proizvođača da poduzme primjerene korektivne mjere te prema 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 48.

Žalbe protiv odluka prijavljenih tijela

Države članice osiguravaju da je na raspolaganju žalbeni postupak protiv odluka prijavljenih tijela.

Članak 49.

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 područje primjene ili uvjete njegove prijave;

(c) svim zahtjevima za dostavu informacija koje su primila od tijelâ 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 podugovaranje.

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

Članak 50.

Razmjena iskustava

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

Članak 51.

Koordinacija prijavljenih tijela

1. Komisija osigurava uspostavu odgovarajuće koordinacije i suradnje 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 IZVRŠAVANJE

Članak 52.

Nadzor tržišta i kontrola proizvoda s digitalnim elementima na tržištu Unije

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

2. Svaka država članica imenuje 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 imenovana u skladu sa stavkom 2. ovog članka odgovorna su i za provedbu aktivnosti nadzora tržišta u vezi s obvezama za upravitelje softvera otvorenog koda utvrđenima u članku 24. Ako tijelo za nadzor tržišta utvrdi da upravitelj softvera otvorenog koda ne ispunjava obveze utvrđene u tom članku, od njega zahtijeva da osigura poduzimanje svih odgovarajućih korektivnih mjera. Upravitelji softvera otvorenog koda osiguravaju poduzimanje svih odgovarajućih korektivnih mjera u pogledu svojih obveza iz ove Uredbe.

4. Tijela za nadzor tržišta prema potrebi surađuju i redovito razmjenjuju informacije s nacionalnim tijelima za kibernetičku sigurnosnu certifikaciju imenovanima na temelju članka 58. Uredbe (EU) 2019/881. Imenovana tijela za nadzor tržišta u pogledu nadzora provedbe obveza u pogledu izvješćivanja na temelju članka 14. ove Uredbe surađuju i redovito razmjenjuju informacije s CSIRT-ovima koji su imenovani koordinatorima i s ENISA-om.

5. Tijela za nadzor tržišta mogu zatražiti od CSIRT-a koji je imenovan koordinatorom ili ENISA-e da pruže tehničke savjete o pitanjima povezanima s provedbom i izvršavanjem ove Uredbe. Pri provedbi istrage u skladu s člankom 54. tijela za nadzor tržišta mogu zatražiti od CSIRT-a koji je imenovan koordinatorom ili ENISA-e da dostave analizu kojom bi se potkrijepile evaluacije sukladnosti proizvoda s digitalnim elementima.

6. Tijela za nadzor tržišta prema potrebi surađuju i redovito razmjenjuju informacije s drugim tijelima za nadzor tržišta imenovanima na temelju zakonodavstva Unije o usklađivanju koje nije ova Uredba.

7. Tijela za nadzor tržišta prema potrebi surađuju s tijelima koja nadziru pravo Unije o zaštiti podataka. Takva suradnja uključuje obavješćivanje tih tijela o svim nalazima relevantnima za ispunjavanje njihovih nadležnosti, među ostalim pri davanju smjernica i savjeta na temelju stavka 10. ako se te smjernice i ti savjeti odnose na obradu osobnih podataka.

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

8. Države članice osiguravaju da imenovana tijela za nadzor tržišta imaju odgovarajuće financijske i tehničke resurse, uključujući, prema potrebi, alate za automatizaciju obrade, kao i ljudske resurse s vještinama u području kibernetičke sigurnosti potrebnima za obavljanje svojih zadaća na temelju ove Uredbe.

9. Komisija potiče i olakšava razmjenu iskustava među imenovanim tijelima za nadzor tržišta.

10. Tijela za nadzor tržišta mogu gospodarskim subjektima pružati smjernice i savjete o provedbi ove Uredbe, uz potporu Komisije i, prema potrebi, CSIRT-ova i ENISA-e.

11. Tijela za nadzor tržišta obavješćuju potrošače o tome gdje podnijeti pritužbe koje bi mogle upućivati na neusklađenost s ovom Uredbom, u skladu s člankom 11. Uredbe (EU) 2019/1020, te potrošačima pružaju informacije o tome gdje i kako pristupiti mehanizmima za lakše prijavljivanje ranjivosti, incidenata i kibernetičkih prijetnji koji mogu utjecati na proizvode s digitalnim elementima.

12. Tijela za nadzor tržišta prema potrebi olakšavaju suradnju s relevantnim dionicima, uključujući znanstvene organizacije, istraživačke organizacije i organizacije potrošača.

13. Tijela za nadzor tržišta na godišnjoj osnovi izvješćuju Komisiju o ishodima relevantnih aktivnosti nadzora tržišta. Imenovana tijela za nadzor tržišta bez odgode izvješćuju Komisiju i relevantna nacionalna tijela za tržišno natjecanje o svim informacijama utvrđenima tijekom aktivnosti nadzora tržišta koje bi mogle biti od interesa za primjenu prava Unije o tržišnom natjecanju.

14. Za proizvode s digitalnim elementima koji su obuhvaćeni područjem primjene ove Uredbe i koji su klasificirani kao visokorizični UI sustavi na temelju članka članaka 6. Uredbe (EU) 2024/1689 tijela za nadzor tržišta imenovana za potrebe te uredbe su tijela nadležna za aktivnosti nadzora tržišta koje se zahtijevaju ovom Uredbom. Tijela za nadzor tržišta imenovana na temelju Uredbe (EU) 2024/1689 prema potrebi surađuju s tijelima za nadzor tržišta imenovanima na temelju ove Uredbe i, u pogledu nadzora provedbe obveza u pogledu izvješćivanja na temelju članka 14. ove Uredbe, s CSIRT-ovima koji su imenovani koordinatorima i ENISA-om. Tijela za nadzor tržišta imenovana na temelju Uredbe (EU) 2024/1689 osobito obavješćuju tijela za nadzor tržišta imenovana na temelju ove Uredbe o svakom nalazu relevantnom za ispunjavanje njihovih zadaća koje se odnose na provedbu ove Uredbe.

15. Radi ujednačene primjene ove Uredbe, u skladu s člankom 30. stavkom 2. Uredbe (EU) 2019/1020, uspostavlja se skupina za ADCO. Skupina za ADCO sastoji se od predstavnika imenovanih tijela za nadzor tržišta i, prema potrebi, predstavnika jedinstvenih ureda za vezu. Skupina za ADCO bavi se i posebnim pitanjima povezanima s aktivnostima nadzora tržišta u vezi s obvezama koje se nameću upraviteljima softvera otvorenog koda.

16. Tijela za nadzor tržišta prate kako su proizvođači primijenili kriterije iz članka 13. stavka 8. pri određivanju razdoblja potpore za svoje proizvode s digitalnim elementima.

Skupina za ADCO u javno dostupnom obliku prilagođenom korisnicima objavljuje relevantne statističke podatke o kategorijama proizvoda s digitalnim elementima, uključujući prosječna razdoblje potpora kako ih odredi proizvođač u skladu s člankom 13. stavkom 8., te pruža smjernice koje uključuju okvirna razdoblja potpore za kategorije proizvoda s digitalnim elementima.

Ako podaci upućuju na neodgovarajuća razdoblja potpore za određene kategorije proizvoda s digitalnim elementima, skupina za ADCO može izdati preporuke tijelima za nadzor tržišta da svoje aktivnosti usmjere na takve kategorije proizvoda s digitalnim elementima.

Članak 53.

Pristup podacima i dokumentaciji

Ako je to potrebno radi ocjenjivanja sukladnosti proizvoda s digitalnim elementima i procesa koje su njihovi proizvođači uspostavili s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I., tijelima za nadzor tržišta, na obrazložen zahtjev, dopušta se pristup podacima potrebnima za ocjenjivanje projektiranja, razvoja i proizvodnje takvih proizvoda te postupanja s njihovim ranjivostima, uključujući povezanu internu dokumentaciju relevantnog gospodarskog subjekta, na jeziku koje ta tijela razumiju bez poteškoća.

Članak 54.

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

1. Ako tijelo za nadzor tržišta države članice ima dovoljno razloga smatrati da proizvod s digitalnim elementima, uključujući njegovo postupanje s ranjivostima, predstavlja znatan kibernetički sigurnosni rizik, ono bez nepotrebne odgode i prema potrebi u suradnji s relevantnim CSIRT-om provodi evaluaciju tog proizvoda s digitalnim elementima koja se odnosi na njegovu usklađenost sa svim zahtjevima utvrđenima u ovoj Uredbi. Relevantni gospodarski subjekti prema potrebi surađuju s tijelom za nadzor tržišta.

Ako tijelo za nadzor tržišta tijekom te evaluacije utvrdi da proizvod s digitalnim elementima nije sukladan sa zahtjevima utvrđenima u ovoj Uredbi, ono od relevantnog gospodarskog subjekta zahtijeva da bez odgode poduzme sve odgovarajuće korektivne mjere kako bi se proizvod s digitalnim elementima uskladio s tim zahtjevima, povukao s tržišta ili opozvao u razumnom roku, razmjerno vrsti kibernetičkog sigurnosnog rizika i ovisno o tome što propiše tijelo za nadzor tržišta.

Tijelo za nadzor tržišta o tome na odgovarajući način obavješćuje relevantno prijavljeno tijelo. Članak 18. Uredbe (EU) 2019/1020 primjenjuje se na korektivne mjere.

2. Pri utvrđivanju znatnosti kibernetičkog sigurnosnog rizika iz stavka 1. ovog članka tijela za nadzor tržišta također razmatraju netehničke čimbenike rizika, posebno one utvrđene na temelju koordiniranih procjena sigurnosnih rizika ključnih lanaca opskrbe na razini Unije provedenih u skladu s člankom 22. Direktive (EU) 2022/2555. Ako tijelo za nadzor tržišta ima dovoljno razloga smatrati da proizvod s digitalnim elementima predstavlja znatan kibernetički sigurnosni rizik s obzirom na netehničke čimbenike rizika, ono o tome obavješćuje nadležna tijela imenovana ili uspostavljena u skladu s člankom 8. Direktive (EU) 2022/2555 i prema potrebi surađuje s tim tijelima.

3. Ako tijelo za nadzor tržišta smatra da neusklađenost nije ograničena samo na državno područje njegove države, ono obavješćuje Komisiju i ostale države članice o rezultatima evaluacije i mjerama za koje je zahtijevalo da ih gospodarski subjekt poduzme.

4. Gospodarski subjekt osigurava da se poduzmu sve odgovarajuće korektivne mjere u pogledu svih predmetnih proizvoda s digitalnim elementima koje je stavio na raspolaganje na tržištu u Uniji.

5. Ako gospodarski subjekt 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 s digitalnim elementima, povuklo ga s tržišta ili ga opozvalo.

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

6. Informacije iz stavka 5. uključuju sve dostupne pojedinosti, posebno podatke potrebne za identifikaciju neusklađenog proizvoda s digitalnim elementima, podrijetlo tog proizvoda s digitalnim elementima, vrstu navodne neusklađenosti i povezanog rizika, prirodu i trajanje poduzetih nacionalnih mjera te argumente koje je iznio relevantni gospodarski subjekt. Tijelo za nadzor tržišta posebno navodi je li neusklađenost uzrokovana nečim od sljedećeg:

(a) proizvod s digitalnim elementima ili procesi koje je proizvođač uspostavio ne ispunjavaju bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u Prilogu I.;

(b) nedostaci usklađenih normi, europskih programa kibernetičke sigurnosne certifikacije ili zajedničkih specifikacija iz članka 27.

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

8. Ako u roku od tri mjeseca od primitka obavijesti navedene u stavku 5. ovog članka nijedna država članica ni Komisija ne podnesu prigovor na privremenu mjeru koju je poduzela država članica, ta mjera se smatra opravdanom. Time se ne dovode u pitanje postupovna prava predmetnog gospodarskog subjekta u skladu s člankom 18. Uredbe (EU) 2019/1020.

9. Tijela za nadzor tržišta svih država članica osiguravaju da se bez odgode poduzmu odgovarajuće restriktivne mjere u pogledu predmetnog proizvoda s digitalnim elementima, primjerice povlačenje tog proizvoda s njihovih tržišta.

Članak 55.

Zaštitni postupak Unije

1. Ako država članica u roku od tri mjeseca od primitka obavijesti iz članka 54. stavka 5. podnese prigovor na mjeru koju je poduzela druga država članica ili ako Komisija smatra da je mjera protivna pravu 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 54. stavka 5. 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 neusklađenog proizvoda s digitalnim elementima s njihova tržišta te o tome obavješćuju Komisiju. Ako se nacionalna mjera ne smatra opravdanom, predmetna država članica povlači mjeru.

3. Ako se nacionalna mjera smatra opravdanom i ako se neusklađenost proizvoda s digitalnim elementima pripisuje nedostacima u usklađenim normama, Komisija primjenjuje postupak iz članka 11. Uredbe (EU) br. 1025/2012.

4. Ako se nacionalna mjera smatra opravdanom i ako se neusklađenost proizvoda s digitalnim elementima pripisuje nedostacima u europskom programu kibernetičke sigurnosne certifikacije iz članka 27., Komisija razmatra izmjenu ili stavljanje izvan snage svakog delegiranog akta donesenog na temelju članka 27. stavka 9. kojim se utvrđuje pretpostavka sukladnosti koja se odnosi na taj program certifikacije.

5. Ako se nacionalna mjera smatra opravdanom i ako se neusklađenost proizvoda s digitalnim elementima pripisuje nedostacima u zajedničkim specifikacijama iz članka 27., Komisija razmatra izmjenu ili stavljanje izvan snage svakog provedbenog akta donesenog na temelju članka 27. stavka 2. kojim su te zajedničke specifikacije utvrđene.

Članak 56.

Postupak na razini Unije za proizvode s digitalnim elementima koji predstavljaju znatan kibernetički sigurnosni 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 kibernetički sigurnosni rizik nije usklađen sa zahtjevima utvrđenima u ovoj Uredbi, ona obavješćuje relevantna tijela za nadzor tržišta. Ako tijela za nadzor tržišta provode evaluaciju tog proizvoda s digitalnim elementima koji može predstavljati znatan kibernetički sigurnosni rizik u pogledu njegove usklađenosti sa zahtjevima utvrđenima u ovoj Uredbi, primjenjuju se postupci iz članaka 54. i 55.

2. Ako Komisija ima dovoljno razloga smatrati da proizvod s digitalnim elementima predstavlja znatan kibernetički sigurnosni rizik s obzirom na netehničke čimbenike rizika, ona obavješćuje relevantna tijela za nadzor tržišta i, prema potrebi, nadležna tijela imenovana ili uspostavljena u skladu s člankom 8. Direktive (EU) 2022/2555 te prema potrebi surađuje s tim tijelima. Komisija također razmatra relevantnost utvrđenih rizika za taj proizvod s digitalnim elementima u kontekstu svojih zadaća povezanih s koordiniranim procjenama sigurnosnih rizika ključnih lanaca opskrbe na razini Unije iz članka 22. Direktive (EU) 2022/2555 te se prema potrebi savjetuje sa skupinom za suradnju osnovanom na temelju članka 14. Direktive (EU) 2022/2555 i s ENISA-om.

3. U okolnostima koje opravdavaju brzu intervenciju radi očuvanja pravilnog funkcioniranja unutarnjeg tržišta i ako Komisija ima dovoljno razloga smatrati da proizvod s digitalnim elementima iz stavka 1. i dalje nije usklađen sa zahtjevima utvrđenima u ovoj Uredbi, a nadležna tijela za nadzor tržišta nisu poduzela nikakve djelotvorne mjere, Komisija provodi evaluaciju usklađenosti i može zahtijevati od ENISA-e da dostavi analizu kojom bi je potkrijepila. Komisija o tome na odgovarajući način obavješćuje relevantna tijela za nadzor tržišta. Relevantni gospodarski subjekti prema potrebi surađuju s ENISA-om.

4. Na temelju evaluacije iz stavka 3. 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 subjektima.

5. Na temelju savjetovanja iz stavka 4. ovog članka Komisija može donijeti provedbene akte kako bi se predvidjele korektivne ili restriktivne mjere na razini Unije, uključujući zahtijevanje povlačenja predmetnih proizvoda s digitalnim elementima s tržišta ili njihova opoziva u razumnom roku, razmjerno vrsti rizika. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 62. stavka 2.

6. Komisija o provedbenim aktima iz stavka 5. odmah obavješćuje relevantne gospodarske subjekte. Države članice bez odgode provode te provedbene akte i o tome obavješćuju Komisiju.

7. Stavci od 3. do 6. primjenjivi su dok traje iznimna situacija koja opravdava intervenciju Komisije, pod uvjetom da nije uspostavljena usklađenost predmetnog proizvoda s digitalnim elementima s ovom Uredbom.

Članak 57.

Usklađeni proizvodi s digitalnim elementima koji predstavljaju znatan kibernetički sigurnosni rizik

1. Tijelo za nadzor tržišta države članice zahtijeva od gospodarskog subjekta da poduzme sve odgovarajuće mjere ako nakon evaluacije provedene u skladu s člankom 54. utvrdi da proizvod s digitalnim elementima i procesi koje je proizvođač uspostavio, iako su u skladu s ovom Uredbom, predstavljaju znatan kibernetički sigurnosni rizik za:

(a) zdravlje ili sigurnost osoba;

(b) ispunjavanje obveza na temelju prava Unije ili nacionalnog prava čija je svrha zaštita temeljnih prava;

(c) dostupnost, autentičnost, cjelovitost ili povjerljivost usluga koje ključni subjekti kako su navedeni u članku 3. stavku 1. Direktive (EU) 2022/2555 nude u okviru elektroničkog informacijskog sustava; ili

(d) druge aspekte zaštite javnog interesa.

Mjere iz prvog podstavka mogu uključivati mjere kojima se osigurava da predmetni proizvod s digitalnim elementima i procesi koje je proizvođač uspostavio više ne predstavljaju relevantne rizike pri stavljaju na raspolaganje na tržištu kao i povlačenje s tržišta predmetnog proizvoda s digitalnim elementima ili njegov opoziv te su razmjerne prirodi tih rizika.

2. Proizvođač ili drugi relevantni gospodarski 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 ostale države članice o mjerama poduzetima u skladu sa stavkom 1. Ta obavijest uključuje sve dostupne pojedinosti, osobito podatke potrebne za identifikaciju 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, ako je to potrebno, predlaže odgovarajuće mjere.

5. Komisija odluku iz stavka 4. 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 je u skladu s ovom Uredbom, predstavlja rizike iz stavka 1. ovog članka, ona obavješćuje relevantna tijela za nadzor tržišta i može od njih zahtijevati da provedu evaluaciju i primijene postupke iz članka 54. i stavaka 1., 2. i 3. ovog članka.

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

8. Na temelju 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 gospodarskim subjektima.

9. Na temelju savjetovanja iz stavka 8. ovog članka Komisija može donijeti provedbene akte kako bi se odlučilo o korektivnim ili restriktivnim mjerama na razini Unije, uključujući zahtijevanje povlačenja predmetnih proizvoda s digitalnim elementima s tržišta ili njihova opoziva u razumnom roku, razmjerno vrsti rizika. Ti se provedbeni akti donose u skladu s postupkom ispitivanja iz članka 62. stavka 2.

10. Komisija o provedbenim aktima iz stavka 9. odmah obavješćuje relevantne gospodarske subjekte. Države članice bez odgode provode te provedbene 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 s digitalnim elementima predstavlja rizike iz stavka 1.

Članak 58.

Formalna neusklađenost

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

(a) oznaka CE stavljena je tako da se krše članci 29. i 30.;

(b) oznaka CE 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 neusklađenost 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 59.

Zajedničke aktivnosti tijelâ za nadzor tržišta

1. Tijela za nadzor tržišta mogu s drugim relevantnim tijelima dogovoriti provedbu zajedničkih aktivnosti za kibernetičku sigurnost i zaštitu potrošača u pogledu određenih proizvoda s digitalnim elementima koji se stavljaju na tržište ili na raspolaganje na tržištu, posebno proizvoda s digitalnim elementima za koje se često ustanovi da predstavljaju kibernetičke sigurnosne rizike.

2. Komisija ili ENISA predlažu zajedničke aktivnosti za provjeru usklađenosti s ovom Uredbom koje će provesti tijela za nadzor tržišta na temelju naznaka ili informacija o tome da u nekoliko država članica postoji potencijalna neusklađenost proizvoda s digitalnim elementima obuhvaćenih područjem primjene ove Uredbe sa zahtjevima utvrđenim u ovoj Uredbi.

3. Tijela za nadzor tržišta i, ako je primjenjivo, Komisija 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 dobivene kao rezultat zajedničkih aktivnosti u okviru bilo koje istrage koju provodi.

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

Članak 60.

Opsežne provjere

1. Tijela za nadzor tržišta provode istodobne koordinirane kontrolne mjere („opsežne provjere”) nad određenim proizvodima s digitalnim elementima ili kategorijama takvih proizvoda radi provjere sukladnosti s ovom Uredbom ili otkrivanja njezina kršenja. Te opsežne provjere mogu uključivati inspekcijske preglede proizvoda s digitalnim elementima kupljenih pod prikrivenim identitetom.

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

3. Ako pri obavljanju svojih zadaća, među ostalim na temelju obavijesti primljenih u skladu s člankom 14. stavcima 1. i 3., ENISA utvrdi kategorije proizvoda s digitalnim elementima za koje se mogu organizirati opsežne provjere, ona podnosi prijedlog za opsežnu provjeru koordinatoru iz stavka 2. ovog članka 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 52. do 58. 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.

DELEGIRANE OVLASTI I POSTUPAK ODBORA

Članak 61.

Izvršavanje delegiranja ovlasti

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

2. Ovlast za donošenje delegiranih akata iz članka 2. stavka 5. drugog podstavka, članka 7. stavka 3. članka 8. stavaka 1. i 2., članka 13. stavka 8. četvrtog podstavka, članka 14. stavka 9., članka 25., članka 27. stavka 9., članka 28. stavka 5. i članka 31. stavka 5. dodjeljuje se Komisiji na razdoblje od pet godina počevši od 10. prosinca 2024. Komisija izrađuje izvješće o delegiranju ovlasti najkasnije devet mjeseci prije kraja razdoblja od pet godina. Delegiranje ovlasti prešutno se produljuje za razdoblja jednakog trajanja, osim ako se Europski parlament ili Vijeće tom produljenju usprotive najkasnije tri mjeseca prije kraja svakog razdoblja.

3. Europski parlament ili Vijeće u svakom trenutku mogu opozvati delegiranje ovlasti iz članka 2. stavka 5. drugog podstavka, članka 7. stavka 3., članka 8. stavaka 1. i 2., članka 13. stavka 8. četvrtog podstavka, članka 14. stavka 9., članka 25., članka 27. stavka 9., članka 28. stavka 5. i članka 31. 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 5. drugog podstavka, članka 7. stavka 3., članka 8. stavka 1. ili 2., članka 13. stavka 8. četvrtog podstavka, članka 14. stavka 9., članka 25., članka 27. stavka 9., članka 28. stavka 5. ili članka 31. 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 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 62.

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

POGLAVLJE VII.

POVJERLJIVOST I SANKCIJE

Članak 63.

Povjerljivost

1. Sve strane uključene u primjenu ove Uredbe poštuju 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 ([37]);

(b) djelotvorna 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 dotičnih 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 64.

Sankcije

1. Države članice utvrđuju pravila o sankcijama koje se primjenjuju na kršenja ove Uredbe i poduzimaju sve potrebne mjere radi osiguranja njihove provedbe. Predviđene sankcije moraju biti učinkovite, proporcionalne i odvraćajuće. Države članice bez odgode obavješćuju Komisiju o tim pravilima i mjerama te je bez odgode obavješćuju o svim naknadnim izmjenama koje na njih utječu.

2. Za neusklađenost s bitnim sigurnosnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. i obvezama utvrđenima u člancima 13. i 14. 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.

3. Za neusklađenost s obvezama utvrđenima u člancima od 18. do 23., članku 28., članku 30. stavcima od 1. do 4., članku 31. stavcima od 1. do 4., članku 32. stavcima 1., 2. i 3., članku 33. stavku 5. i člancima 39., 41., 47., 49. i 53. 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.

4. 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.

([37]) 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.).

5. 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 kršenja te njegovim posljedicama;

(b) eventualnim upravnim novčanim kaznama koje su ista ili druga tijela za nadzor tržišta već izrekla istom gospodarskom subjektu za slično kršenje;

(c) veličini, posebno kad je riječ o mikropoduzećima, malim i srednjim poduzećima, uključujući novoosnovana poduzeća, i tržišnom udjelu gospodarskog subjekta koji je počinio kršenje.

6. Tijela za nadzor tržišta koja izriču upravne novčane kazne o tome obavješćuju tijela za nadzor tržišta drugih država članica u okviru informacijskog i komunikacijskog sustava iz članka 34. Uredbe (EU) 2019/1020.

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

8. 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.

9. 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 isto kršenje.

10. Odstupajući od stavaka od 3. do 9., upravne novčane kazne iz tih stavaka ne primjenjuju se na sljedeće:

(a) proizvođače koji se smatraju mikropoduzećima ili malim poduzećima kad je riječ o nepoštovanju roka iz članka 14. stavka 2. točke (a) ili članka 14. stavka 4. točke (a);

(b) svako kršenje ove Uredbe od strane upraviteljâ softvera otvorenog koda.

Članak 65.

Predstavničke tužbe

Direktiva (EU) 2020/1828 primjenjuje se na predstavničke tužbe podnesene protiv povreda odredaba ove Uredbe od strane gospodarskih subjekata koje štete ili mogu naštetiti kolektivnim interesima potrošača.

POGLAVLJE VIII.

PRIJELAZNE I ZAVRŠNE ODREDBE

Članak 66.

Izmjena Uredbe (EU) 2019/1020

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

„72. Uredba (EU) 2024/2847 Europskog parlamenta i Vijeća (*).

(*) Uredba (EU) 2024/2847 Europskog parlamenta i Vijeća od 23. listopada 2024. o horizontalnim zahtjevima u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima i o izmjeni uredbi (EU) br. 168/2013 i (EU) 2019/1020 te Direktive (EU) 2020/1828 (Akt o kibernetičkoj otpornosti) (SL L, 2024/2847, 20.11.2024., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).”.

Članak 67.

Izmjena Direktive (EU) 2020/1828

U Prilogu I. Direktivi (EU) 2020/1828 dodaje se sljedeća točka:

„69. Uredba (EU) 2024/2847 Europskog parlamenta i Vijeća (*).

(*) Uredba (EU) 2024/2847 Europskog parlamenta i Vijeća od 23. listopada 2024. o horizontalnim zahtjevima u pogledu kibernetičke sigurnosti za proizvode s digitalnim elementima i o izmjeni uredbi (EU) br. 168/2013 i (EU) 2019/1020 te Direktive (EU) 2020/1828 (Akt o kibernetičkoj otpornosti) (SL L, 2024/2847, 20.11.2024., ELI: http://data.europa.eu/eli/reg/2024/2847/oj).".

Članak 68.

Izmjena Uredbe (EU) br. 168/2013

U tablici u dijelu C.1 Priloga II. Uredbi (EU) br. 168/2013 Europskog parlamenta i Vijeća ([38]) dodaje se sljedeći unos:

„

16	18	zaštita vozila od kibernetičkih napada		x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

"

Članak 69.

Prijelazne odredbe

1. Potvrde o EU ispitivanju tipa i odluke o odobrenju izdane u vezi s kibernetičkim sigurnosnim zahtjevima u pogledu proizvoda s digitalnim elementima koji podliježu zakonodavstvu Unije o usklađivanju koje nije ova Uredbe ostaju valjane do 11. lipnja 2028., osim ako isteknu prije tog datuma ili ako je drukčije utvrđeno u tom drugom zakonodavstvu Unije o usklađivanju, u kojem slučaju ostaju valjane onoliko koliko je navedeno u tom zakonodavstvu.

2. Proizvodi s digitalnim elementima koji su stavljeni na tržište prije 11. prosinca 2027. podliježu zahtjevima utvrđenima u ovoj Uredbi samo ako od tog datuma dođe do bitne izmjene proizvoda.

3. Odstupajući od stavka 2. ovog članka, obveze utvrđene u članku 14. primjenjuju se na sve proizvode s digitalnim elementima obuhvaćene područjem primjene ove Uredbe koji su stavljeni na tržište prije 11. prosinca 2027.

Članak 70.

Evaluacija i preispitivanje

1. Do 11. prosinca 2030. i svake četiri godine nakon toga Komisija Europskom parlamentu i Vijeću podnosi izvješće o evaluaciji i preispitivanju ove Uredbe. Ta se izvješća objavljuju.

2. Do 11. rujna 2028. Komisija, nakon savjetovanja s ENISA-om i mrežom CSIRT-ova, podnosi izvješće Europskom parlamentu i Vijeću u kojem ocjenjuje djelotvornost jedinstvene platforme za izvješćivanje iz članka 16. i učinak primjene razloga povezanih s kibernetičkom sigurnošću iz članka 16. stavka 2. od strane CSIRT-ova koji su imenovani koordinatorima na djelotvornost jedinstvene platforme za izvješćivanje u pogledu pravodobnog slanja primljenih obavijesti drugim relevantnim CSIRT-ovima.

Članak 71.

Stupanje na snagu i primjena

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

([38]) Uredba (EU) br. 168/2013 Europskog parlamenta i Vijeća od 15. siječnja 2013. o homologaciji i nadzoru tržišta vozila na dva ili tri kotača i četverocikala (SL L 60, 2.3.2013., str. 52.).

2. Ova Uredba primjenjuje se od 11. prosinca 2027.

Međutim, članak 14. primjenjuje se od 11. rujna 2026., dok se poglavlje IV. (članci od 35. do 51.) primjenjuje od 11. lipnja 2026.

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

Sastavljeno u Strasbourgu 23. listopada 2024.

Za Europski parlament	*Za Vijeće*
Predsjednica	*Predsjednik*
R. METSOLA	ZSIGMOND B. P.

PRILOG I.

BITNI ZAHTJEVI U POGLEDU KIBERNETIČKE SIGURNOSTI

Dio I. Kibernetički sigurnosni zahtjevi koji se odnose na svojstva proizvoda s digitalnim elementima

1. Proizvodi s digitalnim elementima projektiraju se, razvijaju i proizvode tako da osiguravaju odgovarajuću razinu kibernetičke sigurnosti na temelju rizika.

2. Na temelju procjene kibernetičkog sigurnosnog rizika iz članka 13. stavka 2. i ako je primjenjivo, proizvodi s digitalnim elementima,:

   (a) stavljaju se na raspolaganje na tržištu bez poznatih iskoristivih ranjivosti;

   (b) stavljaju se na raspolaganje na tržištu u zadanoj sigurnoj konfiguraciji, osim ako se proizvođač i poslovni korisnik dogovore drukčije u vezi s prilagođenim proizvodom s digitalnim elementima, što uključuje mogućnost vraćanja proizvoda u izvorno stanje;

   (c) osiguravaju da se na ranjivosti može odgovoriti sigurnosnim ažuriranjima, među ostalim, ako je primjenjivo, automatskim sigurnosnim ažuriranjima koja se instaliraju u odgovarajućem vremenskom okviru i koja su omogućena kao zadana postavka, s jasnim i jednostavnim mehanizmom izuzeća, obavješćivanjem korisnika o dostupnim ažuriranjima i uz mogućnost njihove privremene odgode;

   (d) osiguravaju zaštitu od neovlaštenog pristupa u obliku odgovarajućih kontrolnih mehanizama, među kojima su sustavi za upravljanje autentifikacijom, identitetima odnosno pristupom te izvješćuju o mogućem neovlaštenom pristupu;

   (e) štite povjerljivost pohranjenih, prenesenih ili drukčije obrađenih podataka, osobnih ili drugih, primjerice šifriranjem relevantnih podataka u mirovanju ili tijekom prijenosa s pomoću najsuvremenijih mehanizama i korištenjem drugim tehničkim sredstvima;

   (f) štite cjelovitost pohranjenih, prenesenih ili na drukčije obrađenih podataka, osobnih ili drugih, naredbi, programa i konfiguracije od bilo kakve manipulacije ili izmjene koju korisnik nije odobrio te prijavljivati narušavanja te cjelovitosti;

   (g) obrađuju isključivo podatke, osobne ili druge, koji su primjereni, relevantni i ograničeni na ono što je potrebno za namjenu proizvoda s digitalnim elementima („minimizacija podataka”);

   (h) štite dostupnost osnovnih i glavnih funkcija i nakon incidenta, među ostalim s pomoću mjera otpornosti i ublažavanja u odnosu na distribuirane napade uskraćivanjem usluge;

   i. na najmanju moguću mjeru svode negativan utjecaj samih proizvoda ili povezanih uređaja na dostupnost usluga koje pružaju drugi uređaji ili mreže;

   (j) projektiraju se, razvijaju i proizvede tako da ograničavaju površine napada, što uključuje vanjska sučelja;

   (k) projektiraju se, razvijaju i proizvede tako da ublažavaju posljedice incidenta primjenom odgovarajućih mehanizama i tehnika za ublažavanje iskorištavanja;

   (l) pružaju informacije o sigurnosti na temelju bilježenja i praćenja bitnih unutarnjih aktivnosti, među kojima su pristupanje podacima, uslugama ili funkcijama ili njihova izmjena, uz mehanizam za dobrovoljni izlazak iz sustava za korisnika;

   (m) omogućuju korisnicima da na siguran i jednostavan način trajno uklone sve podatke i postavke te da, ako se takvi podaci mogu prenijeti u druge proizvode ili sustave, osiguraju da se to čini na siguran način.

Dio II. Zahtjevi u pogledu postupanja s ranjivostima

Proizvođači proizvoda s digitalnim elementima:

1. definiraju i dokumentiraju ranjivosti i komponente proizvoda s digitalnim elementima, među ostalim sastavljanjem popisa softverskog materijala u uobičajenom, strojno čitljivom formatu koji obuhvaća barem ovisnosti proizvoda na najvišoj razini;

2. kad je riječ o rizicima za proizvode s digitalnim elementima, bez odgode razmatra i otklanja ranjivosti, među ostalim sigurnosnim ažuriranjima; ako je to tehnički izvedivo, nova sigurnosna ažuriranja pružaju se odvojeno od ažuriranja funkcionalnosti;

3. provode djelotvorna i redovita ispitivanja i preispitivanja sigurnosti proizvoda s digitalnim elementima;

4. dijele i javno objavljuju informacije o popravljenim ranjivostima nakon izdavanja sigurnosnog ažuriranja, koje uključuju opis ranjivosti, informacije koje korisnicima omogućuju identifikaciju zahvaćenih proizvoda s digitalnim elementima, posljedice ranjivosti, njihovu težinu i jasne i dostupne informacije koje korisnicima pomažu otkloniti te ranjivosti; u opravdanim slučajevima, ako proizvođači smatraju da sigurnosni rizici od objave nadmašuju sigurnosne koristi, mogu odgoditi objavljivanje informacija o popravljenoj ranjivosti dok se korisnicima ne omogući primjena relevantne zakrpe;

5. uspostavljaju i provode politiku koordiniranog otkrivanja ranjivosti;

6. poduzimaju mjere za lakšu razmjenu informacija o potencijalnim ranjivostima svojeg proizvoda s digitalnim elementima i komponenata treće strane u tom proizvodu, među ostalim tako što daju adresu za kontakt za prijavljivanje ranjivosti otkrivenih u proizvodu s digitalnim elementima;

7. pružaju mehanizme za sigurnu distribuciju ažuriranja za proizvode s digitalnim elementima kako bi se ranjivosti pravodobno i, ako je primjenjivo, za sigurnosna ažuriranja i automatski, popravile ili smanjile;

8. osiguravaju da se sigurnosna ažuriranja za otklanjanje utvrđenih sigurnosnih problema, ako su dostupna, distribuiraju bez odgode, osim ako se proizvođač i poslovni korisnik dogovore drukčije u vezi s prilagođenim proizvodom s digitalnim elementima, besplatno i zajedno s upozorenjima za korisnike s bitnim informacijama, među ostalim o mogućim mjerama koje treba poduzeti.

PRILOG II.

INFORMACIJE I UPUTE ZA KORISNIKA

Uz proizvod s digitalnim elementima daju se barem sljedeće informacije:

1. ime, registrirano trgovačko ime ili registrirani žig proizvođača, poštanska adresa, e-adresa ili drugi digitalni kontakt te, ako je dostupna, internetska stranica na kojoj se može stupiti u kontakt s proizvođačem;
2. jedinstvena kontaktna točka gdje se mogu dojaviti i dobiti informacije o ranjivostima proizvoda s digitalnim elementima te pronaći politika proizvođača u vezi s koordiniranim otkrivanjem ranjivosti;
3. naziv i vrsta proizvoda s digitalnim elementima te svi dodatni podaci na temelju kojih ga je moguće jedinstveno identificirati;
4. namjena proizvoda s digitalnim elementima, uključujući sigurnosno okruženje kako ga je uspostavio proizvođač, te bitne funkcionalnosti proizvoda i informacije o sigurnosnim svojstvima;
5. sve poznate i predvidljive okolnosti povezane s upotrebom proizvoda s digitalnim elementima u skladu s njegovom namjenom ili u uvjetima razumno predvidljive krive upotrebe zbog kojih mogu nastati znatni kibernetički sigurnosni rizici;
6. ako je primjenjivo, internetska adresa na kojoj se može pristupiti EU izjavi o sukladnosti;
7. vrsta tehničke sigurnosne podrške koju nudi proizvođač i datum završetka razdoblja potpore tijekom kojeg korisnici mogu očekivati postupanje s ranjivostima i sigurnosna ažuriranja;
8. detaljne upute ili internetska adresa za takve detaljne upute i informacije o:
   (a) potrebnim mjerama za sigurnu upotrebu proizvoda s digitalnim elementima tijekom njegova stavljanja u upotrebu i cijelog životnog vijeka;
   (b) mogućem utjecaju promjena proizvoda s digitalnim elementima na sigurnost podataka;
   (c) načinu instaliranja ažuriranja važnih za sigurnost;
   (d) sigurnom stavljanju proizvoda s digitalnim elementima izvan upotrebe, uključujući informacije o sigurnom uklanjanju korisničkih podataka;
   (e) pitanju kako se može isključiti zadana postavka koja omogućuje automatsku ugradnju sigurnosnih ažuriranja, kako se zahtijeva u dijelu I. točki 2. podtočki (c) Priloga I.;
   (f) ako je proizvod s digitalnim elementima namijenjen za integraciju u druge proizvode s digitalnim elementima, informacije potrebne kako bi se integrator uskladio s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. i zahtjevima u pogledu dokumentacije utvrđenima u Prilogu VII.
9. Ako proizvođač odluči korisniku staviti na raspolaganje popis softverskog materijala, informacije o tome gdje se može pristupiti popisu softverskog materijala.

PRILOG III.

VAŽNI PROIZVODI S DIGITALNIM ELEMENTIMA

I. razred

1. Sustavi za upravljanje identitetom te softver i hardver za upravljanje povlaštenim pristupom, uključujući čitače za provjeru autentičnosti i kontrolu pristupa, uključujući biometrijske čitače
2. Samostalni i ugrađeni preglednici
3. Upravitelji lozinki
4. Softver za traženje, uklanjanje ili izoliranje zlonamjernog softvera
5. Proizvodi s digitalnim elementima s funkcijom virtualne privatne mreže (VPN)
6. Sustavi za upravljanje mrežom
7. Sustavi za upravljanje sigurnosnim informacijama i događajima (SIEM)
8. Upravitelji pokretanja sustava
9. Infrastruktura javnih ključeva i softver za izdavanje digitalnih certifikata
10. Fizička i virtualna mrežna sučelja
11. Operativni sustavi
12. Ruteri, modemi namijenjeni za spajanje na internet i preklopnici
13. Mikroprocesori s funkcijama povezanima sa sigurnošću
14. Mikrokontroleri s funkcijama povezanima sa sigurnošću
15. Integrirani krugovi specijalizirane namjene (ASIC) i programirljivi logički sklopovi (FPGA) s funkcijama povezanima sa sigurnošću
16. Virtualni asistenti opće namjene za pametne kuće
17. Proizvodi za pametne kuće sa sigurnosnim funkcijama, uključujući pametne brave za vrata, sigurnosne kamere, sustave za nadzor male djece i alarmne sustave
18. Igračke povezane s internetom obuhvaćene Direktivom 2009/48/EZ Europskog parlamenta i Vijeća [1] koje imaju društvene interaktivne značajke (npr. govor ili snimanje) ili imaju značajke praćenja lokacije
19. Osobni nosivi proizvodi koje treba nositi ili staviti na ljudsko tijelo i koji imaju svrhu praćenja zdravlja (kao što je praćenje) i na koje se ne primjenjuju Uredba (EU) 2017/745 ili Uredba (EU) 2017/746 ili osobni nosivi proizvodi koji su namijenjeni za upotrebu od strane djece ili za djecu

II. razred

1. Hipervizori i sustavi za izolirano izvršavanje koji omogućuju virtualizirano izvršavanje operativnih sustava i slična okruženja
2. Vatrozidovi, sustavi za otkrivanje i sprečavanje neovlaštenih upada
3. Mikroprocesori otporni na manipuliranje
4. Mikrokontroleri otporni na manipuliranje

[1] Direktiva 2009/48/EZ Europskog parlamenta i Vijeća od 18. lipnja 2009. o sigurnosti igračaka (SL L 170, 30.6.2009., str. 1.).

PRILOG IV.

KRITIČNI PROIZVODI S DIGITALNIM ELEMENTIMA

1. Hardverski uređaji sa sigurnosnim kutijama
2. Pristupnici pametnih brojila u okviru pametnih sustava mjerenja kako su definirani u članku 2. točki 23. Direktive (EU) 2019/944 Europskog parlamenta i Vijeća ([1]) i drugi uređaji za napredne sigurnosne svrhe, među ostalim za sigurnu kriptoobradu
3. Pametne kartice ili slični uređaji, uključujući sigurne elemente

([1]) Direktiva (EU) 2019/944 Europskog parlamenta i Vijeća od 5. lipnja 2019. o zajedničkim pravilima za unutarnje tržište električne energije i izmjeni Direktive 2012/27/EU (SL L 158, 14.6.2019., str. 125.).

PRILOG V.

EU IZJAVA O SUKLADNOSTI

EU izjava o sukladnosti iz članka 28. sadržava sve sljedeće podatke:

1. naziv i vrstu proizvoda s digitalnim elementima te sve dodatne podatke na temelju kojih ga je moguće jedinstveno identificirati
2. ime i adresu proizvođača ili njegova ovlaštenog zastupnika
3. izjavu da je za izdavanje EU izjave o sukladnosti odgovoran isključivo dobavljač
4. predmet izjave (identifikacijski podaci proizvoda s digitalnim elementima koji omogućuju sljedivost, što prema potrebi može uključivati fotografiju)
5. izjavu da je opisani predmet izjave sukladan s relevantnim zakonodavstvom Unije o usklađivanju
6. upućivanje na sve relevantne primijenjene usklađene norme ili bilo koju drugu zajedničku specifikaciju ili kibernetičku sigurnosnu certifikaciju na temelju koje se izjavljuje sukladnost
7. ako je primjenjivo, ime i identifikacijski broj prijavljenog tijela, opis provedenog postupka ocjenjivanja sukladnosti te identifikacijsku oznaku izdane potvrde
8. dodatne informacije:

   Potpisano za i u ime:

   (mjesto i datum izdavanja):

   (ime, funkcija) (potpis):

PRILOG VI.

POJEDNOSTAVLJENA EU IZJAVA O SUKLADNOSTI

Pojednostavljena EU izjava o sukladnosti iz članka 13. stavka 20. sastavlja se kako slijedi:

[Ime proizvođača] … ovime izjavljuje da je vrsta proizvoda s digitalnim elementima … [oznaka vrste proizvoda s digitalnim elementom] u skladu s Uredbom (EU) 2024/2847 ([1]).

Cjeloviti tekst EU izjave o sukladnosti dostupan je na sljedećoj internetskoj adresi: …

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

PRILOG VII.

SADRŽAJ TEHNIČKE DOKUMENTACIJE

Tehnička dokumentacija iz članka 31. sadržava barem sljedeće informacije, ovisno o tome što je primjenjivo na određeni proizvod s digitalnim elementima:

1. opći opis proizvoda s digitalnim elementima, uključujući:
   (a) njegovu namjenu;
   (b) verzije softvera koje utječu na sukladnost s bitnim zahtjevima u pogledu kibernetičke sigurnosti;
   (c) ako je proizvod s digitalnim elementima hardverski proizvod, fotografije ili ilustracije koje prikazuju vanjska obilježja, oznake i unutarnji raspored;
   (d) informacije i upute za korisnike kako su utvrđene u Prilogu II.;
2. opis projektiranja, razvoja i proizvodnje proizvoda s digitalnim elementima te procese postupanja s ranjivostima, uključujući:
   (a) potrebne informacije o projektiranju i razvoju proizvoda s digitalnim elementima, uključujući, ako je primjenjivo, crteže i sheme i/ili opis arhitekture sustava iz kojih se vidjeti međuovisnost ili odnos softverskih komponenti i kako su integrirane u cjelokupnu obradu;
   (b) potrebne informacije i specifikacije procesa postupanja s ranjivostima koje je uveo proizvođač, uključujući popis softverskog materijala, politiku koordiniranog otkrivanja ranjivosti, dokaz o uspostavljanju adrese za kontakt za prijavljivanje ranjivosti te opis tehničkih rješenja odabranih za sigurnu distribuciju ažuriranja;
   (c) potrebne informacije i specifikacije koje se odnose na procese proizvodnje i praćenja proizvoda s digitalnim elementima i validaciju tih procesa;
3. procjenu kibernetičkih sigurnosnih rizika koji su uzeti u obzir pri projektiranju, razvoju, proizvodnji, isporuci i održavanju proizvoda s digitalnim elementima u skladu s člankom 13., uključujući način na koji se primjenjuju bitni zahtjevi u pogledu kibernetičke sigurnosti utvrđeni u dijelu I. Priloga I.;
4. relevantne informacije koje su uzete u obzir pri utvrđivanju razdoblja potpore u skladu s člankom 13. stavkom 8. za proizvod s digitalnim elementima;
5. popis u cijelosti ili djelomično primijenjenih usklađenih normi na koje su upućivanja objavljena u *Službenom listu Europske unije*, zajedničkih specifikacija kako su utvrđene u članku 27. ove Uredbe ili europskih programa kibernetičke sigurnosne certifikacije donesenih u skladu s Uredbom (EU) 2019/881 u skladu s člankom 27. stavkom 8. ove Uredbe, a ako te usklađene norme, zajedničke specifikacije ili europski programi kibernetičke sigurnosne certifikacije nisu primijenjene, opise rješenja koja su prihvaćena kako bi se ispunili bitni zahtjevi u pogledu kibernetičke sigurnosti utvrđeni u dijelovima I. i II. Priloga I., uključujući popis drugih primijenjenih relevantnih tehničkih specifikacija. Ako su usklađene norme, zajedničke specifikacije ili europski programi kibernetičke sigurnosne certifikacije primijenjeni djelomično, u tehničkoj dokumentaciji navode se dijelovi koji su primijenjeni;
6. izvješća o ispitivanjima provedenima radi provjere sukladnosti proizvoda s digitalnim elementima i procesa postupanja s ranjivostima s primjenjivim bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelovima I. i II. Priloga I.;
7. primjerak EU izjave o sukladnosti;
8. ako je primjenjivo, popis softverskog materijala na obrazložen zahtjev tijela za nadzor tržišta pod uvjetom da je to potrebno kako bi to tijelo moglo provjeriti usklađenost s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I.

PRILOG VIII.

POSTUPCI OCJENJIVANJA SUKLADNOSTI

Dio I. Postupak ocjenjivanja sukladnosti na temelju unutarnje kontrole (na temelju modula A)

1. Unutarnja kontrola je postupak ocjenjivanja sukladnosti kojim proizvođač ispunjava obveze utvrđene u točkama 2., 3. i 4. ovog dijela te osigurava i na vlastitu odgovornost izjavljuje da proizvodi s digitalnim elementima ispunjavaju sve bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu I. Priloga I. te da proizvođač ispunjava bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu II. Priloga I.

2. Proizvođač sastavlja tehničku dokumentaciju opisanu u Prilogu VII.

3. Projektiranje, razvoj, proizvodnja i postupanje s ranjivostima proizvoda s digitalnim elementima

   Proizvođač poduzima sve potrebne mjere kako bi se projektiranjem, razvojem, proizvodnjom i procesima postupanja s ranjivostima i njihovim praćenjem osiguralo da su proizvedeni ili razvijeni proizvodi s digitalnim elementima i procesi koje je uspostavio proizvođač usklađeni s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelovima I. i II. Priloga I.

4. Oznaka sukladnosti i izjava o sukladnosti

   4.1 Proizvođač stavlja oznaku CE na svaki pojedini proizvod s digitalnim elementima koji ispunjava primjenjive zahtjeve utvrđene u ovoj Uredbi.

   4.2 Proizvođač za svaki proizvod s digitalnim elementima sastavlja pisanu EU izjavu o sukladnosti u skladu s člankom 28. i drži je na raspolaganju nacionalnim tijelima zajedno s tehničkom dokumentacijom 10 godina od stavljanja proizvoda s digitalnim elementima na tržište ili tijekom razdoblja potpore, ovisno o tome što je dulje. U EU izjavi o sukladnosti identificira se proizvod s digitalnim elementima za koji je izjava sastavljena. Primjerak EU izjave o sukladnosti stavlja se na raspolaganje relevantnim tijelima na njihov zahtjev.

5. Ovlašteni zastupnici

   Obveze proizvođača iz točke 4. u njegovo ime i na njegovu odgovornost može ispuniti njegov ovlašteni zastupnik ako su relevantne obveze navedene u ovlaštenju.

Dio II. EU ispitivanje tipa (na temelju modula B)

1. EU ispitivanje tipa dio je postupka ocjenjivanja sukladnosti u kojem prijavljeno tijelo pregledava tehničko projektiranje i razvoj proizvoda s digitalnim elementima te procese postupanja s ranjivostima koje je uspostavio proizvođač te potvrđuje da proizvod s digitalnim elementima ispunjava bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu I. Priloga I. te da proizvođač ispunjava bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijela II. Priloga I.

2. EU ispitivanje tipa provodi se ocjenjivanjem prikladnosti tehničkog projektiranja i razvoja proizvoda s digitalnim elementima na temelju pregleda tehničke dokumentacije i popratnih dokaza iz točke 3. i pregleda uzoraka jednog ili više kritičnih dijelova predmetnog proizvoda (kombinacija proizvodnog tipa i projektnog tipa).

3. Proizvođač podnosi zahtjev za EU ispitivanje tipa jednom prijavljenom tijelu po vlastitom izboru.

   Zahtjev sadržava:

   3.1 ime i adresu proizvođača te, ako zahtjev podnosi njegov ovlašteni zastupnik, ime i adresu tog ovlaštenog zastupnika;

   3.2 pisanu izjavu da isti zahtjev nije podnesen nijednom drugom prijavljenom tijelu;

   3.3 tehničku dokumentaciju na temelju koje je moguće ocijeniti sukladnost proizvoda s digitalnim elementima s primjenjivim bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu I. Priloga I. i proizvođačeve procese postupanja s ranjivostima utvrđene u dijelu II. Priloga I. te koja uključuje odgovarajuću analizu i procjenu rizika. U tehničkoj dokumentaciji navode se primjenjivi zahtjevi te se ona, u mjeri u kojoj je to bitno za ocjenjivanje, odnosi na projektiranje, proizvodnju i rad proizvoda s digitalnim elementima. Tehnička dokumentacija mora sadržavati, kad je to primjenjivo, barem elemente utvrđene u Prilogu VII.;

3.4 popratne dokaze o prikladnosti tehničkih projektnih i razvojnih rješenja te procesa postupanja s ranjivostima. U tim se dokazima navode svi korišteni dokumenti, posebno ako relevantne usklađene norme ili tehničke specifikacije nisu primijenjene u cijelosti. Ti dokazi prema potrebi uključuju rezultate ispitivanja provedenih u odgovarajućem laboratoriju proizvođača ili nekom drugom laboratoriju koji vrši ispitivanja u njegovo ime i pod njegovom odgovornošću.

4. Prijavljeno tijelo:

4.1 pregledava tehničku dokumentaciju i popratne dokaze kako bi ocijenilo prikladnost tehničkog projektiranja i razvoja proizvoda s digitalnim elementima s obzirom na bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu I. Priloga I. te procesa postupanja s ranjivostima koje je uspostavio proizvođač s obzirom na bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu II. Priloga I.;

4.2 provjerava jesu li uzorci razvijeni ili proizvedeni sukladno s tehničkom dokumentacijom i utvrđuje elemente koji su projektirani i razvijeni u skladu s primjenjivim odredbama relevantnih usklađenih normi ili tehničkih specifikacija te elemente koji nisu projektirani i razvijeni u skladu s relevantnim odredbama tih normi;

4.3 ako je proizvođač za ispunjavanje zahtjeva utvrđenim u Prilogu I. odlučio primijeniti rješenja iz relevantnih usklađenih normi ili tehničkih specifikacija, provodi odgovarajuće preglede i ispitivanja, ili ih daje provesti, kako bi se provjerilo jesu li te norme i specifikacije pravilno primijenjene;

4.4 ako za ispunjavanje zahtjeva utvrđenih u Prilogu I. nisu primijenjena rješenja iz relevantnih usklađenih normi ili tehničkih specifikacija, provodi odgovarajuće preglede i ispitivanja, ili ih daje provesti, kako bi se provjerilo ispunjavaju li rješenja koja je primijenio proizvođač odgovarajuće bitne zahtjeve u pogledu kibernetičke sigurnosti;

4.5 dogovara s proizvođačem mjesto gdje će se provoditi pregledi i ispitivanja.

5. Prijavljeno tijelo sastavlja izvješće o ocjenjivanju u kojem bilježi mjere poduzete u skladu s točkom 4. i njihove rezultate. Ne dovodeći u pitanje njegove obveze prema tijelima koja provode prijavljivanje, prijavljeno tijelo objavljuje sadržaj tog izvješća, u cijelosti ili djelomično, isključivo uz suglasnost proizvođača.

6. Ako tip i procesi postupanja ranjivostima ispunjavaju bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u Prilogu I., prijavljeno tijelo proizvođaču izdaje potvrdu o EU ispitivanju tipa. Ta potvrda sadržava ime i adresu proizvođača, zaključke ispitivanja, uvjete (ako postoje) njezine valjanosti kao i podatke potrebne za identifikaciju odobrenog tipa i odobrenih procesa postupanja s ranjivostima. Potvrda može imati priloge.

Potvrda i njezini prilozi sadržavaju sve relevantne informacije na temelju kojih je moguće ocijeniti sukladnost proizvedenih ili razvijenih proizvoda s digitalnim elementima s ispitanim tipom i procesa postupanja s ranjivostima te provoditi kontrole u upotrebi.

Ako tip i procesi postupanja s ranjivostima ne ispunjavaju primjenjive bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u Prilogu I., prijavljeno tijelo odbija izdati potvrdu o EU ispitivanju tipa i o tome uz detaljno obrazloženje obavješćuje podnositelja zahtjeva.

7. Prijavljeno tijelo prati sve promjene u onom što se općenito smatra najsuvremenijom tehnologijom koje upućuju na to da odobreni tip i procesi postupanja s ranjivostima možda više ne ispunjavaju primjenjive bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u Prilogu I. te odlučuje zahtijevaju li takve promjene daljnje razmatranje. Ako je to slučaj, prijavljeno tijelo o tome obavješćuje proizvođača.

Proizvođač obavješćuje prijavljeno tijelo koje posjeduje tehničku dokumentaciju koja se odnosi na potvrdu o EU ispitivanju tipa o svim preinakama odobrenog tipa i procesima postupanja s ranjivostima koji mogu utjecati na sukladnost s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u Prilogu I. ili uvjetima valjanosti te potvrde. Za takve je izmjene potrebno dodatno odobrenje u obliku dopune izvornoj potvrdi o EU ispitivanju tipa.

8. Prijavljeno tijelo provodi periodične revizije kako bi osiguralo da se procesi postupanja s ranjivostima utvrđeni u dijelu II. Priloga I. provode na odgovarajući način.

9. Svako prijavljeno tijelo obavješćuje svoja tijela koja provode prijavljivanje o potvrdama o EU ispitivanju tipa i svim njihovim dopunama koje je izdalo ili povuklo i periodično ili na zahtjev svojim tijelima koja provode prijavljivanje stavlja na raspolaganje popis potvrda i svih njihovih dopuna koje je odbilo, suspendiralo ili na drugi način ograničilo.

   Svako prijavljeno tijelo obavješćuje druga prijavljena tijela o potvrdama o EU ispitivanju tipa i svim njihovim dopunama koje je odbilo, povuklo, suspendiralo ili na drugi način ograničilo, a na zahtjev i o potvrdama i njihovim dopunama koje je izdalo.

   Komisija, države članice i druga prijavljena tijela mogu na zahtjev dobiti primjerak potvrda o EU ispitivanju tipa i svih njihovih dopuna. Komisija i države članice mogu na zahtjev dobiti primjerak tehničke dokumentacije i rezultata pregleda koje je provelo prijavljeno tijelo. Prijavljeno tijelo drži primjerak potvrde o EU ispitivanju tipa te njezinih priloga i dopuna, kao i tehnički spis, uključujući dokumentaciju koju je dostavio proizvođač, do isteka valjanosti te potvrde.

10. Proizvođač drži na raspolaganju nacionalnim tijelima primjerak potvrde o EU ispitivanju tipa te njezinih priloga i dopuna te tehničku dokumentaciju 10 godina od stavljanja proizvoda s digitalnim elementima na tržište ili tijekom razdoblja potpore, ovisno o tome što je dulje.

11. Proizvođačev ovlašteni zastupnik može podnijeti zahtjev iz točke 3. i ispuniti obveze iz točaka 7. i 10. ako su relevantne obveze navedene u ovlaštenju.

Dio III. Sukladnost s tipom na temelju unutarnje kontrole proizvodnje (na temelju modula C)

1. Sukladnost s tipom na temelju unutarnje kontrole proizvodnje dio je postupka ocjenjivanja sukladnosti kojim proizvođač ispunjava obveze utvrđene u točkama 2. i 3. ovog dijela te osigurava i izjavljuje da su predmetni proizvodi s digitalnim elementima sukladno s tipom opisanim u potvrdi o EU ispitivanju tipa i da ispunjavaju bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu I. Priloga I. te da proizvođač ispunjava bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu II. Priloga I.

2. Proizvodnja

   Proizvođač poduzima sve potrebne mjere kako bi se proizvodnjom i njezinim praćenjem osigurala sukladnost proizvedenih proizvoda s digitalnim elementima s tipom opisanim u potvrdi o EU ispitivanju tipa i bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu I. Priloga I. te osigurava to da proizvođač ispunjava bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu II. Priloga I.

3. Oznaka sukladnosti i izjava o sukladnosti

   3.1 Proizvođač stavlja oznaku CE na svaki pojedini proizvod s digitalnim elementima koji je sukladan s tipom opisanim u potvrdi o EU ispitivanju tipa i ispunjava primjenjive zahtjeve utvrđene u ovoj Uredbi.

   3.2 Proizvođač za svaki model proizvoda sastavlja pisanu izjavu o sukladnosti i drži je na raspolaganju nacionalnim tijelima 10 godina od stavljanja proizvoda s digitalnim elementima na tržište ili tijekom razdoblja potpore, ovisno o tome što je dulje. U izjavi o sukladnosti identificira se model proizvoda za koji je izjava sastavljena. Primjerak izjave o sukladnosti stavlja se na raspolaganje relevantnim tijelima na njihov zahtjev.

4. Ovlašteni zastupnik

   Obveze proizvođača iz točke 3. u njegovo ime i na njegovu odgovornost može ispuniti njegov ovlašteni zastupnik ako su relevantne obveze navedene u ovlaštenju.

Dio IV. Sukladnost na temelju potpunog osiguranja kvalitete (na temelju modula H)

1. Sukladnost na temelju potpunog osiguranja kvalitete je postupak ocjenjivanja sukladnosti kojim proizvođač ispunjava obveze utvrđene u točkama 2. i 5. ovog dijela te osigurava i izjavljuje na vlastitu odgovornost da predmetni proizvodi s digitalnim elementima (ili kategorije proizvoda) ispunjavaju bitne zahtjeve u pogledu kibernetičke sigurnosti utvrđene u dijelu I. Priloga I. i da procesi postupanja s ranjivostima koje je uspostavio proizvođač ispunjavaju zahtjeve utvrđene u dijelu II. Priloga I.

2. Projektiranje, razvoj, proizvodnja i postupanje s ranjivostima proizvoda s digitalnim elementima

Proizvođač primjenjuje odobreni sustav kvalitete iz točke 3. za projektiranje, razvoj i pregled konačnog proizvoda i ispitivanje predmetnih proizvoda s digitalnim elementima te za postupanje s ranjivostima, održava njegovu djelotvornost tijekom razdoblja potpore te podliježe nadzoru iz točke 4.

3. Sustav kvalitete

3.1 Proizvođač podnosi zahtjev za ocjenjivanje svog sustava kvalitete za predmetne proizvode s digitalnim elementima prijavljenom tijelu prema svojem izboru.

Zahtjev mora sadržavati:

(a) ime i adresu proizvođača te, ako zahtjev podnosi njegov ovlašteni zastupnik, ime i adresu tog ovlaštenog zastupnika;

(b) tehničku dokumentaciju za jedan model iz svake kategorije proizvoda s digitalnim elementima namijenjene za proizvodnju ili razvoj. Tehnička dokumentacija sadržava, kad je to primjenjivo, barem elemente utvrđene u Prilogu VII.;

(c) dokumentaciju o sustavu kvalitete; i

(d) pisanu izjavu da isti zahtjev nije podnesen nijednom drugom prijavljenom tijelu.

3.2 Sustavom kvalitete osigurava se sukladnost proizvoda s digitalnim elementima s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu I. Priloga I. i sukladnost procesa postupanja s ranjivostima koje je uspostavio proizvođač s bitnim zahtjevima u pogledu kibernetičke sigurnosti utvrđenima u dijelu II. Priloga I.

Sve elemente, zahtjeve i odredbe koje proizvođač primjenjuje sustavno i metodično se dokumentira u obliku pisanih pravila, postupaka i uputa. Na temelju te dokumentacije o sustavu kvalitete mora biti moguće dosljedno tumačenje programa, planova, priručnika i zapisa o kvaliteti.

On prije svega sadržava odgovarajući opis:

(a) ciljeva kvalitete, organizacijske strukture te odgovornosti i ovlasti uprave s obzirom na projektiranje, razvoj i kvalitetu proizvoda te postupanje s ranjivostima;

(b) tehničkih specifikacija projektiranja i razvoja, uključujući norme, koje će se primijeniti te, ako se relevantne usklađene norme ili tehničke specifikacije neće primijeniti u cijelosti, načina na koje će se osigurati ispunjavanje bitnih zahtjeva u pogledu kibernetičke sigurnosti utvrđenih u dijelu I. Priloga I. koji se primjenjuju na proizvode s digitalnim elementima;

(c) specifikacija postupaka, uključujući norme, koje će se primijeniti te, ako se relevantne usklađene norme ili tehničke specifikacije neće primijeniti u cijelosti, načina na koje će se osigurati ispunjavanje bitnih zahtjeva u pogledu kibernetičke sigurnosti utvrđenih u dijelu II. Priloga I. koji se primjenjuju na proizvođača;

(d) kontrole projektiranja i razvoja te tehnika, procesa i sustavnih mjera za provjeru projektiranja i razvoja koji će se primjenjivati u projektiranju i razvoju proizvoda s digitalnim elementima iz te kategorije proizvoda;

(e) odgovarajućih tehnika, procesa i sustavnih mjera koji će se primjenjivati u proizvodnji, kontroli kvalitete i osiguranju kvalitete;

(f) pregleda i ispitivanja koji će se provoditi prije, tijekom i nakon proizvodnje te njihove učestalosti;

(g) evidencije kvalitete, kao što su inspekcijska izvješća i podaci iz ispitivanja, podaci o umjeravanju i izvješća o osposobljenosti uključenog osoblja;

(h) načina praćenja postizanja potrebne kvalitete projektiranja i proizvoda te djelotvornosti sustava kvalitete.

3.3 Prijavljeno tijelo ocjenjuje sustav kvalitete kako bi utvrdilo ispunjava li zahtjeve iz točke 3.2.

Ono pretpostavlja sukladnost s tim zahtjevima u pogledu elemenata sustava kvalitete koji su u skladu s odgovarajućim specifikacijama iz nacionalne norme kojom se provodi relevantna usklađena norma ili tehnička specifikacija.

Revizorski tim mora imati iskustva sa sustavima upravljanja kvalitetom i barem jednog člana s iskustvom ocjenjivača u području relevantnog proizvoda i tehnologije proizvoda te mora poznavati primjenjive zahtjeve utvrđene u ovoj Uredbi. Revizija uključuje posjet proizvođačevim objektima, ako postoje, radi ocjenjivanja. Revizorski tim pregledava tehničku dokumentaciju iz točke 3.1. točke (b) kako bi provjerio sposobnost proizvođača da utvrdi primjenjive zahtjeve utvrđene u ovoj Uredbi i provede potrebne preglede za osiguranje sukladnosti proizvoda s digitalnim elementima s tim zahtjevima.

O odluci se obavješćuje proizvođača ili njegova ovlaštenog zastupnika.

Obavijest sadržava zaključke revizije i obrazloženu odluku o ocjeni.

3.4 Proizvođač je dužan ispunjavati obveze koje proizlaze iz odobrenog sustava kvalitete i održavati ga kako bi uvijek bio primjeren i učinkovit.

3.5 Proizvođač obavješćuje prijavljeno tijelo koje je odobrilo sustav kvalitete o svakoj planiranoj izmjeni sustava kvalitete.

Prijavljeno tijelo ocjenjuje sve predložene izmjene i donosi odluku o tome hoće li izmijenjeni sustav kvalitete i dalje ispunjavati zahtjeve iz točke 3.2. ili ga je potrebno ponovno ocijeniti.

O svojoj odluci obavješćuje proizvođača. Obavijest sadržava zaključke pregleda i obrazloženu odluku o ocjeni.

4. Nadzor pod odgovornošću prijavljenog tijela

4.1 Svrha je nadzora osigurati da proizvođač uredno ispunjava obveze koje proizlaze iz odobrenog sustava kvalitete.

4.2 Proizvođač za potrebe ocjenjivanja omogućuje prijavljenom tijelu pristup prostorima za projektiranje, razvoj, proizvodnju, inspekciju, ispitivanje i skladištenje te mu pruža sve potrebne informacije, a posebno:

(a) dokumentaciju o sustavu kvalitete;

(b) zapise o kvaliteti iz dijela sustava kvalitete koji se odnosi na projektiranje, kao što su rezultati analiza, proračuni i ispitivanja;

(c) zapise o kvaliteti iz dijela sustava kvalitete koji se odnosi na proizvodnju, kao što su inspekcijska izvješća i podaci iz ispitivanja, podaci o umjeravanju i izvješća o osposobljenosti uključenog osoblja.

4.3 Prijavljeno tijelo provodi periodične revizije kako bi provjerilo da proizvođač održava i primjenjuje sustav kvalitete te proizvođaču dostavlja izvješće o reviziji.

5. Oznaka sukladnosti i izjava o sukladnosti

5.1 Proizvođač stavlja oznaku CE i, pod odgovornošću prijavljenog tijela iz točke 3.1., identifikacijski broj tog tijela na svaki pojedinačni proizvod s digitalnim elementima koji ispunjava zahtjeve utvrđene u dijelu I. Priloga I.

5.2 Proizvođač za svaki model proizvoda sastavlja pisanu izjavu o sukladnosti i drži je na raspolaganju nacionalnim tijelima 10 godina od stavljanja proizvoda s digitalnim elementima na tržište ili tijekom razdoblja potpore, ovisno o tome što je dulje. U izjavi o sukladnosti mora biti identificiran model proizvoda za koji je izjava sastavljena.

Primjerak izjave o sukladnosti stavlja se na raspolaganje relevantnim tijelima na njihov zahtjev.

6. Proizvođač barem 10 godina od stavljanja proizvoda s digitalnim elementima na tržište ili tijekom razdoblja potpore, ovisno o tome što je dulje, drži na raspolaganju nacionalnim tijelima sljedeću dokumentaciju:

(a) tehničku dokumentaciju iz točke 3.1.;

(b) dokumentaciju sustava kvalitete iz točke 3.1.;

(c) izmjenu iz točke 3.5. kako je odobrena;

(d) odluke i izvješća prijavljenog tijela iz točaka 3.5. i 4.3.

7. Svako prijavljeno tijelo obavješćuje svoja tijela koja provode prijavljivanje o izdanim ili povučenim odobrenjima sustava kvalitete i periodično ili na zahtjev svojim tijelima koja provode prijavljivanje stavlja na raspolaganje popis odobrenja sustava kvalitete koja je odbilo, suspendiralo ili na drugi način ograničilo.

Svako prijavljeno tijelo obavješćuje druga prijavljena tijela o odobrenjima sustava kvalitete koja je odbilo, suspendiralo ili povuklo, a na zahtjev i o odobrenjima sustava kvalitete koja je izdalo.

8. Ovlašteni zastupnik

Obveze proizvođača iz točaka 3.1., 3.5., 5. i 6. može u njegovo ime i na njegovu odgovornost ispuniti njegov ovlašteni zastupnik ako su relevantne obveze navedene u ovlaštenju.

U vezi s ovim aktom dana je izjava koja se može pronaći u SL C, 2024/6786, 20.11.2024., ELI: http://data.europa.eu/eli/C/2024/6786/oj.