C/2026/6013

17.11.2026.

KOMUNIKACIJA KOMISIJE

Smjernice Komisije o primjeni Uredbe (EU) 2024/2847 (Akt o kibernetičkoj otpornosti)

(C/2026/6013)

Sadržaj

Stranica

1. UVOD 3
   1.1. Akt o kibernetičkoj otpornosti 3
   1.2. Svrha smjernica 3
2. PODRUČJE PRIMJENE 4
   2.1. Stavljanje na tržište 4
   2.2. Softver kao proizvod s digitalnim elementima 5
   2.3. Računalni kod 6
   2.4. Kombinacija hardvera i softvera koja čini proizvod s digitalnim elementima 7
   2.5. Podatkovna veza 8
   2.6. Složeni sustavi 8
   2.7. Proizvodi s digitalnim elementima projektirani prije početka primjene Akta o kibernetičkoj otpornosti 9
3. BESPLATNI SOFTVER OTVORENOG KODA 11
   3.1. Utvrđivanje odgovornosti za besplatni softver otvorenog koda 12
   3.2. Utvrđivanje je li besplatni softver otvorenog koda stavljen na tržište EU-a 13
      3.2.1. Naplaćivanje cijene 13
      3.2.2. Unovčenje drugih usluga ili uvjetovanje upotrebe obradom osobnih podataka 13
      3.2.3. Usluge podrške 14
      3.2.4. Donacije 15
      3.2.5. Financiranje besplatnog softvera otvorenog koda 15
      3.2.6. Neprofitni subjekti ustrojeni radi postizanja neprofitnih ciljeva 16
      3.2.7. Integracija koju provode drugi proizvođači 16
   3.3. Upravitelji softvera otvorenog koda 16
      3.3.1. Kontinuirana potpora i osiguravanje održivosti FOSS-a 17
   3.4. Doprinositelji i korisnici niže u lancu opskrbe 18
   3.5. Primjeri scenarija 19
4. BITNE IZMJENE I REZERVNI DIJELOVI 21
   4.1. Fizički popravci 22
   4.2. Rezervni dijelovi 23
   4.3. Ažuriranja softvera kao bitne izmjene 24

4.4. Posljedice bitne izmjene 27
4.4.1. Bitne izmjene koje je učinila osoba koja nije izvorni proizvođač 28
4.4.2. Bitne izmjene koje je učinio izvorni proizvođač 29
5. RAZDOBLJE POTPORE 29
5.1. Bitne izmjene i razdoblje potpore 31
6. VAŽNI I KRITIČNI PROIZVODI S DIGITALNIM ELEMENTIMA 32
6.1. Osnovna funkcionalnost 33
6.2. Ocjenjivanje sukladnosti važnih i kritičnih proizvoda s digitalnim elementima 36
6.3. Značenje za pretpostavku sukladnosti 38
7. PROCJENA KIBERNETIČKOSIGURNOSNIH RIZIKA I INTEGRACIJA PROIZVODA S DIGITALNIM ELEMENTIMA I KOMPONENTI 41
7.1. Procjena i postupanje s kibernetičkosigurnosnim rizicima 41
7.2. Projektiranje, razvoj i proizvodnja proizvoda s digitalnim elementima tako da osiguravaju odgovarajuću razinu kibernetičke sigurnosti na temelju rizika 42
7.3. Procjena rizika i dužna pažnja u kontekstu vanjskih ovisnosti i integriranih komponenti 42
7.4. Ponovna upotreba procjena rizika i dokumentacije o sukladnosti za skupine proizvoda s digitalnim elementima 44
8. DALJINSKA OBRADA PODATAKA 44
8.1. Što se smatra rješenjem za daljinsku obradu podataka za proizvod s digitalnim elementima? 45
8.1.1. Pojam „na daljinu” 46
8.1.2. Bi li nepostojanje takve obrade podataka onemogućilo proizvodu s digitalnim elementima obavljanje neke od njegovih funkcija? 46
8.1.3. Je li proizvođač projektirao i razvio softver odnosno je li to učinjeno pod njegovom odgovornošću? 47
8.2. Praktične i tehničke implikacije rješenja za daljinsku obradu podataka i oslanjanje na rješenja trećih strana 49
8.3. Primjeri upotrebe rješenja za daljinsku obradu podataka 50
8.3.1. Aplikacija za mobilno bankarstvo 51
8.3.2. Pametni termostat 52
8.3.3. e-čitač 53
8.3.4. Industrijski robot 53
8.3.5. Mobilna radiotelefonska mreža 53
9. DODATNI ELEMENTI 54
9.1. Obveze u pogledu izvješćivanja 54
9.2. Postupanje s ranjivostima 56
9.2.1. Obavješćivanje o ranjivostima više u lancu opskrbe i dijeljenje sigurnosnih popravaka 56
9.2.2. Poznate iskoristive ranjivosti 57
9.2.3. Djelotvorna i redovita ispitivanja i preispitivanja 58
9.3. Međudjelovanje s drugim zakonodavstvom 59
9.3.1. Uredba (EU) 2019/2144 i Uredba (EU) br. 168/2013 59
9.3.2. Valjanost potvrda o EU ispitivanju tipa (članak 69. stavak 1.) 59

1. **UVOD**

1.1. **Akt o kibernetičkoj otpornosti**

1. 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) ([1]) stupila je na snagu 10. prosinca 2024. Njome se nastoji ojačati pristup EU-a kibernetičkoj sigurnosti, riješiti pitanje kibernetičke otpornosti na razini EU-a i poboljšati funkcioniranje unutarnjeg tržišta utvrđivanjem jedinstvenog pravnog okvira za bitne zahtjeve u pogledu kibernetičke sigurnosti koji se odnose na stavljanje proizvoda s digitalnim elementima na tržište EU-a te obuhvaćaju cijeli životni ciklus tih proizvoda.

2. Akt o kibernetičkoj otpornosti temelji se na novom zakonodavnom okviru EU-a utvrđenom u Uredbi (EZ) br. 765/2008 Europskog parlamenta i Vijeća od 9. srpnja 2008. o utvrđivanju zahtjeva za akreditaciju i za nadzor tržišta u odnosu na stavljanje proizvoda na tržište i o stavljanju izvan snage Uredbe (EEZ) br. 339/93 i Odluci 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 ([2]).

3. Nadzor tržišta i izvršavanje provode nacionalna tijela za nadzor tržišta. Na proizvode s digitalnim elementima koji su obuhvaćeni područjem primjene Akta o kibernetičkoj otpornosti primjenjuje se 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. Komisija i Agencija Europske unije za kibernetičku sigurnost (ENISA) podupiru gospodarske subjekte i države članice u primjeni Akta o kibernetičkoj otpornosti.

1.2. **Svrha smjernica**

4. U skladu s člankom 26. stavkom 1. Akta o kibernetičkoj otpornosti Komisija treba objaviti smjernice kako bi pomogla gospodarskim subjektima u primjeni Uredbe, a njihova glavna svrha treba biti olakšavanje ispunjavanja obveza za mikropoduzeća te mala i srednja poduzeća (MSP-ovi). U članku 26. stavku 2. utvrđuju se minimalni aspekti koji bi trebali biti obuhvaćeni smjernicama. To su među ostalim: (i) područje primjene Akta o kibernetičkoj otpornosti (prije svega rješenja za daljinsku obradu podataka i besplatni softver otvorenog koda); (ii) pojam „razdoblja potpore”; (iii) povezanost Akta o kibernetičkoj otpornosti i drugog zakonodavstva EU-a; i (iv) pojam „bitna izmjena”.

5. Komisija je 3. prosinca 2025. objavila najčešća pitanja, čija je svrha pomoći gospodarskim subjektima da se pripreme za provedbu Akta o kibernetičkoj otpornosti ([3]).

6. Svrha je ovih smjernica pomoći gospodarskim subjektima da se usklade s Aktom o kibernetičkoj otpornosti i poduprijeti aktivnosti tijela za nadzor tržišta, tijela koja provode prijavljivanje i prijavljenih tijela kako bi se omogućilo usklađeno izvršavanje Akta o kibernetičkoj otpornosti u cijeloj Uniji. Svrha nije obuhvatiti cijelo područje primjene Akta o kibernetičkoj otpornosti, nego obrazložiti određene važne odredbe i opisati način na koji bi se one mogle provesti u praksi. Ove smjernice odnose se na Akt o kibernetičkoj otpornosti i ne primjenjuju se na druge propise EU-a.

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

([2]) U programu rada Komisije za 2026. predviđa se predstavljanje „Europskog akta o proizvodima”, kojim bi se ažurirali novi zakonodavni okvir te pravila o nadzoru tržišta i standardizaciji: https://eur-lex.europa.eu/legal-content/HR/TXT/?uri=CELEX:52025DC0870.

([3]) Najčešća pitanja mogu se preuzeti na internetskim stranicama Komisije o provedbi Akta o kibernetičkoj otpornosti, na posebnoj internetskoj stranici s najčešćim pitanjima.

7. U okviru njihove pripreme provedeno je opsežno savjetovanje s dionicima, među ostalim sa Stručnom skupinom za kibernetičku sigurnost proizvoda s digitalnim elementima ([4]), a održano je i javno savjetovanje od 3. ožujka do 13. travnja 2026 ([5]).

8. Ove smjernice nisu obvezujuće za gospodarske subjekte ili druge subjekte na koje se primjenjuje Akt o kibernetičkoj otpornosti. Mjerodavno tumačenje Akta o kibernetičkoj otpornosti može dati samo Sud Europske unije. Međutim, u ovim se smjernicama iznosi Komisijino tumačenje Akta o kibernetičkoj otpornosti kako bi se pridonijelo usklađenosti i djelotvornoj provedbi Uredbe. Osim toga, smjernice sadržavaju niz primjera primjene konkretnih odredaba. Međutim, svrha tih primjera nije zamijeniti pojedinačnu procjenu, koja će uvijek biti potrebna kako bi se uzele u obzir posebnosti svakog pojedinog slučaja.

9. U skladu s člankom 26. Akta o kibernetičkoj otpornosti Komisija može razmotriti izdavanje dodatnih smjernica, uključujući smjernice za proizvođače na koje se primjenjuje Akt o kibernetičkoj otpornosti i drugo zakonodavstvo Unije o usklađivanju ili drugi povezani pravni akti Unije. U ovim se smjernicama mogu, na primjer, obraditi pitanja povezanosti Akta o kibernetičkoj otpornosti, Uredbe (EU) 2024/1689 o utvrđivanju usklađenih pravila o umjetnoj inteligenciji (UI akt) i Uredbe (EU) 2022/2554 o digitalnoj operativnoj otpornosti za financijski sektor (DORA).

2. **PODRUČJE PRIMJENE**

2.1. **Stavljanje na tržište**

10. Akt o kibernetičkoj otpornosti primjenjuje se na proizvode s digitalnim elementima koji se stavljaju na raspolaganje na tržištu EU-a. Pojam stavljanja na raspolaganje na tržištu definiran je u članku 3. točki 22. Akta o kibernetičkoj otpornosti kao „isporuka proizvoda s digitalnim elementima za distribuciju ili upotrebu na tržištu Unije u okviru trgovačke djelatnosti uz naplatu ili besplatno”. U skladu s člankom 3. točkom 21. smatra se da je proizvod s digitalnim elementima stavljen na tržište EU-a kad je prvi put stavljen na raspolaganje.

11. Najnovije izdanje „Plavog vodiča o provedbi pravila EU-a o proizvodima”, objavljeno 2022. (dalje u tekstu „Plavi vodič”) ([6]), sadržava smjernice čija je svrha olakšati razumijevanje pravila EU-a o proizvodima i omogućiti njihovu ujednačenu primjenu u raznim sektorskim pravnim okvirima usklađenima s novim zakonodavnim okvirom, kao što je Akt o kibernetičkoj otpornosti. U Plavom vodiču navodi se da pojmove „stavljanje na tržište” i „stavljanje na raspolaganje” treba tumačiti kao da se odnose na „svaki proizvod pojedinačno, a ne na vrstu proizvoda te činjenicu je li proizveden kao zasebna jedinica ili kao dio serije” (točka 2.3.).

12. Kad je riječ o „tradicionalnijim” proizvodima s digitalnim elementima obuhvaćenima novim zakonodavnim okvirom, kao što su hardver u obliku strojeva ili radijska oprema s digitalnim elementima, pojam „stavljanje na tržište” već je ustaljen, a u Plavom vodiču iznose se dodatne smjernice kako bi se pojasnilo kad se smatra da su ti proizvodi stavljeni na tržište. U točki 2.12. Plavog vodiča, naslovljenoj „Sažeti primjeri”, navode se dodatni primjeri pojma „stavljanje na tržište”.

13. Međutim, s obzirom na prirodu nematerijalnih proizvoda s digitalnim elementima kao što je samostalni softver, potrebne su dodatne smjernice o pitanju kad se takvi proizvodi s digitalnim elementima smatraju stavljenima na tržište. Nakon završetka faze proizvodnje softvera i nakon što se proizvod s digitalnim elementima ponudi potencijalnim korisnicima na tržištu EU-a, može se smatrati da je njegov proizvođač proizveo više primjeraka istog softverskog proizvoda s digitalnim elementima i isporučio ih za distribuciju ili upotrebu. Zapravo, za razliku od materijalnih proizvoda s digitalnim elementima, na samostalni softver ne primjenjuju se ograničenja koja proizlaze

([4]) Stručna skupina za kibernetičku sigurnost proizvoda s digitalnim elementima u Registru stručnih skupina Komisije i drugih sličnih subjekata.
([5]) Javno savjetovanje o nacrtu smjernica Komisije o Aktu o kibernetičkoj otpornosti.
([6]) Obavijest Komisije – „Plavi vodič” o provedbi pravila EU-a o proizvodima 2022., 2022/C 247/01, SL C 247, 29.6.2022., str. 1.).

iz fizičke proizvodnje ili zaliha: svakim stavljanjem softvera na raspolaganje za preuzimanje ili distribuciju izrađuje se novi identičan primjerak za korisnika. Sve dok se ta verzija softvera ne izmijeni na način koji utječe na ispunjavanje obveza iz Akta o kibernetičkoj otpornosti, smatra se da je do stavljanja na tržište EU-a došlo u trenutku prve ponude za distribuciju ili upotrebu. Mogućnost kasnijeg preuzimanja ili distribucije te verzije softverskog proizvoda s digitalnim elementima stoga treba smatrati slučajem stavljanja tog softverskog proizvoda s digitalnim elementima na raspolaganje ([7]).

14. Stoga bi trebalo smatrati da je samostalni softverski proizvod s digitalnim elementima stavljen na tržište u trenutku u kojem je njegova faza proizvodnje završena i taj se softver prvi put isporučuje za distribuciju ili upotrebu na tržištu EU-a u okviru trgovačke djelatnosti. Trebalo bi smatrati da je proizvođač istodobno stavio na tržište više primjeraka istog softverskog proizvoda s digitalnim elementima. Stoga, iako više primjeraka istog softvera ostaju zasebni proizvodi s digitalnim elementima, smatra se da su oni stavljeni na tržište u isto vrijeme, neovisno o trenutku prijenosa posjedovanja ili upotrebe svakog pojedinačnog primjerka na drugu fizičku ili pravnu osobu. Međutim, ako proizvođač stavlja na raspolaganje različite inačice softvera koje se razlikuju po komponentama, konfiguracijama ili omogućenim funkcionalnostima (npr. verzije za različite operativne sustave ili paketi s različitim značajkama), te se inačice ne mogu smatrati višestrukim primjercima istog softverskog proizvoda s digitalnim elementima. Stoga bi ih za potrebe stavljanja na tržište trebalo smatrati različitim proizvodima s digitalnim elementima.

Primjer 1: Poduzeće A na svojim internetskim stranicama prvi put isporučuje za distribuciju verziju 1.0.0 svojeg softvera X 1. siječnja 2028. Istog dana kupac 1 kupuje primjerak verzije 1.0.0 softvera X. Kupac 2 kupuje primjerak verzije 1.0.0 softvera X 15. siječnja 2028. Oba primjerka verzije 1.0.0 softvera X stavljena su na tržište 1. siječnja 2028.

15. S obzirom na iterativnu prirodu razvoja softvera, trebalo bi dodatno pojasniti da se kasnije iteracije softverskog proizvoda s digitalnim elementima smatraju novim proizvodima stavljenima na tržište ako je u tim iteracijama došlo do „bitne izmjene" softverskog proizvoda s digitalnim elementima koji je već stavljen na tržište, kako je navedeno u uvodnoj izjavi 41. Akta o kibernetičkoj otpornosti. Za iteracije u kojima nije došlo do bitnih izmjena proizvođač ne mora provesti novi postupak ocjenjivanja sukladnosti te se stoga ne mijenja datum stavljanja tog softvera na tržište. Za više smjernica o pojmu bitnih izmjena vidjeti odjeljak *4.* – Bitne izmjene.

Primjer 2: Poduzeće A na svojim internetskim stranicama prvi put isporučuje za distribuciju verziju 1.0.0 svojeg softvera X 1. siječnja 2028. Istog dana kupac 1 kupuje primjerak verzije 1.0.0 softvera X. Poduzeće A 15. siječnja 2028. izdaje ažuriranu verziju 1.0.1 softvera X koja ne predstavlja bitnu izmjenu. Kupac 2 kupuje primjerak verzije 1.0.1 softvera X 30. siječnja 2028. Smatra se da su oba primjerka softvera X u verzijama 1.0.0 i 1.0.1 stavljena na tržište 1. siječnja 2028.

16. Smjernice utvrđene u točkama 13., 14. i 15. primjenjuju se isključivo ako je proizvod s digitalnim elementima samostalni softver. To nije slučaj, na primjer, kad se softver kombinira s hardverom, kako je objašnjeno u odjeljku *2.4.* – Kombinacija hardvera i softvera koja čini proizvod.

2.2. **Softver kao proizvod s digitalnim elementima**

17. U članku 3. točki 1. Akta o kibernetičkoj otpornosti proizvod s digitalnim elementima definiran je kao „softverski ili hardverski proizvod i njegova rješenja za daljinsku obradu podataka, uključujući softverske ili hardverske komponente koje se zasebno stavljaju na tržište". Ti proizvodi s digitalnim elementima obuhvaćeni su područjem primjene Akta o kibernetičkoj otpornosti ako njihova namjena ili razumno predvidljiva upotreba uključuje izravnu ili neizravnu logičku ili fizičku podatkovnu vezu s uređajem ili mrežom.

([7]) U skladu s člankom 13. stavkom 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.

18. Akt o kibernetičkoj otpornosti stoga se može primjenjivati na niz proizvoda s digitalnim elementima, među ostalim na: (i) samostalni softver, kao što su aplikacije i računalni programi, digitalno ili fizički distribuirani; (ii) hardver s ugrađenim softverom (npr. uređaji interneta stvari, prijenosna računala, tablet računala); (iii) samostalni hardver (npr. integrirani krugovi, matične ploče); i (iv) svaku kombinaciju hardvera i softvera isporučenih zasebno, ali namijenjenih zajedničkom radu.

19. Samostalni softver stoga je obuhvaćen područjem primjene Akta o kibernetičkoj otpornosti ako je stavljen na tržište kao proizvod s digitalnim elementima. Korisno je razlikovati softverske proizvode s digitalnim elementima na koje se primjenjuje Akt o kibernetičkoj otpornosti od usluga koje se pružaju na daljinu i koje nisu obuhvaćene područjem primjene tog akta.

20. Kako bi softver bio obuhvaćen područjem primjene Akta o kibernetičkoj otpornosti, softverski proizvod s digitalnim elementima mora se staviti na raspolaganje korisniku, a korisnik ga mora nabaviti i služiti se njime u svojem elektroničkom informacijskom sustavu ili kao dijelom takvog sustava. Softver koji se preuzima, instalira ili na neki drugi način isporučuje korisniku i koji se pokreće na korisnikovu elektroničkom informacijskom sustavu ispunjava te kriterije, među ostalim ako taj softver ima oblik, na primjer, proširenja preglednika ili aplikacije razvijene pomoću internetskih tehnologija, ali isporučene za lokalnu upotrebu.

21. Suprotno tomu, softver koji se izvršava na daljinu i kojem korisnik samo pristupa ne može se samo na temelju toga smatrati proizvodom s digitalnim elementima. U uvodnim izjavama 11. i 12. Akta o kibernetičkoj otpornosti zapravo se pravi razlika između ta dva slučaja tako što se objašnjava da se na obradu ili pohranu na daljinu Akt o kibernetičkoj otpornosti primjenjuje samo u mjeri u kojoj su potrebne kako bi proizvod s digitalnim elementima obavljao svoje funkcije (tj. na temelju pojma daljinske obrade podataka kako je definiran u članku 3. točki 2.), ali te usluge same po sebi ne predstavljaju proizvod s digitalnim elementima. Najčešći su primjer internetske aplikacije, uključujući progresivne internetske aplikacije, kojima se pristupa isključivo preko internetskog preglednika. Isto vrijedi i za internetske stranice: iako one tehnički mogu u ograničenoj mjeri raditi i izvršavati se na korisnikovu uređaju, iz uvodne izjave 12. Akta o kibernetičkoj otpornosti proizlazi da se internetske stranice same po sebi ne smatraju proizvodima s digitalnim elementima te su obuhvaćene područjem primjene Akta o kibernetičkoj otpornosti samo ako podržavaju funkcionalnost proizvoda s digitalnim elementima, tj. u mjeri u kojoj predstavljaju daljinsku obradu podataka (kako je dodatno objašnjeno u odjeljku *8.*, a osobito u odjeljku *8.1.2.* – Bi li nepostojanje takve obrade podataka onemogućilo proizvodu s digitalnim elementima obavljanje neke od njegovih funkcija?).

Primjer 3: Mobilna aplikacija koju korisnik preuzima iz trgovine aplikacijama i instalira na svoj pametni telefon isporučuje se korisniku i izvršava na korisnikovu uređaju te je stoga proizvod s digitalnim elementima. Ako se stavlja na tržište u okviru trgovačke djelatnosti, može biti obuhvaćena područjem primjene Akta o kibernetičkoj otpornosti.

Primjer 4: Stolna aplikacija izrađena pomoću internetskih tehnologija, ali upakirana za lokalnu instalaciju, isporučuje se korisniku i izvršava na korisnikovu uređaju te je stoga proizvod s digitalnim elementima. Ako se stavlja na tržište u okviru trgovačke djelatnosti, može biti obuhvaćena područjem primjene Akta o kibernetičkoj otpornosti.

Primjer 5: Internetska aplikacija kojoj korisnik pristupa isključivo preko internetskog preglednika nije proizvod s digitalnim elementima. Obuhvaćena je područjem primjene Akta o kibernetičkoj otpornosti samo ako podržava funkcionalnost proizvoda s digitalnim elementima. Suprotno tomu, aplikacija koja se isporučuje korisniku kao lokalno instalirani klijentski softver i koja se izvršava na korisnikovu uređaju proizvod je s digitalnim elementima. Ako se stavlja na tržište u okviru trgovačke djelatnosti, može biti obuhvaćena područjem primjene Akta o kibernetičkoj otpornosti.

Ako se taj klijent za obavljanje jedne ili više funkcija oslanja na obradu podataka na daljinu koja odgovara definiciji daljinske obrade podataka, ta je obrada također dio proizvoda s digitalnim elementima.

Primjer 6: Internetske stranice koje samo prikazuju informacije svojim posjetiteljima i ne podržavaju funkcionalnost proizvoda s digitalnim elementima same po sebi nisu proizvod s digitalnim elementima. Stoga nisu obuhvaćene područjem primjene Akta o kibernetičkoj otpornosti.

2.3. **Računalni kod**

22. Korisno je i pojasniti može li izvorni kod predstavljati softverski proizvod s digitalnim elementima. U Aktu o kibernetičkoj otpornosti „softver” je definiran kao „dio elektroničkog informacijskog sustava koji se sastoji od računalnog koda” (članak 3. točka 4.). Računalni kod može biti u obliku (i) strojnog koda, odnosno skupa uputa napisanih u binarnom obliku koje izravno izvršava procesor računala; ili (ii) izvornog koda, odnosno skupa uputa i naredbi napisanih na programskom jeziku, koji prvo treba kompilirati ili interpretirati kako bi ga računalo moglo izvršiti. Definicija softvera utvrđena u Aktu o kibernetičkoj otpornosti obuhvaća oboje.

23. Zasebno je pitanje predstavlja li određena isporuka računalnog koda stavljanje proizvoda s digitalnim elementima na tržište EU-a, za što je potrebna isporuka u okviru trgovačke djelatnosti. To često nije slučaj s izvornim kodom. Na primjer, za potrebe Akta o kibernetičkoj otpornosti općenito se ne smatra da fizička ili pravna osoba koja besplatno dijeli otvoreni računalni kod na javno dostupnim repozitorijima stavlja taj kod na tržište EU-a (kako je detaljnije objašnjeno u odjeljku 3. – Besplatni softver otvorenog koda). Nedovršeni kod koji se dijeli tijekom faze projektiranja i razvoja proizvoda s digitalnim elementima (npr. radi ispitivanja ili preispitivanja) također se ne smatra stavljenim na tržište za potrebe Akta o kibernetičkoj otpornosti jer njegova faza proizvodnje nije završena. Slično tomu, ogledni ili demonstracijski kod dostavljen kao dio uputa ili materijala za osposobljavanje ne smatra se stavljenim na tržište za potrebe Akta o kibernetičkoj otpornosti ([8]).

24. Međutim, ako proizvođač svojim kupcima stavlja na raspolaganje računalni kod kao proizvod s digitalnim elementima, smatra se da je taj kod stavljen na tržište, neovisno o tome je li riječ o strojnom ili izvornom kodu ([9]).

Primjer 7: Poduzeće A daje poduzeću B licenciju za izvorni kod za internu platformu koja se može prilagođavati i dostavlja taj izvorni kod u tekstualnoj datoteci. Čak i ako poduzeće B mora taj izvorni kod dodatno prilagoditi i kompilirati prije njegove upotrebe, poduzeće A stavlja taj izvorni kod na tržište i stoga se na njega primjenjuje Akt o kibernetičkoj otpornosti. Poduzeće A nije odgovorno za usklađenost kasnijih prilagodbi i kompiliranja tog koda koje provodi poduzeće B s Aktom o kibernetičkoj otpornosti.

2.4. **Kombinacija hardvera i softvera koja čini proizvod s digitalnim elementima**

25. Je li softver dio proizvoda s digitalnim elementima ne bi trebalo utvrđivati na temelju toga kako ili kad je taj softver isporučen korisniku, nego na temelju toga je li, s obzirom na namjenu i razumno predvidljivu upotrebu proizvoda, softver potreban kako bi proizvod s digitalnim elementima mogao obavljati svoje predviđene funkcije. Ako je hardverski proizvod s digitalnim elementima projektiran tako da je za obavljanje njegovih funkcija potreban zajednički rad s određenim softverom istog proizvođača, taj hardver i taj softver zajedno čine proizvod s digitalnim elementima. Softver koji je potreban za rad, konfiguraciju, kontrolu ili upotrebu proizvoda s digitalnim elementima u skladu s njegovom namjenom stoga čini dio proizvoda s digitalnim elementima, čak i ako se nabavlja preko zasebnog kanala (npr. trgovina aplikacijama, poveznica za preuzimanje ili drugi digitalni kanal nakon što je hardverski proizvod s digitalnim elementima stavljen na tržište). Stoga se smatra da se on stavlja na tržište u istom trenutku u kojem se na tržište stavljaju hardverske jedinice proizvoda s digitalnim elementima.

Primjer 8: Mrežni pisač stavlja se na tržište kao hardverski proizvod s digitalnim elementima, a softverski upravljački programi koji su potrebni za slanje dokumenata na ispis, konfiguraciju uređaja i upravljanje njegovim radom stavljaju se na raspolaganje za preuzimanje s internetskih stranica proizvođača. Iako se pisač i upravljački programi isporučuju različitim kanalima, oni zajedno čine jedinstven proizvod s digitalnim elementima jer pisač ne može ispuniti svoju namjenu bez upravljačkih programa.

Primjer 9: Nosivi uređaj za praćenje tjelesne aktivnosti stavljen je na tržište za potrebe mjerenja otkucaja srca i aktivnosti korisnika, dok je za prikaz izmjerenih podataka, pregled povijesti mjerenja i konfiguriranje uređaja potrebna aplikacija za pametni telefon koju stavlja na raspolaganje proizvođač. Iako se aplikacija preuzima zasebno u trgovini aplikacijama, uređaj i aplikacija zajedno čine jedinstven proizvod s digitalnim elementima jer su projektirani i namijenjeni za zajednički rad kako bi se ostvarila funkcionalnost proizvoda s digitalnim elementima.

([8]) Treba podsjetiti i na to da se člankom 4. stavkom 3. proizvođačima omogućuje da na raspolaganje na tržištu stave nedovršeni softver koji nije u skladu s Uredbom, kao što su alfa verzije, beta verzije ili potencijalne verzije za izdavanje, pod uvjetom da se taj softver stavlja na raspolaganje samo na razdoblje potrebno za njegovo ispitivanje i prikupljanje povratnih informacija.

([9]) Valja napomenuti i da za potrebe prava o odgovornosti za proizvode računalni kod sam po sebi nije proizvod te se stoga proizvođači koji stavljaju takav kod na tržište ne mogu smatrati odgovornima na temelju Direktive (EU) 2024/2853 (Direktiva o odgovornosti za proizvode). U uvodnoj izjavi 13. te direktive navedeno je da se „[…] informacije […] ne smatraju proizvodom i stoga se pravila o odgovornosti za proizvode ne bi trebala primjenjivati na sadržaj digitalnih datoteka, kao što su medijske datoteke ili e-knjige ili sâm izvorni programski kod softvera”. To ne isključuje mogućnost odgovornosti proizvođača na temelju nacionalnog odštetnog prava.

2.5. **Podatkovna veza**

26. U članku 2. stavku 1. Akta o kibernetičkoj otpornosti navodi se da se taj akt „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”. Područje primjene Akta o kibernetičkoj otpornosti stoga se ne temelji samo na prisutnosti elektroničkih komponenti, nego na sposobnosti proizvoda s digitalnim elementima da razmjenjuje digitalne informacije.

27. Pojmovi „logička veza” i „fizička veza” definirani su u članku 3., no pojmovi „podatkovna veza” i „digitalni podaci” nisu definirani u Aktu o kibernetičkoj otpornosti. Stoga je korisno protumačiti što se podrazumijeva pod podatkovnom vezom kako bi se pojasnila granica područja primjene Akta o kibernetičkoj otpornosti. Ta je granica posebno važna kako bi se razlikovali proizvodi s digitalnim elementima koji se samo oslanjaju na električne signale od onih koji sudjeluju u digitalnoj komunikaciji i koji su stoga izloženi kibernetičkosigurnosnim rizicima.

28. U najjednostavnijem smislu, podatkovna veza podrazumijeva prijenos informacija u binarnom obliku, tj. kao slijed nula i jedinica. Jednostavno uključivanje i isključivanje izlaza (tj. prebacivanje između nule i jedinice) samo po sebi ne predstavlja podatkovnu vezu ako ta stanja nisu namijenjena prikazu podataka ili ih ne očitava digitalni ulaz. Da bi postojala podatkovna veza, izvorni uređaj mora binarna stanja namjerno kodirati kao informacije te se ona moraju moći dekodirati kao informacije na odredištu. Drugim riječima, mora postojati pošiljatelj koji namjerno stvara digitalne simbole prema utvrđenoj shemi i primatelj koji te simbole može tumačiti kao podatke. Ako se električni ili elektronički signali upotrebljavaju isključivo za pokretanje ili napajanje funkcije, bez prenošenja digitalno kodiranih informacija, ne postoji podatkovna veza u smislu Akta o kibernetičkoj otpornosti te stoga proizvod s digitalnim elementima nije obuhvaćen područjem primjene članka 2. stavka 1.

2.6. **Složeni sustavi**

29. Proizvodi s digitalnim elementima obuhvaćeni područjem primjene Akta o kibernetičkoj otpornosti mogu se sastojati od pojedinačnih uređaja ili softverskih komponenti, ali i od složenih sustava, uključujući sustave koji se sastoje od više hardverskih i softverskih elemenata koji rade zajedno u svrhu obavljanja određene funkcije. Ako je takav sustav stavljen na tržište kao jedinstveni proizvod s digitalnim elementima, riječ je o proizvodu s digitalnim elementima u smislu Akta o kibernetičkoj otpornosti.

30. Takve složene sustave često karakteriziraju dugi ciklusi projektiranja i razvoja, s ugovorima koji su možda potpisani prije početka primjene Akta o kibernetičkoj otpornosti, produljenim radnim vijekom trajanja i visokim stupnjem tehničke i organizacijske složenosti. Ti sustavi, koji se stavljaju na tržište nakon početka primjene Akta o kibernetičkoj otpornosti, mogu se oslanjati na komponente stavljene na tržište prije početka primjene tog akta, na uspostavljenu arhitekturu ili na često korištene standarde interoperabilnosti, uključujući standarde iz drugog zakonodavstva EU-a ili sektorskih okvira. Zbog toga određene tehničke značajke tih sustava može biti teško ili nerazmjerno izmijeniti a da to ne utječe na njihovu namjenu, sigurnost, pouzdanost ili interoperabilnost s postojećom infrastrukturom.

31. Te značajke same po sebi ne isključuju složene sustave iz područja primjene Akta o kibernetičkoj otpornosti. Naprotiv, one pokazuju kako se primjenjuje pristup iz Akta o kibernetičkoj otpornosti koji se temelji na procjeni rizika i koji omogućuje dokazivanje usklađenosti na razne načine ovisno o značajkama i ograničenjima proizvoda s digitalnim elementima u skladu s člankom 13. stavkom 3. tog akta. Te su značajke dio njegove namjene i operativnog konteksta te su stoga relevantne pri ocjenjivanju usklađenosti s bitnim zahtjevima u pogledu kibernetičke sigurnosti („bitni zahtjevi”). Prije svega, u uvodnoj izjavi 55. izričito se priznaje da određeni bitni zahtjevi možda nisu u potpunosti u skladu s prirodom proizvoda s digitalnim elementima. Na primjer, to može biti slučaj ako bi se postizanjem usklađenosti ugrozilo ispunjavanje obveznih zahtjeva interoperabilnosti ili pravilno funkcioniranje sustava.

32. U skladu s tim proizvođači su dužni ukloniti kibernetičkosigurnosne rizike na temelju njihove procjene iz članka 13. stavka 2. Kao što se također objašnjava u uvodnoj izjavi 55., u nekim slučajevima određeni bitni zahtjevi nisu primjenjivi ili ih nije moguće ispuniti provedbom najsuvremenijih sigurnosnih mjera, na primjer zbog namjene

sustava koja iziskuje da proizvod s digitalnim elementima mora biti u interakciji s postojećim ovisnostima ili ispunjavati određene zahtjeve interoperabilnosti. U tim bi slučajevima proizvođači trebali utvrditi i dokumentirati ta posebna ograničenja, procijeniti povezane rizike i provesti odgovarajuće alternativne ili kompenzacijske mjere za ublažavanje rizika kako se ne bi ugrozila sigurnost proizvoda s digitalnim elementima. U tom kontekstu tehnička dokumentacija iz članka 31. te informacije i upute za korisnika iz Priloga II. imaju važnu ulogu u transparentnom opisivanju utvrđenih ograničenja, povezanih kibernetičkosigurnosnih rizika i provedenih mjera za ublažavanje rizika. U skladu s obvezom ažuriranja procjene rizika za vrijeme trajanja razdoblja potpore proizvođači bi osim toga trebali periodično ponovno procjenjivati postoje li i dalje takva ograničenja. Ako se takva ograničenja s vremenom mogu ukinuti ili smanjiti, proizvođači bi trebali na odgovarajući način ažurirati proizvod s digitalnim elementima kako bi mogao dosegnuti odgovarajuću razinu kibernetičke sigurnosti ([10]).

Primjer 10: Proizvođač stavlja na tržište proizvod s digitalnim elementima koji preko mrežnog protokola razmjenjuje podatke s vanjskim sustavima. U okviru primjene bitnih zahtjeva proizvođač na temelju procjene kibernetičkosigurnosnih rizika utvrđuje da je upotreba sigurnog komunikacijskog protokola nužna kako bi se zajamčile povjerljivost i cjelovitost podataka koje proizvod s digitalnim elementima razmjenjuje.

Međutim, njegova namjena uključuje interoperabilnost s postojećim sustavima koji podržavaju samo stariji ili manje siguran protokol. U tim slučajevima proizvođač može primijeniti taj protokol ako je to potrebno za postizanje interoperabilnosti, pod uvjetom da su povezani kibernetičkosigurnosni rizici utvrđeni i ublaženi na drugi način.

Ako je tehnički izvedivo da proizvod s digitalnim elementima podržava i sigurni protokol i manje siguran protokol, od proizvođača se očekuje da primijeni sigurni protokol i omogući njegovu automatsku upotrebu. Manje siguran protokol bio bi dopušten samo ako je to potrebno za interoperabilnost.

Primjer 11: Proizvođač sustava za industrijsku automatizaciju kupuje mikrokontrolere prije početka primjene Akta o kibernetičkoj otpornosti. Proizvođač provodi procjenu kibernetičkosigurnosnih rizika za svoj sustav za industrijsku automatizaciju koji će se staviti na tržište nakon početka primjene Akta o kibernetičkoj otpornosti. Na temelju te procjene kibernetičkosigurnosnih rizika proizvođač ne utvrđuje posebne kibernetičkosigurnosne rizike povezane s upotrebom jednog od tih mikrokontrolera. Proizvođač ga integrira u svoj sustav za industrijsku automatizaciju i osigurava da proizvod s digitalnim elementima u cjelini (sustav za industrijsku automatizaciju) ispunjava bitne zahtjeve.

2.7. **Proizvodi s digitalnim elementima projektirani prije početka primjene Akta o kibernetičkoj otpornosti**

33. U nekim slučajevima proizvođač će nakon što se Akt o kibernetičkoj otpornosti počne primjenjivati 11. prosinca 2027. staviti na tržište jedinice proizvoda s digitalnim elementima proizvedene u skladu s vrstom ili modelom koji je projektiran i razvijen prije datuma početka primjene tog akta. U tim slučajevima nije nužno ponovno projektirati predmetne jedinice proizvoda s digitalnim elementima kako bi se postigla usklađenost s tom uredbom. Proizvođač je dužan provesti procjenu kibernetičkosigurnosnih rizika u skladu s člankom 13. stavkom 2. Akta o kibernetičkoj otpornosti kako bi na temelju namjene i razumno predvidljive upotrebe proizvoda s digitalnim elementima utvrdio koji se bitni zahtjevi iz dijela I. Priloga I. primjenjuju na taj proizvod s digitalnim elementima i kako se ti zahtjevi ispunjavaju.

34. Ako ishod te procjene rizika pokaže da proizvod s digitalnim elementima već uključuje odgovarajuće i djelotvorne sigurnosne mjere za uklanjanje relevantnih rizika, proizvođač se može osloniti na te postojeće mjere kako bi dokazao usklađenost s Aktom o kibernetičkoj otpornosti. Akt o kibernetičkoj otpornosti ne obvezuje proizvođača na uvođenje novih sigurnosnih značajki ili ponovno projektiranje proizvoda s digitalnim elementima ako to nije potrebno za uklanjanje utvrđenih rizika.

([10]) Valja napomenuti da razmatranja utvrđena u ovoj točki mogu biti primjenjiva, ovisno o slučaju, na sve proizvode s digitalnim elementima obuhvaćene područjem primjene Akta o kibernetičkoj otpornosti, a ne samo na „složene sustave”.

35. Međutim, na proizvođača se i dalje primjenjuju obveze utvrđene u Aktu o kibernetičkoj otpornosti. Među ostalim riječ je o obvezi da se osigura da je prije stavljanja proizvoda s digitalnim elementima na tržište proveden primjenjivi postupak ocjenjivanja sukladnosti, da je sastavljena EU izjava o sukladnosti i da je na proizvod stavljena oznaka CE. Usklađenost s tim zahtjevima ne ovisi o tome je li na temelju procjene rizika bilo potrebno ponovno projektirati proizvod s digitalnim elementima. Kad je riječ o proizvodima s digitalnim elementima koji su projektirani prije datuma početka primjene Akta o kibernetičkoj otpornosti, ali su stavljeni na tržište nakon tog datuma, ako proizvođač ne može dokazati kako je procjena rizika uzeta u obzir u fazi projektiranja i razvoja proizvoda s digitalnim elementima, obvezu iz članka 13. stavka 2. trebalo bi tumačiti na način da se njome od proizvođača zahtijeva da provedu procjenu kibernetičkosigurnosnih rizika i na temelju nje dokažu da proizvod s digitalnim elementima ima ugrađene odgovarajuće sigurnosne mjere za smanjenje tih rizika te sprečavanje incidenata i smanjenje njihovih posljedica, među ostalim na zdravlje i sigurnost korisnika.

36. U skladu s tim, proizvodi s digitalnim elementima projektirani prije početka primjene Akta o kibernetičkoj otpornosti mogli bi se staviti na tržište u skladu s tim aktom bez potrebe za ponovnim projektiranjem, pod uvjetom da proizvođač na temelju procjene kibernetičkosigurnosnih rizika i tehničke dokumentacije može dokazati da proizvod s digitalnim elementima postiže odgovarajuću razinu kibernetičke sigurnosti s obzirom na svoju namjenu i razumno predvidljivu upotrebu te da ispunjava bitne zahtjeve u pogledu kibernetičke sigurnosti.

37. Nadalje, korisno je pojasniti primjenu obveza u kontekstu ocjenjivanja sukladnosti za proizvođače proizvoda s digitalnim elementima koji su stavljeni na tržište nakon početka primjene Akta o kibernetičkoj otpornosti, ali su proizvedeni u skladu s vrstom ili modelom koji je projektiran i razvijen prije tog datuma. U skladu s člankom 13. stavkom 12. proizvođač je dužan na temelju odgovarajućeg postupka ocjenjivanja sukladnosti dokazati da je njegov proizvod s digitalnim elementima sukladan s primjenjivim bitnim zahtjevima te u tehničku dokumentaciju proizvoda uključiti dokaze o tome (točka 6. Priloga VII.).

38. Međutim, primjenu takvih zahtjeva treba tumačiti s obzirom na procjenu kibernetičkosigurnosnih rizika i profil kibernetičkosigurnosne rizičnosti proizvoda s digitalnim elementima. Kad je konkretno riječ o proizvodima s digitalnim elementima koji su projektirani prije datuma početka primjene Akta o kibernetičkoj otpornosti (ali stavljeni na tržište nakon tog datuma) i na koje se primjenjuju postupci ocjenjivanja sukladnosti iz članka 32. stavka 1., ako procjena rizika pokaže da proizvod s digitalnim elementima već uključuje odgovarajuće i djelotvorne sigurnosne mjere za uklanjanje rizika tog proizvoda, obvezu dostavljanja dokaza u okviru postupka ocjenjivanja sukladnosti ne bi trebalo tumačiti na način da se njome od proizvođača zahtijeva da dostavi rezultate ispitivanja koji obuhvaćaju izvorne faze projektiranja i razvoja tih proizvoda s digitalnim elementima. To ne bi bilo potrebno jer ne bi doprinijelo povećanju sigurnosti samog proizvoda s digitalnim elementima. Ako su ispitivanja ipak potrebna, od proizvođača se ne očekuje da dostave dokaze o ispitivanjima provedenima na svim inačicama proizvoda, ali mogu za potrebe ispitivanja grupirati proizvode s digitalnim elementima, kao što je dodatno objašnjeno u odjeljku *7.4.* – Ponovna upotreba procjena rizika i dokumentacije o sukladnosti za skupine proizvoda s digitalnim elementima.

39. Međutim, proizvođač bi trebao dostaviti dokaze o provedbi procesa postupanja s ranjivostima utvrđenih u dijelu II. Priloga I., redovito ažurirati svoju procjenu rizika u skladu s člankom 13. stavkom 3. te ispuniti sve druge obveze utvrđene u Aktu o kibernetičkoj otpornosti, među ostalim pružanjem informacija i uputa korisnicima u skladu s člankom 13. stavkom 18.

Primjer 12: Proizvođač stavlja na tržište mikrokontroler koji je projektiran i razvijen prije datuma početka primjene Akta o kibernetičkoj otpornosti. Mikrokontroler je namijenjen integraciji u niz elektroničkih proizvoda s digitalnim elementima, uključujući proizvode s digitalnim elementima s funkcijama povezivosti.

Prije stavljanja novih jedinica mikrokontrolera na tržište nakon početka primjene Akta o kibernetičkoj otpornosti proizvođač provodi procjenu kibernetičkosigurnosnih rizika u skladu s člankom 13. stavkom 2. Na temelju namjene mikrokontrolera i njegove razumno predvidljive upotrebe proizvođač utvrđuje relevantne kibernetičkosigurnosne rizike, kao što su neovlašteni pristup, manipulacija softverom ili podacima i kriva upotreba dostupnih sučelja.

Ishod procjene rizika pokazuje da mikrokontroler, kako je izvorno projektiran, već uključuje odgovarajuće i djelotvorne sigurnosne mjere za uklanjanje utvrđenih rizika. Proizvođač stoga zaključuje da proizvod s digitalnim elementima ispunjava relevantne bitne zahtjeve iz dijela I. Priloga I. i da nije potrebno ponovno projektirati proizvod niti uvesti dodatne sigurnosne funkcionalnosti.

Ako nije moguće dokazati kako je procjena kibernetičkosigurnosnih rizika uzeta u obzir u izvornoj fazi projektiranja i razvoja, proizvođač dokumentira trenutačnu procjenu tog rizika i objašnjava kako se proizvodom kako je trenutačno projektiran i postojećim mjerama ublažavaju utvrđeni rizici. Proizvođač nije dužan ponovno izraditi dokumentaciju koja se odnosi na izvorno projektiranje i ispitivanje jer to ne bi doprinijelo poboljšanju kibernetičke sigurnosti proizvoda s digitalnim elementima. Ako se nekoliko inačica mikrokontrolera temelji na istom projektu i imaju isti profil kibernetičkosigurnosne rizičnosti, proizvođač se može osloniti i na reprezentativne dokaze koji obuhvaćaju odgovarajuću skupinu proizvoda.

*Proizvođač osigurava i ispunjavanje zahtjeva u pogledu postupanja s ranjivostima utvrđenih u dijelu II. Priloga I., među ostalim provedbom postupaka za razmatranje i otklanjanje ranjivosti te redovitim preispitivanjem procjene kibernetičkosigurnosnih rizika u skladu s članku*m *13. stavkom 3.*

U tim se okolnostima mikrokontroler projektiran prije datuma početka primjene Akta o kibernetičkoj otpornosti može staviti na tržište bez potrebe za ponovnim projektiranjem, pod uvjetom da proizvođač na temelju procjene kibernetičkosigurnosnih rizika i tehničke dokumentacije može dokazati da proizvod postiže odgovarajuću razinu kibernetičke sigurnosti s obzirom na svoju namjenu i razumno predvidljivu upotrebu te da ispunjava primjenjive bitne zahtjeve.

3. **BESPLATNI SOFTVER OTVORENOG KODA**

40. Kao što je navedeno u odjeljku *2.1.* – Stavljanje na tržište, Akt o kibernetičkoj otpornosti primjenjuje se na proizvode s digitalnim elementima koji se prvi put stavljaju na raspolaganje na tržištu EU-a u okviru trgovačke djelatnosti („stavljanje na tržište"), kao i na sve kasnije slučajeve u kojima se taj isti proizvod s digitalnim elementima stavlja na raspolaganje na tržištu. U Plavom vodiču (točka 2.2.) pojašnjava se da „trgovačku djelatnost" treba tumačiti kao isporuku robe u kontekstu poslovanja, uz plaćanje ili besplatno, i da se ona može procijeniti samo posebno za svaki pojedini slučaj uzimajući u obzir redovitost isporuke, značajke proizvoda, namjere dobavljača itd.

41. Isporuku u okviru trgovačke djelatnosti karakterizira niz okolnosti koje su podrobno opisane u Plavom vodiču i navedene u uvodnoj izjavi 15. Akta o kibernetičkoj otpornosti. One mogu uključivati izravno naplaćivanje cijene, ali 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" (uvodna izjava 15.) ([11]).

42. Međutim, u Aktu o kibernetičkoj otpornosti prepoznaju se posebnosti raznih načina razvoja i objavljivanja „besplatnog softvera otvorenog koda" (FOSS) te se navode određene smjernice za utvrđivanje je li FOSS proizvod s digitalnim elementima koji se stavlja na tržište (tj. u okviru trgovačke djelatnosti) u smislu Akta o kibernetičkoj otpornosti. Kao što je to objašnjeno u uvodnoj izjavi 18. „[s]ame okolnosti u kojima je proizvod s digitalnim elementima razvijen, ili način financiranja njegova razvoja, ne bi […] trebalo uzimati u obzir pri određivanju komercijalne ili nekomercijalne prirode te djelatnosti". Točnije, „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".

([11]) Treba podsjetiti i na to da, iako se proizvodi s digitalnim elementima često unovčuju (među ostalim) na temelju obrade osobnih podataka, zaštita osobnih podataka temeljno je pravo i stoga se osobni podaci ne mogu smatrati robom, kako je navedeno u uvodnoj izjavi 24. Direktive (EU) 2019/770 Europskog parlamenta i Vijeća od 20. svibnja 2019. o određenim aspektima ugovora o isporuci digitalnog sadržaja i digitalnih usluga, *SL L 136, 22.5.2019., str. 1.*, ELI: http://data.europa.eu/eli/dir/2019/770/oj.

43. Stoga je korisno (i) pojasniti što je FOSS; (ii) utvrditi situacije u kojima se smatra da je za njega odgovorna fizička ili pravna osoba; i (iii) navesti primjere koji će dionicima pomoći da razumiju kad se distribucija FOSS-a smatra stavljanjem na tržište. Ako se FOSS ne stavlja na tržište, nije obuhvaćen područjem primjene Akta o kibernetičkoj otpornosti, osim ako je subjekt koji ga objavljuje pravna osoba koja odgovara definiciji „upravitelja softvera otvorenog koda" (dalje u tekstu „upravitelj") iz članka 3. točke 14. U tom se slučaju na njega primjenjuju samo obveze utvrđene u članku 24.

44. U članku 3. točki 48. FOSS je definiran kao „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". Iako se u ovim smjernicama ne utvrđuju konkretne besplatne licencije otvorenog koda koje su u skladu s definicijom utvrđenom u članku 3. točki 48., iz teksta te odredbe proizlazi da se samo softver koji kumulativno ispunjava oba uvjeta smatra FOSS-om za potrebe Akta o kibernetičkoj otpornosti: (i) softver mora biti stavljen na raspolaganje na temelju besplatne licencije otvorenog koda kojom se dodjeljuju sva prava iz članka 3. točke 48.; i (ii) njegov izvorni kod mora se otvoreno dijeliti.

45. Zahtjev da se licencijom predvidi da softver bude „slobodno dostupan, upotrebljiv, promjenjiv i preraspodjeljiv" ukazuje na tradicionalno shvaćanje FOSS-a, odnosno da korisnici moraju moći pristupiti izvornom kodu, upotrebljavati ga bez nepotrebnih ograničenja, mijenjati ga i redistribuirati izvorne ili izmijenjene verzije. Pristup izvornom kodu stoga je nužan preduvjet za ostvarivanje drugih prava: bez pristupa izvornom kodu u praksi nije moguće izmijeniti softver ili ga ponovno upotrijebiti na smislen način.

46. Međutim, u članku 3. točki 48. ne navode se samo uvjeti licencije, već se njime izričito propisuje da se izvorni kod „otvoreno dijeli". Izraz „otvoreno dijeli" upućuje na to da izvorni kod mora biti javno dostupan („više u lancu opskrbe" ili „niže u lancu opskrbe"), a ne samo ograničeno ili uvjetno stavljen na raspolaganje. U skladu s tim, softver koji se stavlja na raspolaganje na temelju besplatne licencije otvorenog koda, ali čiji se izvorni kod dijeli (ili se smije dijeliti) samo s korisnicima koji plaćaju ili s ograničenom skupinom korisnika, ne smatra se FOSS-om u smislu članka 3. točke 48. Stoga bi se za potrebe Akta o kibernetičkoj otpornosti FOSS-om trebao smatrati samo softver čiji je izvorni kod javno dostupan i koji je licenciran na temelju besplatne licencije otvorenog koda kojom se dodjeljuju sva prava iz članka 3. točke 48.

3.1. **Utvrđivanje odgovornosti za besplatni softver otvorenog koda**

47. Aktom o kibernetičkoj otpornosti glavne odgovornosti dodjeljuju se gospodarskim subjektima koji isporučuju proizvode s digitalnim elementima na tržištu EU-a. U njemu se proizvođač definira kao fizička ili pravna osoba koja isporučuje proizvod s digitalnim elementima pod svojim imenom ili žigom i koja to čini u okviru trgovačke djelatnosti (odnosno stavlja ga na tržište). Slično tomu, uvoznik je fizička ili pravna osoba s poslovnim nastanom u EU-u koja isporučuje proizvod s digitalnim elementima osobe s poslovnim nastanom izvan EU-a i to čini u okviru trgovačke djelatnosti (odnosno stavlja ga na tržište). Obveze upravitelja primjenjuju se na pravnu osobu koja isporučuje FOSS namijenjen komercijalnim djelatnostima ([12]), ali ga ne stavlja na tržište u smislu Akta o kibernetičkoj otpornosti.

48. Stoga, kako bi se utvrdilo stavlja li fizička ili pravna osoba FOSS na tržište EU-a, prvo je potrebno utvrditi isporučuje li ta fizička ili pravna osoba doista FOSS. Kako bi se pravilno utvrdile obveze koje se primjenjuju na temelju Akta o kibernetičkoj otpornosti, ključno je utvrditi isporučuje li fizička ili pravna osoba doista FOSS. Naime, u smislu uvodne izjave 18., Akt o kibernetičkoj otpornosti ne primjenjuje se na fizičke ili pravne osobe koje izvornim kodom doprinose proizvodima s digitalnim elementima koji se smatraju FOSS-om i za koje nisu odgovorne.

([12]) To je nužan, ali ne i dovoljan uvjet da bi se pravna osoba smatrala upraviteljem softvera otvorenog koda jer se definicijom iz članka 3. točke 14. utvrđuju dodatni uvjeti koji moraju biti ispunjeni kako bi se pravna osoba mogla smatrati upraviteljem.

49. S obzirom na posebnosti razvoja FOSS-a, koji često uključuje više doprinositelja, decentralizirane modele suradnje i odvajanje pružanja doprinosa od donošenja odluka, korisno je pojasniti da se smatra da je FOSS „pod odgovornošću” fizičkih ili pravnih osoba koje ga objavljuju i imaju primarnu kontrolu nad odlukama o razvoju, izdanjima i distribuciji (često se nazivaju „održavatelji”). „Doprinositeljima” se smatraju osobe koje doprinose izvornim kodom, ali ne kontroliraju izdanja i planove niti donose odluke o upravljanju; u tim slučajevima FOSS nije pod njihovom odgovornošću, iako su mu doprinijeli kodom. Samo postojanje tehničkih ovlasti, kao što je ovlast predaje koda u repozitorij, nije dovoljno da bi se utvrdilo da je FOSS pod odgovornošću te osobe; odgovornost snose oni koji objavljuju i kontroliraju FOSS.

Primjer 13: Razvojni programer ili zaposlenik poduzeća podnosi zahtjev za povlačenje ili spajanje izmjena koje sadržavaju sigurnosnu zakrpu ili novu funkcionalnost za projekt FOSS-a. Održavatelji projekta pregledavaju i prihvaćaju izmjene te predaju kod u glavni repozitorij, a zatim ga uključuju u novo izdanje. U tom je scenariju osoba koja je podnijela zahtjev za povlačenje „doprinositelj” i na nju se ne primjenjuje Akt o kibernetičkoj otpornosti. Iako je ta osoba pridonijela softveru izvornim kodom, ona nema primarnu kontrolu nad odlukama o razvoju, izdanjima ili distribuciji.

3.2. **Utvrđivanje je li besplatni softver otvorenog koda stavljen na tržište EU-a**

50. Nakon što se utvrdi da je za FOSS odgovorna fizička ili pravna osoba, potrebno je utvrditi isporučuje li ga ta osoba u okviru trgovačke djelatnosti, odnosno stavlja li ga na tržište.

3.2.1. *Naplaćivanje cijene*

51. Ako fizička ili pravna osoba koja isporučuje FOSS naplaćuje cijenu za sam softver (npr. naplaćuje cijenu za unaprijed kompilirane binarne datoteke), ta osoba stavlja proizvod s digitalnim elementima na tržište. Osoba koja stavlja FOSS na tržište stoga je proizvođač prema Aktu o kibernetičkoj otpornosti.

52. Proizvođači FOSS-a često besplatno isporučuju verzije tog softvera (koje se često nazivaju verzijama „za zajednicu”), čija je baza koda (gotovo) identična plaćenoj verziji. Međutim, ti proizvodi s digitalnim elementima različiti su proizvodi: plaćena verzija na neki se način unovčuje (npr. naplatom cijene ili na drugi način kako je opisano u ovom odjeljku) i stoga se smatra stavljenom na tržište, zbog čega nastaju obveze proizvođača. Besplatna verzija (ili verzija za zajednicu) ne unovčuje se i stoga se za potrebe Akta o kibernetičkoj otpornosti ne smatra da je stavljena na tržište. To vrijedi i ako je plaćena verzija „poboljšana” komercijalna verzija u kojoj je proširena baza koda besplatne verzije ili ako se putem nje ta verzija ugrađuje u širi proizvod s digitalnim elementima (npr. kao u slučaju modela „otvorene jezgre”).

53. Ako je osoba koja isporučuje verziju za zajednicu pravna osoba, na nju se također primjenjuju obveze upravitelja u pogledu verzije koju isporučuje besplatno (verzija za zajednicu). Ako je subjekt fizička osoba, besplatna verzija (verzija za zajednicu) nije obuhvaćena područjem primjene Akta o kibernetičkoj otpornosti.

3.2.2. *Unovčenje drugih usluga ili uvjetovanje upotrebe obradom osobnih podataka*

54. Fizička ili pravna osoba koja objavljuje FOSS može ga ujedno staviti na tržište (tj. isporučiti u okviru trgovačke djelatnosti) ako stavlja na raspolaganje softver kojim unovčuje druge proizvode s digitalnim elementima ili usluge ili ako uvjetuje upotrebu softvera obradom osobnih podataka u svrhe koje nisu isključivo poboljšanje sigurnosti, kompatibilnosti ili interoperabilnosti softvera.

Primjer 14: Fizička ili pravna osoba objavljuje besplatnu aplikaciju otvorenog koda za trgovanje na internetu. Aplikacija je dostupna besplatno i omogućuje korisnicima da na njoj kupe robu ili usluge. Omogućuje osobi koja ju je objavila da unovči druge proizvode s digitalnim elementima i usluge koje se na njoj nude (npr. na temelju oglasa, provizija ili pretplata). Stoga se smatra da je aplikacija stavljena na tržište u okviru trgovačke djelatnosti.

Primjer 15: Fizička ili pravna osoba objavljuje besplatan VPN otvorenog koda. Aplikacija je dostupna besplatno, ali korisnicima omogućuje da plate pristup dodatnim poslužiteljima ili namjenskim IP adresama. Aplikacija omogućuje toj osobi da unovči druge usluge koje se nude na njoj, zbog čega se smatra da je stavljena na tržište u okviru trgovačke djelatnosti.

Primjer 16: Fizička ili pravna osoba objavljuje besplatnu aplikaciju otvorenog koda za praćenje tjelesne aktivnosti. Aplikacija je dostupna besplatno, ali njezina je upotreba uvjetovana obradom osobnih podataka korisnika u svrhe kao što su ciljano oglašavanje ili analitika koje nisu povezane sa sigurnošću, kompatibilnošću ili interoperabilnošću softvera. Budući da je obrada takvih podataka uvjet za upotrebu aplikacije, smatra se da se aplikacija stavlja na tržište u okviru trgovačke djelatnosti.

3.2.3. *Usluge podrške*

55. Činjenica da fizička ili pravna osoba koja objavljuje FOSS nudi i s njim povezane plaćene usluge podrške sama po sebi ne znači da se proizvod s digitalnim elementima isporučuje u okviru trgovačke djelatnosti. Usluge podrške mogu uključivati na primjer savjetovanje, osposobljavanje ili profesionalne usluge povezane s korisnikovom upotrebom, dokumentacijom, konfiguracijom i uvođenjem softvera.

56. Odlučujući je čimbenik to je li pristup samom FOSS-u (tj. pružanje proizvoda s digitalnim elementima), uključujući njegovo održavanje, uvjetovan plaćanjem naknade ili je riječ samo o ponudi profesionalnih usluga povezanih sa slobodno dostupnim proizvodom s digitalnim elementima, u smislu uvodne izjave 18. Akta o kibernetičkoj otpornosti („pružanje proizvoda s digitalnim elementima koji se smatraju besplatnim softverom otvorenog koda koje njihovi proizvođači ne unovčuju ne bi trebalo smatrati komercijalnom djelatnošću"). Ako se FOSS može besplatno preuzeti i instalirati, a korisnici mogu odlučiti žele li odvojeno kupiti profesionalne usluge, smatra se da FOSS nije stavljen na tržište.

57. S druge strane, u nekim je slučajevima pristup određenoj verziji proizvoda s digitalnim elementima, uključujući određene koristi kao što su tehnička pomoć ili optimizacija performansi, omogućen samo uz plaćanje naknade. Takvo stavljanje na raspolaganje predstavlja unovčenu isporuku proizvoda s digitalnim elementima u okviru trgovačke djelatnosti i stoga se taj proizvod smatra stavljenim na tržište. To uključuje slučajeve u kojima se plaćeno izdanje ili poslovna verzija stavlja na raspolaganje na temelju trgovačkog sporazuma, neovisno o tome je li funkcionalno istovjetan softver dostupan i besplatno na temelju besplatne licencije otvorenog koda.

Primjer 17: Fizička ili pravna osoba objavljuje besplatan operativni sustav otvorenog koda, ali nudi i plaćenu verziju tog operativnog sustava koja uključuje usluge podrške, kao što su tehnička pomoć ili optimizacija performansi. Plaćena verzija operativnog sustava smatra se stavljenom na tržište u okviru trgovačke djelatnosti.

Primjer 18: Fizička ili pravna osoba objavljuje besplatan alat otvorenog koda za naredbeni redak. Alat je slobodno dostupan i svatko ga može preuzeti i instalirati. Ta fizička ili pravna osoba zasebno nudi profesionalne usluge, kao što su neobvezne savjetodavne usluge za osposobljavanje korisnika i pružanje podrške pri instalaciji i upotrebi alata. Taj se FOSS ne smatra stavljenim na tržište u smislu Akta o kibernetičkoj otpornosti.

58. Kad je konkretno riječ o fizičkim osobama koje objavljuju FOSS, pružanje tehničke pomoći izravno povezane s pristupom proizvodu s digitalnim elementima i dalje se ne bi smatralo komercijalnom djelatnošću ako, kao što je navedeno u uvodnoj izjavi 15. Akta o kibernetičkoj otpornosti, naplaćena cijena služi samo za povrat stvarnih troškova. Ti stvarni troškovi uključuju niz troškova povezanih s projektiranjem, razvojem i održavanjem softvera, uključujući razumne životne troškove osobe. Stoga se samo na temelju činjenice da fizička osoba koja objavljuje FOSS ujedno nudi tehničku pomoć kako bi pokrila svoje troškove i dobila pravednu naknadu ne može smatrati da ta osoba stavlja softver na tržište EU-a.

59. Ne smatra se da fizička ili pravna osoba koja nudi tehničku pomoć povezanu s FOSS-om koji nije pod njezinom odgovornošću stavlja taj softver na tržište, osim ako, u skladu s člankom 22., ta osoba bitno izmijeni FOSS u okviru pružanja takve pomoći.

Primjer 19: Pružatelj usluga ne objavljuje FOSS, ali pomaže kupcu da ga instalira na poslužitelj u svojim poslovnim prostorima. To čini bez bitne izmjene tog FOSS-a. Stoga se ne smatra da pružatelj usluga stavlja FOSS na tržište.

3.2.4. *Donacije*

60. Fizičke ili pravne osobe koje objavljuju projekte FOSS-a redovito u njih uključuju načine na koje korisnici tog softvera mogu dobrovoljno donirati novac kako bi zahvalili izdavačima projekta i osigurali da projekt bude aktivan.

61. Kao što je navedeno u uvodnoj izjavi 15. Akta o kibernetičkoj otpornosti, „[p]rihvaćanje donacija bez namjere ostvarivanja dobiti ne bi se trebalo smatrati komercijalnom djelatnošću". Uključivanje poveznice na platformu za donaciju ili slične alate za prikupljanje donacija ne bi samo po sebi trebalo smatrati namjerom ostvarivanja dobiti, čak i ako iznos prikupljen donacijama premašuje troškove projektiranja, razvoja i pružanja proizvoda s digitalnim elementima. To uključuje razumnu naknadu za doprinositelje koje zapošljava pravna osoba i/ili razumne životne troškove fizičke osobe. Donacije po svojoj prirodi variraju tijekom vremena te je stoga potreban određeni stupanj fleksibilnosti pri procjeni toga smatra li se da je FOSS koji je unovčen isključivo na temelju donacija stavljen na tržište. Stoga nije vjerojatno da će se FOSS koji se financira samo donacijama smatrati stavljenim na tržište u smislu Akta o kibernetičkoj otpornosti.

Primjer 20: Fizička ili pravna osoba objavljuje FOSS u javnom internetskom repozitoriju, čime svima omogućuje da ga preuzimaju, upotrebljavaju, mijenjaju i redistribuiraju na temelju besplatne licencije otvorenog koda. Izdavač poziva korisnike da na platformi za donacije dobrovoljno doniraju sredstva kako bi podržali kontinuirani razvoj i održavanje projekta. Pristup softveru, njegovu izvornom kodu i njegovim ažuriranjima nije uvjetovan donacijom. Taj se FOSS ne smatra isporučenim u okviru trgovačke djelatnosti i ne smatra se stavljenim na tržište u smislu Akta o kibernetičkoj otpornosti.

62. Međutim, postoje slučajevi u kojima se može smatrati da je FOSS koji se financira donacijama stavljen na tržište. O takvoj situaciji može biti riječ ako su, na temelju ukupne procjene okolnosti, donacije zapravo istovjetne naplaćivanju cijene za pristup proizvodu s digitalnim elementima ili nekim njegovim funkcionalnostima. To konkretno može biti slučaj ako je pristup FOSS-u, njegovim osnovnim funkcionalnostima ili ažuriranjima u praksi uvjetovan donacijom ili ako su donacije povezane s ugovornim pogodnostima ili ekskluzivnim prednostima koje nadilaze one za članove zajednice.

Primjer 21: Fizička ili pravna osoba objavljuje softverski proizvod s digitalnim elementima na temelju besplatne licencije otvorenog koda, ali omogućuje preuzimanje izdanja i sigurnosnih ažuriranja samo korisnicima koji daju donaciju. Korisnici koji ne daju donaciju nemaju pristup trenutačnoj verziji softvera.

U tom su slučaju donacije zapravo uvjet za pristup proizvodu s digitalnim elementima, pa se smatraju naplatom cijene. Taj se FOSS stoga smatra stavljenim na tržište u smislu Akta o kibernetičkoj otpornosti.

Primjer 22: Fizička ili pravna osoba objavljuje izvorni kod FOSS-a, ali unaprijed kompilirane binarne datoteke, redovita ažuriranja i zajamčene sigurnosne popravke stavlja na raspolaganje samo donatorima. U tom su slučaju donacije povezane s pristupom ključnim aspektima proizvoda s digitalnim elementima te se smatraju naknadom za isporuku tog proizvoda. Taj se FOSS stoga smatra stavljenim na tržište u okviru trgovačke djelatnosti.

3.2.5. *Financiranje besplatnog softvera otvorenog koda*

63. Činjenica da je treća strana platila, sponzorirala ili na neki drugi način financirala razvoj FOSS-a sama po sebi nije dovoljna za utvrđivanje je li taj FOSS stavljen na tržište. Uobičajena je praksa u ekosustavu FOSS-a da razvojni programeri, zaklade ili zajednice primaju financijska sredstva od poduzeća, javnih tijela ili drugih sponzora za rad na posebnim značajkama, ispravljanju pogrešaka ili održavanju važnih komponenti. Ta se financijska sredstva mogu dodijeliti na više načina, na primjer u obliku bespovratnih sredstava, u okviru programa nagrađivanja pronalaska pogrešaka („bug bounty"), u obliku sponzorstava, na temelju ugovora o uslugama ili u okviru plaćenog razvojnog rada.

64. Kao što je već navedeno, u uvodnoj izjavi 18. Akta o kibernetičkoj otpornosti pojašnjava se da same okolnosti u kojima je proizvod s digitalnim elementima razvijen ili način financiranja njegova razvoja ne bi trebalo uzimati u obzir pri određivanju komercijalne prirode te djelatnosti.

65. Stoga, ako se FOSS otvoreno dijeli i ako mu korisnici mogu slobodno pristupiti, upotrebljavati ga, mijenjati i redistribuirati, činjenica da je komercijalni subjekt možda financirao taj projekt ne bi trebala imati ulogu u utvrđivanju toga stavlja li se softver na tržište. Zapravo, ako taj FOSS nije na neki drugi način unovčen, ne smatra se stavljenim na tržište. Ako poduzeće koje je financiralo razvoj FOSS-a (ili bilo koje drugo poduzeće) integrira FOSS u svoj proizvod s digitalnim elementima, ono mora postupati s dužnom pažnjom u skladu s člankom 13. stavkom 5. Akta o kibernetičkoj otpornosti.

Primjer 23: Razvojni programer objavljuje projekt FOSS-a i aktivno ga održava. Proizvođač A traži od razvojnog programera da doda posebnu značajku za taj FOSS i financira taj razvoj. Razvojni programer dodaje tu značajku u bazu koda FOSS-a i otvoreno dijeli FOSS kako bi mu svi mogli slobodno pristupiti, upotrebljavati ga, mijenjati i redistribuirati. Ne smatra se da je razvojni programer stavio taj FOSS na tržište. Ako proizvođač integrira FOSS u svoj proizvod s digitalnim elementima, mora postupati s dužnom pažnjom u skladu s člankom 13. stavkom 5.

3.2.6. *Neprofitni subjekti ustrojeni radi postizanja neprofitnih ciljeva*

66. Ako je pravna osoba koja objavljuje FOSS neprofitna organizacija „ustrojena na način kojim se osigurava da se sva zarada nakon troškova upotrebljava za postizanje neprofitnih ciljeva” (uvodna izjava 18. Akta o kibernetičkoj otpornosti), FOSS koji objavljuje ne smatra se stavljenim na tržište. Ako ta pravna osoba odgovara definiciji „upravitelja”, na nju se primjenjuju odgovarajuće obveze (članak 24. Akta o kibernetičkoj otpornosti).

Primjer 24: Pravna osoba objavljuje besplatan preglednik otvorenog koda koji se izravno unovčuje na temelju partnerstava s tražilicama, ali sva se njezina zarada nakon troškova upotrebljava za neprofitne ciljeve. Preglednik se ne smatra stavljenim na tržište u smislu Akta o kibernetičkoj otpornosti. Na pravnu osobu koja ga objavljuje primjenjuju se obveze za upravitelje.

3.2.7. *Integracija koju provode drugi proizvođači*

67. U nekim slučajevima FOSS objavljuje fizička ili pravna osoba koja se može jasno identificirati, ali taj je FOSS „namijenjen[…] tome da [ga] drugi proizvođači integriraju u vlastite proizvode s digitalnim elementima”. U tim se slučajevima taj FOSS ne smatra stavljenim na tržište EU-a, osim ako ga unovčuje i osoba koja ga objavljuje (tj. izvorni proizvođač), u skladu s prethodnim odjeljcima ovih smjernica.

68. Ako taj FOSS nije stavljen na tržište, na pravnu osobu koja ga objavljuje primjenjivale bi se obveze upravitelja ako pruža kontinuiranu potporu, u skladu s definicijom pojma „upravitelj”.

Primjer 25: Pravna osoba objavljuje knjižnicu FOSS-a za izradu korisničkih sučelja. Ne unovčuje isporuku te knjižnice, nego je integrira u jedan od svojih proizvoda s digitalnim elementima (koji se zatim stavlja na tržište). Knjižnica se ne smatra stavljenom na tržište u smislu Akta o kibernetičkoj otpornosti, ali je namijenjena za integraciju u proizvode s digitalnim elementima. Pravna osoba koja je objavljuje njezin je upravitelj.

Primjer 26: Pravna osoba stavlja operativni sustav na tržište i objavljuje knjižnice FOSS-a koje služe kao referentne implementacije za korisnike tog operativnog sustava. Pravna osoba ne unovčuje knjižnice FOSS-a, koje su namijenjene za integraciju u druge proizvode s digitalnim elementima. Pravna osoba koja ih objavljuje upravitelj je tih knjižnica FOSS-a.

3.3. **Upravitelji softvera otvorenog koda**

69. 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 [Akta o kibernetičkoj otpornosti]” (uvodna izjava 19. Akta o kibernetičkoj otpornosti), tim se aktom uvodi nova pravna kategorija „upravitelj softvera otvorenog koda”.

70. U nekim slučajevima FOSS objavljuje, ali ga ne stavlja na raspolaganje na tržištu u smislu Akta o kibernetičkoj otpornosti pravna osoba „čija je svrha ili cilj sustavno pružati kontinuiranu potporu za razvoj [FOSS-a] […] namijenjen[og] […] komercijalnim djelatnostima […] te koja osigurava održivost tih proizvoda” (članak 3. točka 14. Akta o kibernetičkoj otpornosti). U tim se slučajevima na tu pravnu osobu primjenjuju obveze upravitelja.

71. Upravitelj je definiran kao „pravna osoba koja nije proizvođač” jer je proizvođač po definiciji fizička ili pravna osoba koja stavlja proizvode s digitalnim elementima na tržište pod svojim imenom ili žigom. Pravna osoba može biti upravitelj samo proizvoda s digitalnim elementima koji se smatraju FOSS-om i koji se objavljuju, ali se ne stavljaju na raspolaganje na tržištu u smislu Akta o kibernetičkoj otpornosti. Pojam upravitelja stoga se primjenjuje na posebne slučajeve FOSS-a koji „su u konačnici namijenjeni komercijalnim djelatnostima, kao što su integracija u komercijalne usluge ili u unovčene proizvode s digitalnim elementima” (uvodna izjava 19. Akta o kibernetičkoj otpornosti ([13])), ali nisu stavljeni na raspolaganje na tržištu u smislu tog akta, i za koje pravna osoba koja objavljuje FOSS sustavno pruža potporu.

72. Činjenica da je pravna osoba upravitelj određenog FOSS-a ne znači da je ona nužno upravitelj i drugog FOSS-a koji objavljuje. Slično tomu, to što je pravna osoba proizvođač određenog FOSS-a ne znači da ona možda nije upravitelj drugog FOSS-a. To uključuje pružanje verzija istog FOSS-a namijenjenih „zajednici”, kako je opisano u odjeljku *3.2.1.* – Naplaćivanje cijene.

73. Pravna osoba tako može istodobno biti upravitelj jednog FOSS-a (za koji upravitelj sustavno pruža kontinuiranu potporu i osigurava održivost softvera) i proizvođač drugog FOSS-a (koji stavlja na tržište). Drugim riječima, isti pravni subjekt može biti obvezan obavljati razne uloge u okviru različitih projekata FOSS-a.

74. Pravna osoba će za svaki pojedini FOSS koji objavi morati utvrditi smatra li se da je taj FOSS stavljen na tržište u smislu Akta o kibernetičkoj otpornosti. Ako da, pravni subjekt je proizvođač softvera. Ako se FOSS ne smatra stavljenim na tržište, pravna osoba može biti njegov upravitelj ako je softver namijenjen komercijalnim djelatnostima i ako ga pravna osoba održava u skladu s definicijom upravitelja ([14]).

3.3.1. *Kontinuirana potpora i osiguravanje održivosti FOSS-a*

75. U uvodnoj izjavi 19. objašnjava se da pružanje kontinuirane potpore razvoju proizvoda s digitalnim elementima može uključivati (među ostalim): (i) smještaj na poslužitelju i upravljanje platformama za suradnju u razvoju softvera; (ii) smještaj izvornog koda ili softvera na poslužitelju; (iii) upravljanje ili raspolaganje proizvodima s digitalnim elementima koji se smatraju FOSS-om; i (iv) upravljanje razvojem takvih proizvoda s digitalnim elementima.

76. O takvoj situaciji može biti riječ, na primjer, ako pravni subjekt koji razvija FOSS za potrebe integracije u vlastite proizvode s digitalnim elementima i zatim ga objavljuje bez stavljanja na tržište. O tome se govori i u odjeljku *3.2.7.* – Integracija koju provode drugi proizvođači. U tom slučaju pravni subjekt nije proizvođač softvera, ali može biti njegov upravitelj. Osim toga, kako je objašnjeno i u prethodnim odjeljcima, pravni subjekt koji objavljuje besplatnu verziju (ili verziju za zajednicu) i unovčenu verziju istog FOSS-a smatra se upraviteljem besplatne verzije (ili verzije za zajednicu) i proizvođačem unovčene verzije.

77. Slično tomu, pravni subjekt koji unovčuje FOSS, ali je neprofitni subjekt čija se zarada nakon troškova upotrebljava za postizanje neprofitnih ciljeva (i stoga se njegov FOSS ne stavlja na tržište u smislu Akta o kibernetičkoj otpornosti, kako je navedeno u odjeljku *3.2.6.* – Neprofitni subjekti), smatra se upraviteljem FOSS-a koji objavljuje.

78. Nadalje, određene zaklade nude platforme za suradnju s raznim oblicima upravljanja koje proizvođačima omogućuju da redovito doprinose razvoju FOSS-a i/ili koje proizvođači redovito financiraju. Takve zaklade treba smatrati upraviteljima konkretnog FOSS-a namijenjenog komercijalnim djelatnostima za koji zaklada pruža kontinuiranu potporu. Međutim, kao što je objašnjeno u odjeljku *3.3.* – Upravitelji softvera otvorenog koda, na takvu se zakladu ne mogu primjenjivati obveze na temelju Akta o kibernetičkoj otpornosti za drugi konkretni FOSS koji je smješten na njezinu poslužitelju ako ne pruža sustavnu potporu tom konkretnom FOSS-u, ne osigurava njegovu održivost i/ili ako taj konkretni softver nije namijenjen komercijalnim djelatnostima.

([13]) Taj je pojam sadržan i u formulaciji „namijenjeni komercijalnim djelatnostima” uključenoj u definiciju pojma „upravitelj softvera otvorenog koda” iz članka 3. točke 14. Akta o kibernetičkoj otpornosti.

([14]) Moguće je i da se na pravnu osobu uopće neće primjenjivati obveze na temelju Akta o kibernetičkoj otpornosti, konkretno u sljedećim slučajevima: (i) određeni FOSS ne stavlja se na tržište u smislu Akta o kibernetičkoj otpornosti; i (ii) pravni subjekt ne odgovara definiciji upravitelja u odnosu na taj konkretni FOSS.

79. Vrsta „kontinuirane potpore” koju zaklade i slične organizacije pružaju konkretnim projektima FOSS-a može se znatno razlikovati. Na primjer, određeni pravni subjekti pružaju samo netehničku potporu, kao što su upravljanje brendiranjem projekata, utvrđivanje pravila upravljanja, organizacija događanja na razini zajednice ili prikupljanje donacija. Drugi subjekti omogućuju i osnovnu informatičku infrastrukturu potrebnu za funkcioniranje projekta, kao što su repozitoriji izvornog koda, sustavi za kontrolu verzija ili generiranje potpisnih ključeva. Drugi pak idu korak dalje u pogledu vrste potpore koju pružaju tako što aktivno doprinose projektu u obliku osiguravanja inženjerskih resursa, na primjer zapošljavanjem razvojnih programera, koordinacijom razvojnih aktivnosti, pregledavanjem ili spajanjem kodova, upravljanjem izdanjima ili postupanjem s izvješćima o ranjivostima i sigurnosnim zakrpama. Iako svi pravni subjekti koji se smatraju upraviteljima u skladu s Aktom o kibernetičkoj otpornosti moraju ispunjavati obveze iz članka 24. stavaka 1. i 2., mjera u kojoj se obveze utvrđene u članku 14. stavcima 1., 3. i 8. primjenjuju na te pravne subjekte razlikuje se ovisno o vrsti potpore koju pružaju, u skladu s člankom 24. stavkom 3.

80. Na primjer, upravitelj koji pruža samo netehničku potporu po definiciji nije uključen u razvoj proizvoda s digitalnim elementima, pa nije dužan obavješćivati o aktivno iskorištenim ranjivostima. Taj upravitelj ne pruža ni mrežne i informacijske sustave za razvoj tih proizvoda s digitalnim elementima, stoga nije obvezan obavijestiti ENISA-u i CSIRT-ove ili pogođene korisnike o značajnim incidentima. Međutim, ako upravitelj dozna za aktivno iskorištenu ranjivost (npr. iz izvješća vanjskih izvora, kao što su istraživači u području sigurnosti), trebao bi podijeliti te informacije s održavateljima proizvoda s digitalnim elementima u skladu sa svojom politikom kibernetičke sigurnosti. Održavatelji proizvoda s digitalnim elementima i/ili upravitelji trebali bi razmotriti i dobrovoljno izvješćivanje o ranjivostima u skladu s člankom 15.

81. Međutim, ako upravitelj omogućuje osnovnu informatičku infrastrukturu za određene proizvode s digitalnim elementima, dužan je obavijestiti ENISA-u i CSIRT-ove o svim značajnim incidentima povezanima s tom infrastrukturom koji utječu na sigurnost proizvoda s digitalnim elementima u skladu s člankom 14. stavkom 3. Osim toga je dužan, prema potrebi, obavijestiti sve korisnike (npr. općom objavom). Kao što je navedeno u prethodnoj točki, iako upravitelj nije dužan obavijestiti o aktivno iskorištenim ranjivostima za koje dozna, trebao bi poticati pravilno postupanje s ranjivostima i razmotriti dobrovoljno izvješćivanje u skladu s člankom 15.

82. Naposljetku, ako upravitelj osigurava i inženjerske resurse za određene proizvode s digitalnim elementima, dužan je: (i) u skladu s člankom 14. stavkom 1. obavijestiti o aktivno iskorištenim ranjivostima za koje dozna; i (ii) prema potrebi, obavijestiti sve korisnike. Ako upravitelj ima i izravan odnos s pogođenim korisnicima, dužan ih je i izravno obavijestiti u skladu s člankom 14. stavkom 8.

83. Ako subjekt prestane pružati sustavnu i kontinuiranu potporu za određeni FOSS, možda više neće odgovarati definiciji upravitelja i stoga se možda na njega više neće primjenjivati povezane obveze. U tim se slučajevima taj subjekt potiče da jasno priopći promjenu svojeg statusa u odnosu na taj konkretni FOSS.

84. U određenim situacijama subjekt koji je upravljao određenim projektom može odlučiti izravno unovčiti taj projekt, što dovodi do stavljanja proizvoda s digitalnim elementima na tržište i aktiviranja obveza proizvođača na temelju Akta o kibernetičkoj otpornosti. U tim okolnostima taj se subjekt smatra proizvođačem proizvoda s digitalnim elementima od datuma na koji ga stavi na tržište (ali ne u odnosu na ranije verzije za koje je djelovao kao upravitelj).

3.4. **Doprinositelji i korisnici niže u lancu opskrbe**

85. Kako je već navedeno u odjeljku *3.1.* – Utvrđivanje odgovornosti za besplatni softver otvorenog koda, u Aktu o kibernetičkoj otpornosti pojašnjava se da se on 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” (uvodna izjava 18.).

86. Proizvođači proizvoda s digitalnim elementima koji integriraju komponente FOSS-a u vlastite proizvode s digitalnim elementima isto tako ne postaju odgovorni za pojedinačnu usklađenost takvih komponenti s Aktom o kibernetičkoj otpornosti, čak i ako doprinose njihovu održavanju izvornim kodom.

87. Slično tomu, sama činjenica da proizvođači integriraju komponente FOSS-a u vlastite (unovčene) proizvode s digitalnim elementima ne utječe na status te komponente FOSS-a na temelju Akta o kibernetičkoj otpornosti. Održavatelji komponenti FOSS-a koje nisu stavljene na tržište nemaju obveze u odnosu na druge subjekte koji takve komponente mogu integrirati u svoje proizvode s digitalnim elementima. Primjena Akta o kibernetičkoj otpornosti na određenu komponentu FOSS-a ovisi isključivo o tome stavlja li je fizička ili pravna osoba koja je objavljuje na tržište.

88. Međutim, proizvođači proizvoda s digitalnim elementima koji integriraju komponente FOSS-a moraju se pridržavati Akta o kibernetičkoj otpornosti u pogledu vlastitih proizvoda s digitalnim elementima. U skladu s člankom 13. stavkom 5. imaju i obvezu dužne pažnje u odnosu na komponente FOSS-a koje integriraju. Osim toga, dužni su obavijestiti o ranjivostima u integriranim komponentama i podijeliti sigurnosne popravke u skladu s člankom 13. stavkom 6. Za više smjernica o toj temi vidjeti odjeljak *9.2.1.* – Obavješćivanje o ranjivostima više u lancu opskrbe i dijeljenje sigurnosnih popravaka.

3.5. **Primjeri scenarija**

89. Primjeri navedeni u nastavku potpuno su hipotetski i namijenjeni samo za ilustraciju raznih slučajeva objašnjenih u prethodnim odjeljcima.

Primjer 27: Razvojni programer A razvio je FOSS. Razvojni programer A objavljuje taj FOSS pod svojim imenom ili žigom, ali ne naplaćuje cijenu za njegovu upotrebu. Softver se otvoreno dijeli i svi mu mogu slobodno pristupiti, upotrebljavati ga, mijenjati i redistribuirati. Razvojni programer A navodi i poveznicu na platformu za prikupljanje dobrovoljnih donacija.

Poduzeća B, C i D integriraju taj FOSS u vlastite proizvode s digitalnim elementima. Kako bi poduprla kontinuirano održavanje, poduzeća B, C i D daju dobrovoljne donacije razvojnom programeru A. Te mu donacije omogućuju da nastavi aktivno održavati projekt.

Taj FOSS nije stavljen na tržište u smislu Akta o kibernetičkoj otpornosti. Razvojni programer A nema obveze na temelju Akta o kibernetičkoj otpornosti. Pri integraciji tog FOSS-a u vlastite proizvode s digitalnim elementima poduzeća B, C i D moraju postupati s dužnom pažnjom u skladu s člankom 13. stavkom 5.

Primjer 28: Neprofitna zaklada F objavljuje komponentu FOSS-a namijenjenu integraciji u druge komercijalne proizvode s digitalnim elementima. Zaklada F obvezuje se pružati kontinuiranu potporu za taj FOSS kako bi osigurala njegovu održivost i primjenu. Poduzeća A, B i C integriraju taj FOSS u vlastite proizvode s digitalnim elementima. Poduzeća A i B dobrovoljno izdvajaju dio vremena svojih razvojnih programera za potrebe razvoja i održavanja projekata FOSS-a u okviru zaklade F, među ostalim za predmetni FOSS.

Budući da je zaklada F neprofitni subjekt ustrojen tako da se njegova zarada nakon troškova koristi za postizanje neprofitnih ciljeva, ne smatra se da je FOSS stavljen na tržište u smislu Akta o kibernetičkoj otpornosti. Zaklada F upravitelj je FOSS-a i na nju se primjenjuju odgovarajuće obveze utvrđene u članku 24. Pri integraciji tog FOSS-a u vlastite proizvode s digitalnim elementima poduzeća A, B i C moraju postupati s dužnom pažnjom u skladu s člankom 13. stavkom 5.

Primjer 29: Poduzeće A razvilo je komponentu FOSS-a namijenjenu integraciji u vlastite proizvode s digitalnim elementima. Uz to, taj FOSS objavljuje zasebno pod svojim imenom ili žigom te ga aktivno održava. Međutim, ne naplaćuje njegovu upotrebu niti ga unovčuje na druge načine. Poduzeća B, C i D integriraju taj FOSS u vlastite proizvode s digitalnim elementima i dobrovoljno izdvajaju dio vremena svojih razvojnih programera za potrebe njegova održavanja.

Taj se FOSS ne smatra stavljenim na tržište u smislu Akta o kibernetičkoj otpornosti. Poduzeće A nije njegov proizvođač, ali jest njegov upravitelj. Pri integraciji tog FOSS-a u vlastite proizvode s digitalnim elementima poduzeća B, C i D moraju postupati s dužnom pažnjom u skladu s člankom 13. stavkom 5.

Primjer 30: Poduzeće A objavljuje FOSS pod svojim imenom ili žigom i nudi njegovu plaćenu verziju, koja uključuje određene koristi kao što su tehnička pomoć ili optimizacija performansi. Razvojni programeri iz poduzeća B, C i D doprinose održavanju FOSS-a, ali je on i dalje pod nadzorom poduzeća A.

Poduzeće A smatra se proizvođačem tog FOSS-a ([15]). Na poduzeća B, C i D ne primjenjuju se obveze iz Akta o kibernetičkoj otpornosti za taj konkretni FOSS. Ako taj FOSS integriraju u vlastite proizvode s digitalnim elementima, dužna su postupati s dužnom pažnjom u skladu s članком 13. stavkom 5.

Primjer 31: Poduzeće A objavljuje FOSS pod svojim imenom ili žigom i kontinuirano održava softver kako bi osiguralo njegovu dugoročnu održivost i omogućilo integraciju u proizvode s digitalnim elementima drugih poduzeća. Poduzeće A ne naplaćuje njegovu upotrebu, ne obrađuje osobne podatke koje prikuplja putem proizvoda s digitalnim elementima niti prodaje usluge podrške povezane s objavljivanjem FOSS-a.

Poduzeće B doprinosi održavanju FOSS-a kodom i izdvajanjem dijela vremena svojih razvojnih programera, ali ga ne distribuira u komercijalne svrhe. Poduzeće B nudi usluge tehničke podrške neovisno o distribuciji FOSS-a. Poduzeće A smatra se upraviteljem tog FOSS-a, dok poduzeće B nema obveze povezane s tim FOSS-om na temelju Akta o kibernetičkoj otpornosti.

Primjer 32: Komponentu FOSS-a objavljuje neprofitni subjekt ustrojen na način kojim se osigurava da se sva zarada nakon troškova upotrebljava za postizanje neprofitnih ciljeva. Subjekt pruža kontinuiranu potporu kako bi osigurao dugoročnu održivost projekta. Održavanje se financira javnim sredstvima, kao što su bespovratna sredstva za istraživanje. Dodatne razvojne aktivnosti, uključujući one za nove značajke, financiraju se donacijama i posebnim projektima koji se provode u partnerstvu s proizvođačima koji integriraju taj FOSS u svoje proizvode s digitalnim elementima. Takve su značajke ugrađene u bazu koda FOSS-a.

Neprofitni subjekt koji objavljuje FOSS smatra se upraviteljem te komponente FOSS-a. Proizvođač koji je doprinio razvoju određenih značajki ne postaje proizvođač te komponente FOSS-a. Ako proizvođač integrira tu komponentu FOSS-a u vlastiti proizvod s digitalnim elementima, mora postupati s dužnom pažnjom u skladu s članком 13. stavkom 5.

Primjer 33: Neprofitni subjekt ustrojen na način kojim se osigurava da se sva zarada nakon troškova upotrebljava za postizanje neprofitnih ciljeva objavljuje komplet za razvoj softvera FOSS i osigurava njegovo kontinuirano održavanje. Komplet za razvoj softvera otvoreno se dijeli i svi mu mogu slobodno pristupiti, upotrebljavati ga, mijenjati i redistribuirati. Financiranje se osigurava članarinama koje se plaćaju neprofitnom subjektu, a razvojni programeri zaposleni u organizacijama članicama pridonose razvoju kompleta za razvoj softvera kodom i drugim resursima. Proizvođači upotrebljavaju komplet za razvoj softvera kao komponentu za izradu drugih proizvoda s digitalnim elementima.

Neprofitni subjekt koji objavljuje taj komplet za razvoj softvera njegov je upravitelj. Članovi zaklade nisu odgovorni za usklađenost kompleta za razvoj softvera s Aktom o kibernetičkoj otpornosti. Ako proizvođači upotrebljavaju komplet za razvoj softvera za izradu vlastitog proizvoda s digitalnim elementima, moraju postupati s dužnom pažnjom u skladu s članком 13. stavkom 5.

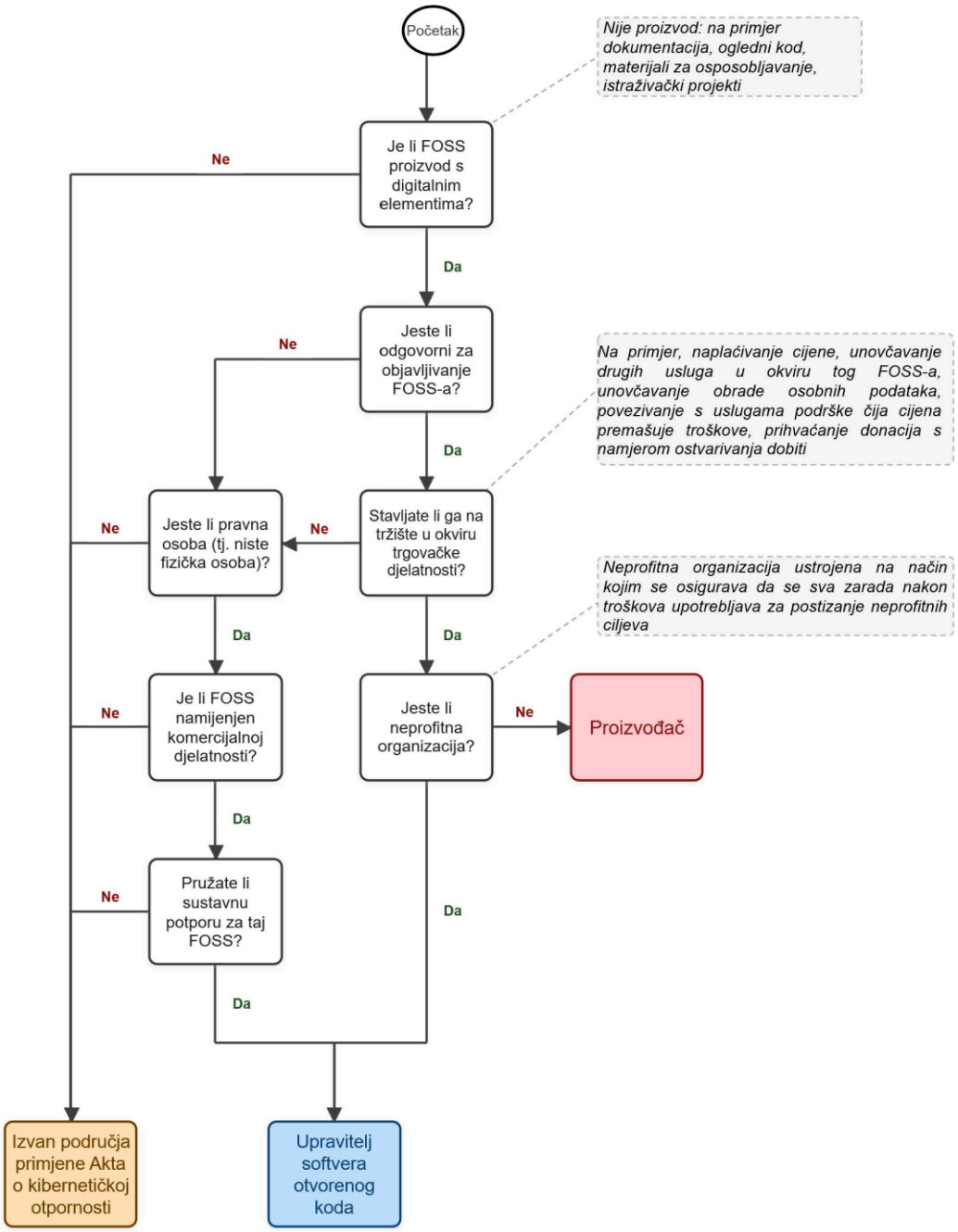
Primjer 34: Razvojni programer objavljuje knjižnicu FOSS-a u javnom repozitoriju paketa za određeni programski jezik i aktivno je održava. U dokumentaciji paketa razvojni programer dodaje poveznicu za prikupljanje donacija. Proizvođač besplatno preuzima tu knjižnicu iz repozitorija i integrira je u vlastiti proizvod s digitalnim elementima.

Za razvojnog programera i repozitorij paketa ne postoje obveze na temelju Akta o kibernetičkoj otpornosti. Proizvođač koji integrira knjižnicu mora postupati s dužnom pažnjom u skladu s članком 13. stavkom 5.

([15]) Osim ako je poduzeće A neprofitni subjekt ustrojen na način kojim se osigurava da se sva zarada nakon troškova upotrebljava za postizanje neprofitnih ciljeva, u kojem bi slučaju ono bilo upravitelj tog FOSS-a.

Slika 1:

Stilizirani dijagram toka o obuhvaćenosti besplatnog softvera otvorenog koda područjem primjene Akta o kibernetičkoj otpornosti



4. **BITNE IZMJENE I REZERVNI DIJELOVI**

90. U članku 3. točki 30. Akta o kibernetičkoj otpornosti „bitna izmjena” definirana je kao promjena proizvoda s digitalnim elementima nakon njegova stavljanja na tržište koja (i) utječe na sukladnost proizvoda s digitalnim elementima s bitnim zahtjevima utvrđenima u dijelu I. Priloga I.; ili (ii) prouzroči promjenu namjene prema kojoj je proizvod s digitalnim elementima bio ocijenjen.

91. Pojam bitne izmjene relevantan je za utvrđivanje obveza na temelju Akta o kibernetičkoj otpornosti u nizu slučajeva, među ostalim u sljedećim:

(a) u skladu s člankom 21. uvoznik ili distributer koji učini bitnu izmjenu proizvoda s digitalnim elementima koji je već stavljen na tržište smatra se njegovim proizvođačem;

(b) u skladu s člankom 22. svaka fizička ili pravna osoba koja učini bitnu izmjenu proizvoda s digitalnim elementima i stavi ga na raspolaganje na tržištu smatra se njegovim proizvođačem;

(c) u skladu s člankom 69. stavkom 2. svaka fizička ili pravna osoba koja nakon 11. prosinca 2027. učini bitnu izmjenu proizvoda s digitalnim elementima koji je stavljen na tržište prije tog datuma i stavi ga na tržište smatra se proizvođačem;

(d) u slučaju proizvođača proizvoda s digitalnim elementima koji su stavljeni na tržište nakon 11. prosinca 2027., za potrebe utvrđivanja mora li se za taj proizvod s digitalnim elementima provesti novi postupak ocjenjivanja sukladnosti zbog izmjena učinjenih nakon tog datuma, posebno s obzirom na iterativnu prirodu razvoja softvera.

92. Stoga je važno pružiti smjernice koje će gospodarskim subjektima pomoći da razumiju u kojim se slučajevima izmjene hardvera ili softvera smatraju bitnim izmjenama.

4.1. **Fizički popravci**

93. Kao što je navedeno u uvodnoj izjavi 42. Akta o kibernetičkoj otpornosti, „[a]ko 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, 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." To je u skladu s točkom 2.1. Plavog vodiča, u kojem se podsjeća na to da se „proizvod koji je podvrgnut znatnim izmjenama ili preinaci nakon stavljanja u uporabu mora […] smatrati novim proizvodom: (i) ako su njegove izvorne radne značajke, svrha ili vrsta izmijenjeni, a to nije predviđeno u prvotnoj procjeni rizika; (ii) ako se promijenila priroda opasnosti ili se povećala razina rizika u vezi s relevantnim zakonodavnim propisima Unije o usklađivanju; i (iii) ako se proizvod stavlja na raspolaganje (ili u uporabu ako primjenjivi zakonodavni propisi obuhvaćaju i stavljanje u uporabu). To treba procijeniti posebno za svaki pojedini slučaj, a osobito s obzirom na cilj zakonodavstva i vrstu proizvoda obuhvaćenih predmetnim zakonodavstvom."

94. Postupci obnove, održavanja ili popravka koji dovedu do fizičkih izmjena proizvoda s digitalnim elementima koji su već stavljeni na tržište ne predstavljaju nužno bitne izmjene. Stoga bi trebalo provesti procjenu svakog pojedinog slučaja kako bi se utvrdilo utječe li takva fizička izmjena na usklađenost proizvoda s digitalnim elementima s bitnim zahtjevima iz dijela I. Priloga I. ili uzrokuje promjenu namjene proizvoda obuhvaćene procjenom kibernetičkosigurnosnih rizika.

95. Zamjena neispravnih ili istrošenih dijelova dijelovima koji bolje rade (npr. zbog tehničkog napretka ili zato što se stari dio više ne proizvodi) sama po sebi ne podrazumijeva bitnu izmjenu popravljenog proizvoda s digitalnim elementima. O bitnoj je izmjeni riječ samo ako promjena u radnim značajkama ili načinu rada popravljenog proizvoda s digitalnim elementima (i) utječe na njegovu usklađenost s bitnim zahtjevima ili (ii) prouzroči promjenu namjene, pri čemu nova namjena nije bila obuhvaćena procjenom rizika.

Primjer 35: Proizvođač računalnog poslužitelja obavlja popravak tako što neispravni RAM zamjenjuje novim, učinkovitijim RAM-om. To ne utječe na usklađenost poslužitelja s bitnim zahtjevima. Poslužitelj bolje radi, ali njegove nove performanse ostaju u okviru predviđene namjene poslužitelja obuhvaćene procjenom kibernetičkosigurnosnih rizika. Računalni poslužitelj ne smatra se bitno izmijenjenim.

4.2. **Rezervni dijelovi**

96. U članku 2. stavku 6. Akta o kibernetičkoj otpornosti utvrđuje se da se taj akt ne primjenjuje na rezervne dijelove namijenjene zamjeni istovjetnih komponenti proizvedene u skladu s istim specifikacijama kao te komponente. U uvodnoj izjavi 29. nadalje se navodi da izuzeće obuhvaća rezervne dijelove za proizvode s digitalnim elementima koji su stavljeni na raspolaganje prije početka primjene Akta o kibernetičkoj otpornosti i rezervne dijelove koji su već prošli postupak ocjenjivanja sukladnosti kako je utvrđeno u Uredbi.

97. Izuzeće iz članka 2. stavka 6. Akta o kibernetičkoj otpornosti trebalo bi tumačiti na način da se primjenjuje samo ako se rezervni dio isporučuje konkretno radi popravka ili produljenja trajnosti proizvoda s digitalnim elementima koji je već stavljen na tržište (prije ili nakon 11. prosinca 2027.). Ako se proizvod s digitalnim elementima isporučuje kao samostalni proizvod, bez ikakve veze s održavanjem ili popravkom postojećeg proizvoda s digitalnim elementima, stavlja se na tržište u smislu Akta o kibernetičkoj otpornosti i ne bi se trebao smatrati rezervnim dijelom obuhvaćenim područjem primjene članka 2. stavka 6. Svrha održavanja ili popravka trebala bi biti očita iz konteksta isporuke, na primjer identifikacijom proizvoda s digitalnim elementima ili skupine proizvoda u narudžbi ili komercijalnoj ponudi ili isporukom preko postprodajnih ili servisnih kanala. Dokaze kojima se to potkrepljuje trebalo bi staviti na raspolaganje i tijelima za nadzor tržišta. Činjenica da bi se proizvod s digitalnim elementima tehnički mogao upotrijebiti za zamjenu komponente nije sama po sebi dovoljna da bi se na njega primjenjivalo izuzeće ako nije isporučen konkretno za te potrebe.

98. U skladu s tim, ako je rezervni dio istovjetan komponenti koja je već uključena u proizvod s digitalnim elementima koji je stavljen na tržište prije datuma početka primjene Akta o kibernetičkoj otpornosti ili je stavljen na tržište u skladu s njim, na taj se rezervni dio sam po sebi Akt o kibernetičkoj otpornosti ne primjenjuje.

99. Procjena toga treba li se rezervni dio smatrati istovjetnim komponenti trebala bi se odnositi na njegovu funkcionalnu ulogu u proizvodu s digitalnim elementima i značajke koje mogu biti relevantne za kibernetičku sigurnost. Iako je uvijek potrebno provesti procjenu svakog pojedinog slučaja, razlike koje ne utječu na sigurnosne značajke ili profil kibernetičkosigurnosne rizičnosti komponente same po sebi ne sprečavaju da taj rezervni dio bude obuhvaćen područjem primjene članka 2. stavka 6. Akta o kibernetičkoj otpornosti.

100. Suprotno tomu, razlike u značajkama relevantnima za kibernetičku sigurnost komponente, kao što su algoritmi, protokoli, kriptografski mehanizmi, značajke kontrole pristupa ili druge značajke relevantne za sigurnost, mogu značiti da se novi dio ne može smatrati istovjetnim komponenti koju bi trebao zamijeniti.

101. Ako rezervni dio nije istovjetan izvornoj komponenti, taj rezervni dio sam po sebi čini proizvod s digitalnim elementima i stoga se na njega primjenjuje Akt o kibernetičkoj otpornosti. U tim slučajevima usklađenost s bitnim zahtjevima mora se ocijeniti s obzirom na namjenu zamjenske komponente. Posebno je važna funkcija zamjenske komponente u osiguravanju kompatibilnosti ili interoperabilnosti s postojećim proizvodom s digitalnim elementima, među ostalim ako je taj proizvod s digitalnim elementima stavljen na tržište prije početka primjene Akta o kibernetičkoj otpornosti. Ako se zbog te namjene ili tehničkih ograničenja određeni bitni zahtjevi ne mogu razumno ispuniti, proizvođač to mora uzeti u obzir u procjeni kibernetičkosigurnosnih rizika i provesti odgovarajuće alternativne ili kompenzacijske mjere za ublažavanje rizika kako se ne bi ugrozila sigurnost proizvoda s digitalnim elementima. Kako je objašnjeno i u odjeljku *2.6.* – Složeni sustavi, tehnička dokumentacija te informacije i upute za korisnika imaju važnu ulogu u transparentnom opisivanju utvrđenih ograničenja, povezanih kibernetičkosigurnosnih rizika i provedenih mjera za ublažavanje rizika. Kao što je to objašnjeno u odjeljku *4.1.* – Fizički popravci, zamjena neispravnih ili istrošenih dijelova dijelovima koji bolje rade sama po sebi ne podrazumijeva bitnu izmjenu popravljenog proizvoda s digitalnim elementima.

Primjer 36: Proizvođač je povezane kontrolere stavio na tržište EU-a. U jednom je slučaju kontroler stavljen na tržište 2026., prije datuma početka primjene Akta o kibernetičkoj otpornosti. U drugom je slučaju kontroler stavljen na tržište 2028. u skladu s Aktom o kibernetičkoj otpornosti. U 2028. dolazi do kvara modula za digitalnu komunikaciju u obje vrste kontrolera. Proizvođač kao rezervni dio isporučuje zamjenski modul koji je istovjetan i proizveden u skladu s istim specifikacijama kao izvorni modul.

U oba slučaja zamjenski modul obuhvaćen je područjem primjene izuzeća iz članka 2. stavka 6. Akt o kibernetičkoj otpornosti ne primjenjuje se na rezervni dio sam po sebi, iako je riječ o proizvodu s digitalnim elementima, jer on zamjenjuje istovjetnu komponentu proizvoda s digitalnim elementima. Popravak ne dovodi do bitne izmjene proizvoda s digitalnim elementima.

Primjer 37: Proizvođač je povezani industrijski kontroler stavio na tržište EU-a 2026., prije datuma početka primjene Akta o kibernetičkoj otpornosti. U 2028. dolazi do kvara komunikacijskog čipa u tom kontroleru. Budući da proizvođač više ne proizvodi taj čip, kao rezervni dio isporučuje noviji čip jednake funkcionalnosti, ali s drukčijom kriptografskom implementacijom i ažuriranim mehanizmom sigurnog pokretanja kako bi se održala kompatibilnost i omogućio nastavak rada.

U tom se slučaju zamjenski čip ne može smatrati istovjetnim jer razlike u kriptografskoj implementaciji i mehanizmu sigurnog pokretanja utječu na kibernetičkosigurnosna svojstva čipa. Stoga on nije obuhvaćen područjem primjene izuzeća iz članka 2. stavka 6. te se smatra proizvodom s digitalnim elementima na koji se primjenjuje Akt o kibernetičkoj otpornosti. Usklađenost zamjenskog dijela mora se ocijeniti s obzirom na njegovu namjenu, uključujući njegovu ulogu u osiguravanju interoperabilnosti s proizvodom s digitalnim elementima koji je stavljen na tržište prije početka primjene Akta o kibernetičkoj otpornosti.

Primjer 38: Proizvođač 2028. stavlja na tržište kontroler za pametne zgrade u skladu s Aktom o kibernetičkoj otpornosti. U 2029. dolazi do kvara bežičnog modula u tom kontroleru. Budući da proizvođač više ne proizvodi taj modul, kao rezervni dio isporučuje novi modul koji ima istu funkciju, iste komunikacijske protokole i sigurnosne mehanizme, ali se temelji na drugom sklopu čipova i ima ažurirani integrirani softver koji ne mijenja značajke koje mogu biti relevantne za kibernetičku sigurnost.

U tom se slučaju zamjenski modul može smatrati istovjetnim. Modul je stoga obuhvaćen područjem primjene izuzeća iz članka 2. stavka 6. te se na njega ne primjenjuje Akt o kibernetičkoj otpornosti.

102. Izuzeće za rezervne dijelove primjenjuje se neovisno o tome zamjenjuje li rezervni dio komponentu proizvoda s digitalnim elementima ili zamjenjuje cijeli proizvod s digitalnim elementima koji je sam po sebi dio većeg proizvoda, među ostalim ako se taj veći proizvod s digitalnim elementima sastoji od više integriranih komponenata, pod uvjetom da se zamjenski dio isporučuje konkretno kao rezervni dio, kao što je to objašnjeno u prethodnim točkama.

Primjer 39: Proizvođač 2027. stavlja na tržište sustav za industrijsku automatizaciju čija je komponenta programabilni logički kontroler. U 2031. dolazi do kvara središnje procesorske jedinice (CPU) programabilnog logičkog kontrolera. Proizvođač nudi dvije mogućnosti popravka: (i) isporuku zamjenske jedinice središnje procesorske jedinice, koja se može smatrati istovjetnom onoj koja je izvorno ugrađena u sustav; ili (ii) isporuku zamjenskog cjelokupnog programabilnog logičkog kontrolera, koji se može smatrati istovjetnim onom koji je izvorno ugrađen u sustav. U svakom slučaju, zamjena se isporučuje preko proizvođačeva postprodajnog servisnog kanala kao rezervni dio, a sustav za industrijsku automatizaciju za koji je zamjena namijenjena jasno je identificiran. U oba slučaja zamjena je obuhvaćena područjem primjene izuzeća iz članka 2. stavka 6., neovisno o tome odnosi li se ona na komponentu programabilnog logičkog kontrolera ili kontroler u cjelini.

4.3. **Ažuriranja softvera kao bitne izmjene**

103. Razvoj softvera iterativne je prirode, a softverski proizvodi s digitalnim elementima koji su već stavljeni na tržište često se i kontinuirano ažuriraju. U tom je kontekstu korisno pružiti više smjernica za utvrđivanje slučajeva u kojima softver treba smatrati bitno izmijenjenim. Te su smjernice prije svega namijenjene proizvođačima softverskih proizvoda s digitalnim elementima koji mijenjaju vlastite proizvode te bi im trebale pomoći u utvrđivanju toga smatraju li se te promjene bitnim izmjenama.

104. U uvodnoj izjavi 39. navodi se da je proizvod s digitalnim elementima bitno izmijenjen ako se promjenom mijenja razina kibernetičkog sigurnosnog rizika i ako proizvođač taj izmijenjeni ili dodatni rizik nije predvidio u procjeni rizika, a time ni u primjeni bitnih zahtjeva. Proizvođač bi stoga trebao posebno za svaki pojedini slučaj procijeniti dovodi li ažuriranje softvera do novih ili većih kibernetičkosigurnosnih rizika te jesu li ti rizici već uzeti u obzir u njegovoj procjeni rizika.

105. Ako proizvođač u proizvod s digitalnim elementima uvede nove funkcionalnosti koje prouzroče promjenu namjene proizvoda u cjelini, vjerojatno je da proizvođač te promjene nije uzeo u obzir u svojoj procjeni rizika. U tim okolnostima promjena bi se općenito smatrala bitnom izmjenom.

Primjer 40: Proizvođač stavlja na tržište nadzornu ploču koja prikuplja podatke iz strojeva i prikazuje trendove i upozorenja, a pritom nema mogućnost upravljanja tim strojevima. Proizvođač zatim razvija novu verziju te nadzorne ploče pri čemu uvodi funkcionalnosti koje joj omogućuju upravljanja strojevima, među ostalim prilagodbom radnih parametara i ponovnim pokretanjem strojeva u slučaju kvara. Zbog tih promjena namjena nadzorne ploče promijenila se u odnosu na ono što je predviđeno u procjeni rizika, pri čemu je s alata za informiranost o stanju pretvorena u proizvod s digitalnim elementima namijenjen upravljanju drugim uređajima. Stoga je nadzorna ploča bitno izmijenjena.

Primjer 41: Proizvođač stavlja na tržište korisničku softversku aplikaciju namijenjenu organiziranju i prikazivanju osobnih podataka, kao što su e-pošta, poruke ili dokumenti, koja podržava osnovne funkcije pretraživanja i filtriranja. Proizvođač zatim uvodi ažuriranje koje aplikaciji omogućuje automatsku analizu korisničkog sadržaja radi izrade profila ponašanja i donošenja automatiziranih odluka koje utječu na davanje prednosti, ograničavanje ili preporučivanje sadržaja bez intervencije korisnika. Zbog te promjene namjena softvera mijenja se iz alata za upravljanje informacijama pod nadzorom korisnika u sustav za automatizirano donošenje odluka, što nije bilo predviđeno u procjeni rizika. Aplikacija je stoga bitno izmijenjena.

106. Međutim, proizvođač može postupno uvoditi nove funkcionalnosti koje su već obuhvaćene procjenom rizika ili koje same po sebi ne mijenjaju profil kibernetičkosigurnosne rizičnosti proizvoda s digitalnim elementima. O takvoj situaciji može biti riječ, na primjer, ako je proizvođač predvidio razvoj tih funkcionalnosti, već opisao i procijenio povezane rizike te proveo odgovarajuće mjere ublažavanja kako bi omogućio kontinuirano ispunjavanje bitnih zahtjeva. Isto vrijedi i ako se novim funkcionalnostima ne uvode promjene koje dovode do novih ili većih rizika. Takva ažuriranja stoga ne bi trebalo smatrati bitnim izmjenama jer ona ne povećavaju kibernetički sigurnosni rizik i stoga nema promjena u primjeni bitnih zahtjeva.

Primjer 42: Aplikacija za razmjenu poruka prvotno je objavljena s funkcionalnošću ograničenom na razmjenu poruka između dva korisnika. Proizvođačeva procjena rizika obuhvaća kasnije uvođenje grupne razmjene poruka, uključujući, na primjer, povećanu složenost usmjeravanja poruka. U sljedećem ažuriranju proizvođač dodaje funkcionalnost grupnog razgovora zajedno s administratorskim kontrolama i alatima za moderiranje koji su već predviđeni i procijenjeni u okviru izvornog projekta. Ažuriranjem se uvode funkcionalnosti koje su obuhvaćene prvotnom namjenom i procjenom rizika. Aplikacija za razmjenu poruka stoga nije bitno izmijenjena.

Primjer 43: Na tržište je stavljen sustav za praćenje proizvodnje s omogućenim nadzornim pločama samo za čitanje, dok su funkcionalnosti automatizirane kontrole prisutne u arhitekturi sustava, ali su i dalje onemogućene. Proizvođačeva procjena rizika izričito obuhvaća buduću aktivaciju automatiziranih kontrolnih petlji, uključujući kibernetičkosigurnosne rizike povezane s kontrolom na temelju zatvorene petlje, kao i zaštitne mjere kao što su mehanizmi kojima operater može preuzeti upravljanje i sigurna stanja. U sljedećem ažuriranju proizvođač omogućuje funkcionalnosti automatizirane kontrole i aktivira zaštitne mjere kako su izvorno procijenjene. Sustav za praćenje proizvodnje stoga nije bitno izmijenjen.

107. S druge strane, čak i ograničene ili naizgled manje nove funkcionalnosti mogu dovesti do znatnih kibernetičkosigurnosnih rizika koji utječu na ispunjavanje bitnih zahtjeva. Ocjena toga je li došlo do bitne izmjene stoga se ne bi trebala temeljiti na opsegu ili složenosti promjene nego na njezinu potencijalno negativnom učinku na profil kibernetičkosigurnosne rizičnosti proizvoda s digitalnim elementima, a time i na primjenu bitnih zahtjeva.

Primjer 44: Proizvođač uvodi ažuriranje softverske aplikacije kojim dodaje funkcionalnost „zapamti me” odnosno mogućnost trajne prijave u okviru koje se tokeni za autentifikaciju pohranjuju lokalno kako bi korištenje aplikacije bilo praktičnije za korisnike. Iako je ta funkcionalnost ograničenog opsega, ona dovodi do novih rizika povezanih s krađom tokena, neovlaštenim pristupom i otimanjem sesije koji nisu uzeti u obzir u procjeni rizika. Ažuriranje stoga utječe na ispunjavanje bitnih zahtjeva. Softverska aplikacija bitno je izmijenjena.

Primjer 45: Proizvođač postojećem softverskom proizvodu s digitalnim elementima dodaje novu funkcionalnost evidentiranja i dijagnostike koja omogućuje izvoz detaljnih evidencija iz sustava radi rješavanja problema. Iako se čini da je ta funkcionalnost neznatna, ona omogućuje prikupljanje i pohranu osjetljivih operativnih podataka u nešifriranom formatu, što dovodi do rizika od izlaganja podataka koji prethodno nisu procijenjeni ili ublaženi. Promjena stoga može znatno utjecati na profil kibernetičkosigurnosne rizičnosti proizvoda s digitalnim elementima. Softverski proizvod s digitalnim elementima bitno je izmijenjen.

108. U skladu s uvodnom izjavom 39. Akta o kibernetičkoj otpornosti sigurnosna ažuriranja općenito se ne smatraju bitnim izmjenama jer je njihova primarna svrha smanjiti razinu kibernetičkog sigurnosnog rizika povezanog s proizvodom s digitalnim elementima. Sigurnosno ažuriranje kojim se ne mijenja namjena proizvoda i koje ne dovodi do novih kibernetičkosigurnosnih rizika stoga ne bi trebalo smatrati bitnom izmjenom, čak i ako bi se tim ažuriranjem mogle uvesti znatne tehničke promjene. To uključuje slučajeve u kojima su određene funkcionalnosti izmijenjene ili ograničene isključivo radi ublažavanja utvrđenih ranjivosti i osiguravanja kontinuiranog ispunjavanja bitnih zahtjeva.

Primjer 46: Proizvođač uvodi sigurnosno ažuriranje kako bi otklonio ranjivost u bazi koda proizvoda s digitalnim elementima ispravljanjem pogreške pri validaciji unosa koja bi mogla dovesti do prelijevanja međuspremnika ili ispravljanjem logičkog nedostatka koji omogućuje zaobilaženje autentifikacije zbog nepravilne validacije tokena sesije. Ažuriranjem se mijenja unutarnja implementacija softvera a da se pritom ne utječe na namjenu tog proizvoda niti dovodi do nove izloženosti riziku. Takvo ažuriranje namijenjeno je isključivo smanjenju kibernetičkog sigurnosnog rizika. Sigurnosno ažuriranje ne bi trebalo smatrati bitnom izmjenom.

Primjer 47: Proizvođač uvodi sigurnosno ažuriranje kojim se pooštravaju postojeće sigurnosne konfiguracije, kao što su postroživanje pravila za vatrozid, onemogućavanje nekorištenih mrežnih portova, izmjena zadanih pravila za administratorske lozinke ili uvođenje obvezne višefaktorske autentifikacije ako je takva funkcionalnost već dostupna ili predviđena. Iako ažuriranje može utjecati na to kako korisnici konfiguriraju proizvod s digitalnim elementima ili mu pristupaju, ono ne mijenja njegovu namjenu i služi isključivo poboljšanju njegova sigurnosnog stanja. Sigurnosno ažuriranje ne bi trebalo smatrati bitnom izmjenom.

Primjer 48: Proizvođač stavlja na tržište softverski proizvod s digitalnim elementima koji omogućuje sigurnu komunikaciju primjenom okvira za šifriranje koji se može konfigurirati i koji podržava više kriptografskih algoritama i veličina ključeva, kako je opisano u tehničkoj dokumentaciji proizvoda i procjeni rizika. Procjena rizika obuhvaća sve kriptografske opcije koje proizvod s digitalnim elementima pruža i u njoj se predviđa buduće povlačenje određenih algoritama iz upotrebe. Procjena rizika obuhvaća i mjere ublažavanja, kao što su kriptografska agilnost, interno upravljanje ključevima i testiranje kompatibilnosti. Kao odgovor na nove kriptografske smjernice proizvođač uvodi sigurnosno ažuriranje kojim se deaktivira zastarjeli algoritam i aktivira snažnija, već podržana alternativa, bez stvaranja novih vanjskih ovisnosti ili izmjene tokova podataka. Budući da se tim ažuriranjem provodi sigurnosna mjera koja je predviđena i procijenjena u okviru izvornog projekta i ne dovodi do novih kibernetičkosigurnosnih rizika, sigurnosno ažuriranje ne bi trebalo smatrati bitnom izmjenom.

109. Suprotno tomu, sigurnosno ažuriranje može se smatrati bitnom izmjenom ako, neovisno o njegovu sigurnosnom cilju, ažuriranje prouzroči izmjenu namjene proizvoda s digitalnim elementima u većoj mjeri nego što je prvotno predviđeno ili ako ono dovodi do novih ili većih kibernetičkosigurnosnih rizika. To može biti slučaj, na primjer, ako ažuriranje bitno mijenja granice ili strukturu ovisnosti tog proizvoda na način koji nije predviđen u procjeni rizika, npr. bitnom izmjenom tokova podataka ili dodavanjem novih sučelja dostupnih izvana.

Primjer 49: Proizvođač stavlja na tržište softverski proizvod s digitalnim elementima namijenjen lokalnom šifriranju datoteka za podatke pohranjene na korisnikovu uređaju, koji korisnicima omogućuje šifriranje i dešifriranje datoteka na zahtjev. Nakon što se otkrije ranjivost u tijeku rada šifriranja, proizvođač uvodi sigurnosno ažuriranje kojim se uklanja funkcionalnost lokalnog šifriranja i umjesto toga se sve datoteke moraju učitati u sustav za šifriranje na daljinu kojim upravlja proizvođač te se ondje pohraniti i obrađivati. Zbog te promjene proizvod s digitalnim elementima više ne obavlja lokalno šifriranje kako je prvotno predviđeno, nego funkcionira kao usluga šifriranja i obrade podataka na daljinu. Iako se ažuriranje uvodi zbog sigurnosnih razloga, ono iz temelja mijenja namjenu tog proizvoda na način koji nije predviđen u procjeni rizika te se stoga smatra bitnom izmjenom.

Primjer 50: Proizvođač stavlja na tržište softverski proizvod s digitalnim elementima koji se za sigurnu komunikaciju među komponentama proizvoda s digitalnim elementima oslanja na uspostavljeni protokol šifriranja i životni ciklus ključeva kojim se interno upravlja. Kao odgovor na novoutvrđene kriptografske slabosti proizvođač uvodi sigurnosno ažuriranje kojim se postojeći mehanizam šifriranja zamjenjuje drugim protokolom koji iziskuje upotrebu vanjske usluge upravljanja ključevima koju pruža treća strana. Zbog te se promjene bitno mijenjaju ovisnosti i tokovi podataka proizvoda s digitalnim elementima te se uvode nova vanjska sučelja i dolazi do oslanjanja na usluge trećih strana koje nisu uzete u obzir u procjeni rizika. Iako je ažuriranje potaknuto sigurnosnim razlozima, ono dovodi do novih kibernetičkosigurnosnih rizika te se stoga smatra bitnom izmjenom.

110. Kao što je navedeno u točki 104., pitanje predstavlja li ažuriranje softvera bitnu izmjenu trebalo bi procijeniti posebno za svaki pojedini slučaj. Pri provedbi te procjene proizvođači mogu razmotriti, ne ograničavajući se na navedeno, dovodi li ažuriranje softvera do:

(a) uvođenja novih vektora prijetnji, kao što su dodatna sučelja, komunikacijski kanali, okruženja za izvršavanje ili vanjske ovisnosti preko kojih bi se prijetnje mogle ostvariti;

(b) mogućnosti ostvarenja novih scenarija napada, uključujući, na primjer, nove načine na koje bi moglo doći do neovlaštenog pristupa, manipulacije, ometanja ili krive upotrebe proizvoda s digitalnim elementima ili podataka koje on obrađuje;

(c) promjene vjerojatnosti prethodno utvrđenih scenarija napada, na primjer smanjenjem razine truda ili stručnog znanja potrebnog za njihovu provedbu, povećanjem izloženosti nepouzdanim akterima ili slabljenjem postojećih zaštitnih mjera;

(d) promjene potencijalnog učinka prethodno utvrđenih scenarija napada, uključujući, na primjer, opseg zahvaćenih podataka ili funkcija, ozbiljnost operativnih, sigurnosnih ili gospodarskih posljedica ili sposobnost otkrivanja, zaustavljanja ili oporavka od incidenta.

111. U nekim slučajevima ažuriranje softvera ne dovodi do novih vektora prijetnji, ne omogućuje nove scenarije napada i ne mijenja bitno vjerojatnost ili učinak prethodno utvrđenih scenarija napada. Ta činjenica može ukazivati na to da zbog ažuriranja ne nastaju novi ili povećani kibernetičkosigurnosni rizici, pod uvjetom da su pretpostavke i mjere ublažavanja na koje se oslanja u procjeni rizika i dalje valjane i djelotvorne. Stoga je vjerojatno da se ažuriranje ne može smatrati bitnom izmjenom.

112. S druge strane, ažuriranje softvera može uvesti nove vektore prijetnji, omogućiti nove scenarije napada ili bitno izmijeniti vjerojatnost ili učinak postojećih scenarija napada. U tim slučajevima proizvođač bi trebao ponovno procijeniti kibernetičkosigurnosne rizike proizvoda s digitalnim elementima i utvrditi jesu li bitni zahtjevi i dalje ispunjeni te dovodi li ažuriranje do novih ili većih rizika koji nisu predviđeni u procjeni rizika.

113. Pitanje smatra li se ažuriranje softvera bitnom izmjenom relevantno je da bi se utvrdilo primjenjuju li se određene obveze iz Akta o kibernetičkoj otpornosti, kako je navedeno u točki 91. Međutim, neovisno o tome ustanovi li se da je riječ o bitnoj izmjeni, proizvođači su u svakom slučaju odgovorni za jamčenje sigurnosti ažuriranja softvera i svojeg proizvoda s digitalnim elementima u razdoblju potpore, u skladu sa zahtjevima u pogledu postupanja s ranjivostima utvrđenima u dijelu II. Priloga I. Aktu o kibernetičkoj otpornosti. Nadalje, bez obzira na to smatraju li se ažuriranja softvera bitnim izmjenama, proizvođači su dužni osigurati da procjena rizika i tehnička dokumentacija budu točne i potpune i da se redovito ažuriraju, u skladu s člankom 13. stavkom 7. i člankom 31. stavkom 2.

4.4. **Posljedice bitne izmjene**

114. Posljedice bitne izmjene koju je učinio akter koji nije izvorni proizvođač proizvoda s digitalnim elementima koji je već stavljen na tržište uređene su člancima 21. i 22. Akta o kibernetičkoj otpornosti. Članak 21. odnosi se na uvoznike i distributere, dok se članak 22. odnosi na sve fizičke ili pravne osobe osim proizvođača, uvoznika ili distributera.

115. Ako bitnu izmjenu učini izvorni proizvođač proizvoda s digitalnim elementima, posljedice proizlaze iz uvriježenog koncepta bitne izmjene iz uvodne izjave 41. Akta o kibernetičkoj otpornosti i dodatno su razrađene u točki 2.1. Plavog vodiča. U toj je točki navedeno da proizvod koji je podvrgnut znatnim izmjenama ili preinaci nakon stavljanja na tržište treba smatrati novim proizvodom ako su njegove izvorne radne značajke, svrha ili vrsta izmijenjeni, priroda opasnosti se promijenila ili se razina rizika povećala, a proizvod s digitalnim elementima stavlja se na raspolaganje na tržištu.

116. Stoga je uvriježena posljedica to da se, ako se izmjena proizvoda s digitalnim elementima smatra bitnom izmjenom i izmijenjeni se proizvod s digitalnim elementima stavlja na raspolaganje na tržištu, taj proizvod smatra novim proizvodom s digitalnim elementima za potrebe Akta o kibernetičkoj otpornosti. Stoga stavljanje bitno izmijenjenog proizvoda na raspolaganje na tržištu predstavlja novo stavljanje na tržište. To vrijedi neovisno o tome je li bitnu izmjenu učinio izvorni proizvođač ili druga osoba. Radi ujednačene i proporcionalne primjene Akta o kibernetičkoj otpornosti na razne kategorije aktera koji mogu učiniti bitnu izmjenu, pododjeljci u nastavku odnose se na obveze koje nastaju osobama koje učine bitnu izmjenu i stave taj proizvod s digitalnim elementima na tržište. Posljedice za razdoblje potpore za proizvod s digitalnim elementima navedene su u odjeljku 5. – Razdoblje potpore.

4.4.1. *Bitne izmjene koje je učinila osoba koja nije izvorni proizvođač*

117. U skladu s člancima 21. i 22., ako bitnu izmjenu proizvoda s digitalnim elementima koji je već stavljen na tržište učini fizička ili pravna osoba koja nije proizvođač proizvoda s digitalnim elementima, osoba koja učini bitnu izmjenu i stavi izmijenjeni proizvod s digitalnim elementima na raspolaganje na tržištu smatra se proizvođačem tog izmijenjenog proizvoda s digitalnim elementima, neovisno o tome je li ta osoba bila uključena u izvorni projekt ili stavljanje na tržište tog proizvoda.

118. U članku 22. dodatno se pojašnjava da osoba koja učini izmjenu podliježe obvezama utvrđenima u člancima 13. i 14. samo za dio proizvoda s digitalnim elementima na koji utječe bitna izmjena ako ta izmjena ne utječe na kibernetičku sigurnost proizvoda s digitalnim elementima u cjelini.

119. Ako bitna izmjena utječe na ispunjavanje bitnih zahtjeva, ali ne utječe negativno na kibernetičku sigurnost proizvoda s digitalnim elementima u cjelini, na osobu koja učini izmjenu primjenjuju se članak 13. (uključujući obvezu osiguravanja usklađenosti s bitnim zahtjevima i provedbe postupka ocjenjivanja sukladnosti) i članak 14. (obveze u pogledu izvješćivanja) samo u odnosu na dio proizvoda s digitalnim elementima koji je bitno izmijenjen ([16]). Nadalje, obveze izvornog proizvođača na temelju Akta o kibernetičkoj otpornosti i dalje se primjenjuju na izvorni proizvod s digitalnim elementima stavljen na tržište, čime se osigurava kontinuitet postupanja s ranjivostima i usklađenost neizmijenjenih dijelova.

120. Slučaj bitne izmjene ne bi trebalo miješati sa slučajevima integracije, u kojima osoba sastavlja komponente (među ostalim, prema potrebi, njihovom izmjenom) u novi proizvod s digitalnim elementima koji sama stavlja na tržište. U tim slučajevima integrator ne mijenja proizvod s digitalnim elementima koji je drugi proizvođač već stavio na tržište, nego na tržište stavlja novi proizvod s vlastitim digitalnim elementima. Integrator je proizvođač tog novog proizvoda s digitalnim elementima za potrebe Akta o kibernetičkoj otpornosti te je dužan ispuniti sve obveze iz Uredbe u pogledu proizvoda s digitalnim elementima u cjelini. Ako proizvođač integrira komponente na koje se primjenjuje Akt o kibernetičkoj otpornosti, pri ispunjavanju svojih obveza iz Akta može se osloniti na aktivnosti usklađivanja koje su već proveli proizvođači komponenti.

Primjer 51: Poduzeće kupuje gotove module mikrokontrolera i komponente za povezivost od dobavljača trećih strana, razvija vlastiti integrirani softver i paket senzora te ih sastavlja u povezani poljoprivredni proizvod za praćenje s digitalnim elementima koji stavlja na tržište pod svojim imenom. Iako je poduzeće izmijenilo osnovne module mikrokontrolera i kombiniralo ih s drugim komponentama, ono ne mijenja bitno proizvod s digitalnim elementima koji je već stavljen na tržište, nego na tržište stavlja novi proizvod s digitalnim elementima. Poduzeće je proizvođač poljoprivrednog proizvoda za praćenje za potrebe Akta o kibernetičkoj otpornosti i dužno je pridržavati se Uredbe u pogledu tog proizvoda u cjelini.

([16]) U skladu s točkom 2.1. Plavog vodiča „[n]ije nužno ponavljati ispitivanja i sastavljati novu dokumentaciju o aspektima na koje izmjena ne utječe. Fizička ili pravna osoba koja izvršava izmjene ili koja je naručila izmjene na proizvodu mora dokazati da nije potrebno ažurirati sve elemente tehničke dokumentacije. Fizička ili pravna osoba koja izvršava izmjene ili koja je naručila izmjene na proizvodu odgovorna je za sukladnost izmijenjenog proizvoda i sastavlja izjavu o sukladnosti, čak i ako upotrebljava postojeća ispitivanja i tehničku dokumentaciju.”

121. Ako bitna izmjena koju je učinila osoba koja nije izvorni proizvođač negativno utječe na kibernetičku sigurnost proizvoda s digitalnim elementima u cjelini, na primjer zato što izmjena više nije usmjerena ili ograničena na određenu komponentu ili podsustav, izmijenjeni proizvod s digitalnim elementima koji je stavljen na raspolaganje na tržištu trebalo bi u cijelosti smatrati novim proizvodom s digitalnim elementima na koji se primjenjuje Akt o kibernetičkoj otpornosti. U tim se slučajevima promijenio ukupni profil kibernetičkosigurnosne rizičnosti tog proizvoda, a izmjena se ne može procijeniti bez razmatranja proizvoda s digitalnim elementima u cjelini. Na osobu koja je učinila izmjenu primjenjuju se obveze proizvođača utvrđene u člancima 13. i 14. u pogledu izmijenjenog proizvoda s digitalnim elementima u cjelini.

4.4.2. *Bitne izmjene koje je učinio izvorni proizvođač*

122. Ako bitnu izmjenu učini izvorni proizvođač, među ostalim u kontekstu iterativnog razvoja softverskih proizvoda s digitalnim elementima, taj proizvođač i dalje se smatra proizvođačem za potrebe Akta o kibernetičkoj otpornosti. Međutim, bitno izmijenjeni proizvod s digitalnim elementima treba smatrati novim proizvodom stavljenim na tržište.

123. U skladu s točkom 2.1. Plavog vodiča izvorni proizvođač koji na tržište stavlja bitno izmijenjeni proizvod s digitalnim elementima može ponovno upotrijebiti postojeću dokumentaciju i ispitivanja za aspekte proizvoda s digitalnim elementima na koje bitna izmjena ne utječe. Konkretno, ako proizvođač na tržište stavlja bitno izmijenjene verzije istog proizvoda s digitalnim elementima, u središtu postupka ocjenjivanja sukladnosti trebali bi biti znatno izmijenjeni dijelovi proizvoda s digitalnim elementima. Slično tomu, ako ocjenjivanje sukladnosti provodi treća strana, pri ocjenjivanju koje provodi tijelo za ocjenjivanje sukladnosti posebnu pozornost trebalo bi obratiti na bitno izmijenjene dijelove. Za neizmijenjene dijelove proizvoda s digitalnim elementima može ponovno upotrijebiti postojeću dokumentaciju i rezultate ispitivanja.

124. Aspekti proporcionalnosti iz prethodnog pododjeljka jednako se primjenjuju na bitne izmjene koje je proveo izvorni proizvođač proizvoda s digitalnim elementima stavljenog na tržište prije 11. prosinca 2027. Proizvođač ne treba samo zbog te bitne izmjene koju je proveo izvorni proizvođač cijeli proizvod s digitalnim elementima koji je stavljen na tržište prije tog datuma u potpunosti uskladiti s Aktom o kibernetičkoj otpornosti, osim ako izmjena negativno utječe na kibernetičku sigurnost proizvoda s digitalnim elementima u cjelini. Ako izmjena ne utječe na kibernetičku sigurnost proizvoda s digitalnim elementima u cjelini, obveze izvornog proizvođača u pogledu izmjene trebale bi biti ograničene na bitno izmijenjene dijelove.

5. **RAZDOBLJE POTPORE**

125. U skladu s člankom 13. stavkom 8. Akta o kibernetičkoj otpornosti proizvođač je dužan odrediti razdoblje potpore u kojem se s ranjivostima proizvoda s digitalnim elementima, uključujući njegove komponente, postupa djelotvorno i u skladu s bitnim zahtjevima utvrđenima u dijelu II. Priloga I. Razdoblje potpore obuhvaća razdoblje u kojem se očekuje da će se proizvod s digitalnim elementima upotrebljavati (očekivano vrijeme upotrebe) te bi ga trebalo odrediti s obzirom na kriterije utvrđene u članku 13. stavku 8., a to su konkretno razumna očekivanja korisnika, priroda proizvoda s digitalnim elementima, uključujući njegovu namjenu, kao i mjerodavno pravo Unije kojim se utvrđuje vijek trajanja proizvoda s digitalnim elementima ([17]). Općenito, te kriterije treba uzeti u obzir na način kojim se osigurava proporcionalnost pri određivanju razdoblja potpore.

([17]) Dodatni kriteriji koji se mogu uzeti u obzir, u skladu s člankom 13. stavkom 8., jesu 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 skupine za administrativnu suradnju u okviru Akta za kibernetičku otpornost (skupina za ADCO) i Komisije.

126. Člankom 13. stavkom 8. nadalje je propisano da razdoblje potpore traje najmanje pet godina, osim ako se očekuje da će proizvod s digitalnim elementima biti u upotrebi kraće od pet godina, u kojem slučaju razdoblje potpore odgovara očekivanom vremenu upotrebe. Minimalno razdoblje potpore stoga služi samo kao zaštitna mjera koja jamči da se s ranjivostima postupa dovoljno dugo, a istodobno se proizvođačima omogućuje da uzmu u obzir proizvode s digitalnim elementima čije je očekivano vrijeme upotrebe doista kraće. U uvodnoj izjavi 60. navodi se više smjernica u tom pogledu te se pojašnjava da bi proizvodi s digitalnim elementima za koje se razumno očekuje da će se upotrebljavati dulje od pet godina trebali imati dulja razdoblja potpore. Stoga razdoblje potpore od pet godina ne treba smatrati zadanim razdobljem za sve proizvode s digitalnim elementima. Umjesto toga, proizvođač bi trebao odrediti odgovarajuće razdoblje potpore s obzirom na kriterije iz članka 13. stavka 8.

127. U skladu s člankom 13. stavkom 19. proizvođači su dužni u trenutku kupnje na jasan i razumljiv način navesti datum završetka razdoblja potpore (barem mjesec i godinu). Osim toga su dužni nakon isteka razdoblja potpore korisnicima prikazati obavijest o tome ako je to tehnički izvedivo s obzirom na prirodu proizvoda s digitalnim elementima. Tom se obvezom nastoji osigurati transparentnost za korisnike u pogledu razdoblja u kojem mogu očekivati sigurnosnu potporu.

128. U slučaju softverskih proizvoda s digitalnim elementima, koji se često razvijaju i objavljuju iterativno i u kojima se bitno izmijenjene verzije mogu tijekom vremena često stavljati na tržište, razdoblje potpore mora se tumačiti s obzirom na taj razvojni model. Za svaku bitno izmijenjenu verziju softverskog proizvoda s digitalnim elementima stavljenu na tržište mora postojati prijavljeno razdoblje potpore koje je u skladu s člankom 13. stavkom 8. To uključuje minimalno razdoblje potpore od najmanje pet godina, osim ako je očekivano vrijeme upotrebe te verzije očito kraće, kao što je pojašnjeno i u uvodnoj izjavi 60. U odjeljku *5.1.* – Bitne izmjene i razdoblje potpore dodatno je pojašnjeno da, ako bitna izmjena ne prouzroči promjenu čimbenika koji su izvorno odredili očekivano vrijeme upotrebe proizvoda s digitalnim elementima, izvorno razdoblje potpore ostaje nepromijenjeno (tj. uključujući u slučajevima u kojima je preostalo razdoblje potpore kraće od pet godina).

129. Člankom 13. stavkom 10. predviđena je fleksibilnost za softverske proizvode s digitalnim elementima tako što se proizvođačima omogućuje da pod određenim uvjetima osiguraju ispunjavanje zahtjeva u pogledu postupanja s ranjivostima utvrđenog u dijelu II. točki 2. Priloga I. (razmatranje i otklanjanje ranjivosti) samo za verziju softverskog proizvoda s digitalnim elementima koja je posljednja stavljena na tržište. To je dopušteno ako korisnici verzija prethodno stavljenih na tržište imaju besplatan pristup posljednjoj verziji koja je stavljena na tržište i ne snose dodatne troškove za prilagodbu hardverskog i softverskog okruženja unutar kojeg se upotrebljavala izvorna verzija tog proizvoda.

130. Za potrebe članka 13. stavka 10. pojam „dodatni troškovi” trebalo bi tumačiti na praktičan i proporcionalan način, uzimajući u obzir uobičajenu i očekivanu praksu u održavanju i radu softvera. Ne obuhvaća razumne operativne radnje koje su svojstvene primjeni ažuriranja softvera ili održavanju sigurnog operativnog okruženja, kao što su vrijeme osoblja, rutinsko ispitivanje, prilagodbe konfiguracije ili nadogradnje temeljnih softverskih ovisnosti koje su potrebne za uklanjanje komponenti na kraju životnog vijeka ili poznatih sigurnosnih ranjivosti. Međutim, „dodatni troškovi” odnose se na opterećenja koja nadilaze ono što se obično može očekivati u kontekstu ažuriranja softvera, kao što su obvezna kupnja novog hardvera, zamjena infrastrukture ili temeljne promjene operativnog okruženja.

131. Kad je riječ o softverskim proizvodima s digitalnim elementima koji se stalno razvijaju, proizvođači mogu staviti na tržište uzastopne bitno izmijenjene verzije u relativno kratkim intervalima i očekivati da će ih korisnici redovito nadograđivati. U tim slučajevima prijavljeno razdoblje potpore za svaku bitno izmijenjenu verziju u trenutku stavljanja na tržište mora biti u skladu s člankom 13. stavkom 8. Drugim riječima, proizvođač mora prijaviti novo razdoblje potpore za tu bitno izmijenjenu verziju. Međutim, proizvođači se mogu osloniti na članak 13. stavak 10. kako bi prekinuli razmatranje i otklanjanje ranjivosti za ranije verzije nakon što se korisnicima omogući

nadogradnja softvera na noviju verziju besplatno i bez dodatnih troškova kako je prethodno navedeno, čak i ako stvarno razdoblje potpore za te ranije verzije zbog toga bude kraće ([18]). Na proizvođača se i dalje primjenjuju drugi zahtjevi u pogledu postupanja s ranjivostima iz dijela II. Priloga I. te obveze u pogledu izvješćivanja iz članka 14. Kako je objašnjeno i u uvodnoj izjavi 40., za sve bitno izmijenjene verzije softverskog proizvoda s digitalnim elementima koje su kasnije stavljene na tržište ti su zahtjevi, među ostalim, sljedeći: (i) održavanje politike koordiniranog otkrivanja ranjivosti; i (ii) mjere za lakšu razmjenu informacija o potencijalnim ranjivostima ([19]).

Primjer 52: Proizvođač stavlja model pametnog telefona na tržište EU-a i prijavljuje razdoblje potpore od X godina od datuma stavljanja na tržište u kojem će pružati sigurnosna ažuriranja kojima se otklanjaju ranjivosti. U tom razdoblju proizvođač objavljuje redovita ažuriranja softvera i bitno izmijenjene verzije operativnog sustava, koje korisnici mogu besplatno instalirati bez potrebe za novim hardverom.

Proizvođač može, u skladu s člankom 13. stavkom 10., razmotriti i otkloniti ranjivosti najnovije verzije operativnog sustava koja je stavljena na raspolaganje za taj model pametnog telefona, pod uvjetom da se ranije verzije mogu nadograditi besplatno i bez dodatnih troškova. U razdoblju potpore na proizvođača se i dalje primjenjuju drugi zahtjevi u pogledu postupanja s ranjivostima, kao što su koordinirano otkrivanje ranjivosti i mjere za razmjenu informacija.

Primjer 53: Proizvođač stavlja na tržište softverski proizvod s digitalnim elementima za poduzeća i svakih nekoliko mjeseci objavljuje bitno izmijenjene verzije, koje obuhvaćaju sigurnosna poboljšanja i nove značajke i omogućuju kompatibilnost s ažuriranim operativnim sustavima i platformama. Svaka se verzija stavlja na tržište s prijavljenim razdobljem potpore u skladu s člankom 13. stavkom 8. Proizvođač od korisnika očekuje redovitu nadogradnju u okviru uobičajenog rada i omogućuje besplatan pristup najnovijoj verziji. Za primjenu nadogradnji može biti potreban razuman operativni trud, kao što su ispitivanja ili prilagodbe konfiguracije, ali ne i dodatni troškovi, kao što su kupnja novog hardvera ili izmjene temeljne infrastrukture. U tom kontekstu proizvođač se može osloniti na članak 13. stavak 10. kako bi prekinuo razmatranje i otklanjanje ranjivosti za ranije verzije nakon što se korisnicima omogući nadogradnja softvera na najnoviju verziju, a da pritom i dalje ispunjava druge zahtjeve u pogledu postupanja s ranjivostima za sve kasnije bitno izmijenjene verzije.

5.1. **Bitne izmjene i razdoblje potpore**

132. Kako je utvrđeno u odjeljku 4.4. – Posljedice bitne izmjene, ako se izmjena proizvoda s digitalnim elementima smatra bitnom izmjenom i izmijenjeni se proizvod s digitalnim elementima stavlja na raspolaganje na tržištu, taj proizvod treba smatrati novim proizvodom za potrebe Akta o kibernetičkoj otpornosti, a stavljanje bitno izmijenjenog proizvoda s digitalnim elementima na raspolaganje na tržištu smatra se novim stavljanjem na tržište. Stoga je korisno pojasniti učinak koji to novo stavljanje na tržište ima na razdoblje potpore bitno izmijenjenog proizvoda s digitalnim elementima.

133. Razdoblje potpore bitno izmijenjenog proizvoda s digitalnim elementima trebalo bi odrediti s obzirom na očekivano vrijeme upotrebe tog proizvoda, uzimajući u obzir kriterije utvrđene u članku 13. stavku 8. Akta o kibernetičkoj otpornosti. Za bitnu izmjenu stoga bi bilo nužno provesti ponovnu procjenu na temelju tih kriterija, ali to ne znači automatski ponovno određivanje ili pak produljenje razdoblja potpore. Relevantno je pitanje utječe li bitna izmjena na čimbenike na temelju kojih je prvotno određeno očekivano vrijeme upotrebe tog proizvoda, a time i prvotno razdoblje potpore.

([18]) Valja podsjetiti na to da je člankom 13. stavkom 19. propisano da, 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. Stoga, ako se razmatranje i otklanjanje ranjivosti za prethodne verzije prekine, očekuje se da će korisnici koji nisu nadogradili na najnoviju verziju biti obaviješteni, ako je to tehnički izvedivo.

([19]) Valja napomenuti da, ako korisnici mogu nadograditi softver na najnoviju verziju bez dodatnih troškova, proizvođači mogu odlučiti da će ipak nastaviti razmatrati i otklanjati ranjivosti u ranijim verzijama tog softvera, među ostalim uz naplatu ili u okviru drugih komercijalnih aranžmana. U skladu s Aktom o kibernetičkoj otpornosti proizvođači nisu dužni besplatno pružati sigurnosna ažuriranja za te ranije verzije.

134. Ako bitna izmjena ne utječe na te čimbenike, kriteriji utvrđeni u članku 13. stavku 8. ukazuju na to da je očekivano vrijeme upotrebe isto kao ono prvotno određeno, a razdoblje potpore za izmijenjeni proizvod s digitalnim elementima trebalo bi odgovarati preostalom očekivanom vremenu upotrebe izvornog proizvoda stavljenog na tržište. O takvom je slučaju obično riječ ako je očekivano vrijeme upotrebe prije svega određeno na temelju čimbenika na koje izmjena ne utječe, kao što je fizička trajnost hardverskih komponenti, a bitna se izmjena odnosi samo na softversku funkcionalnost ili pozadinske usluge.

Primjer 54: Proizvođač stavlja na tržište robotski usisavač s očekivanim vremenom upotrebe od X godina, određenim na temelju prirode proizvoda s digitalnim elementima, uključujući fizičku trajnost i značajke istrošenosti hardverskih komponenti, te uzimajući u obzir razumna očekivanja korisnika u pogledu životnog vijeka tog proizvoda. Proizvođač određuje razdoblje potpore od X godina. Nakon Y godina proizvođač objavljuje ažuriranje softvera koje se smatra bitnom izmjenom, pri čemu dodaje nove načine čišćenja i funkcije navigacije. Ažuriranje softvera ne utječe na fizičku trajnost hardvera i ne mijenja razumna očekivanja korisnika u pogledu životnog vijeka tog proizvoda. Stoga kriteriji iz članka 13. stavka 8. ukazuju na isto očekivano vrijeme upotrebe. Razdoblje potpore za izmijenjeni proizvod s digitalnim elementima odgovara preostalom očekivanom vremenu upotrebe kako je određeno za izvorni proizvod.

Primjer 55: Proizvođač stavlja na tržište složeni industrijski strojarski proizvod s digitalnim elementima s pozadinskim sustavom u oblaku koji predstavlja rješenje za daljinsku obradu podataka. Očekivano vrijeme upotrebe je X godina, određeno s obzirom na razumna očekivanja korisnika i prirodu proizvoda s digitalnim elementima, kao što su fizička trajnost strojarske opreme i očekivano trošenje. Razdoblje potpore odgovara očekivanom vremenu upotrebe od X godina. Nakon Y godina proizvođač mijenja pozadinski sustav u oblaku (rješenje za daljinsku obradu podataka) uvođenjem novih API-ja i tokova podataka na način koji se smatra bitnom izmjenom proizvoda s digitalnim elementima, ali ne mijenja prirodu tog proizvoda niti utječe na očekivanja korisnika. Stoga kriteriji iz članka 13. stavka 8. ukazuju na isto očekivano vrijeme upotrebe. Razdoblje potpore za izmijenjeni proizvod s digitalnim elementima odgovara preostalom očekivanom vremenu upotrebe kako je određeno za izvorni proizvod.

135. Ako bitna izmjena utječe na čimbenike na temelju kojih je prvotno određeno očekivano vrijeme upotrebe proizvoda s digitalnim elementima, proizvođač bi trebao ponovno izračunati razdoblje potpore kako bi se uzelo u obzir novo očekivano vrijeme upotrebe, uz odgovarajuću primjenu kriterija iz članka 13. stavka 8. O takvoj situaciji može biti riječ u slučaju, na primjer, revitalizacijskih izmjena hardvera kojima se produljuje radni vijek tog proizvoda ili bitnog reprogramiranja ili ponovnog pisanja osnovnog softvera tog proizvoda kojim se bitno mijenja njegovo očekivano vrijeme upotrebe ([20]).

Primjer 56: Proizvođač stavlja na tržište programabilni logički kontroler s očekivanim vremenom upotrebe od X godina, određenim prije svega na temelju prirode proizvoda s digitalnim elementima i trajnosti osnovnog hardvera. Razdoblje potpore određuje se u skladu s tim. Nekoliko godina nakon prvog stavljanja na tržište proizvođač čini bitnu izmjenu koja se sastoji od zamjene ugrađene računalne platforme programabilnog logičkog kontrolera, uključujući procesor, memoriju i radno okruženje, novom generacijom komponenti projektiranih za znatno dulji radni vijek. Zbog izmjene se mijenjaju razumna očekivanja korisnika i priroda proizvoda s digitalnim elementima: korisnik programabilnog logičkog kontrolera sad može razumno očekivati da će kontroler moći ispunjavati svoju funkciju dulje od prvotno prijavljenog očekivanog vremena upotrebe, podržan novom računalnom platformom. Kriteriji iz članka 13. stavka 8. stoga ukazuju na dulje očekivano vrijeme upotrebe, a proizvođač u skladu s tim ponovno izračunava razdoblje potpore za taj konkretni kontroler.

6. **VAŽNI I KRITIČNI PROIZVODI S DIGITALNIM ELEMENTIMA**

136. U članku 7. stavku 1. Akta o kibernetičkoj otpornosti navodi se da se proizvodi s digitalnim elementima koji imaju osnovnu funkcionalnost kategorije proizvoda utvrđene u Prilogu III. Uredbi smatraju „važnim proizvodima s digitalnim elementima”. U Prilogu III. važni proizvodi s digitalnim elementima dodatno su podijeljeni u I. i II. razred. Slično tomu, u članku 8. stavku 1. navodi se da se proizvodi s digitalnim elementima koji imaju osnovnu funkcionalnost kategorije proizvoda utvrđene u Prilogu IV. Aktu o kibernetičkoj otpornosti smatraju „kritičnim proizvodima s digitalnim elementima” ([21]).

([20]) Valja podsjetiti na to da se, kao što je navedeno u odjeljku 4.1. – Fizički popravci, postupci obnove, održavanja ili popravka općenito ne smatraju bitnim izmjenama.

([21]) U Provedbenoj uredbi Komisije (EU) 2025/2392 utvrđen je tehnički opis kategorija važnih i kritičnih proizvoda.

137. Razvrstavanje proizvoda s digitalnim elementima u kategoriju važnih ili kritičnih proizvoda ili, s druge strane, u kategoriju „uobičajenih” proizvoda ([22]) relevantno je pri utvrđivanju postupka ocjenjivanja sukladnosti koji proizvođač mora slijediti, u skladu s člankom 32., prije nego što taj proizvod s digitalnim elementima može staviti na tržište. Konkretno, proizvodi s digitalnim elementima u kategoriji uobičajenih proizvoda uvijek se mogu osloniti na postupak unutarnje kontrole na temelju modula A („samoprocjena”) ([23]). Na važne proizvode s digitalnim elementima I. ili II. razreda i kritične proizvode s digitalnim elementima primjenjuju se stroži postupci ocjenjivanja sukladnosti. To ne uključuje važne proizvode s digitalnim elementima I. ili II. razreda koji se smatraju besplatnim softverom otvorenog koda i koji se stavljaju na tržište, za koje je proizvođačima u skladu s člankom 32. stavkom 5. dopušteno slijediti postupke za kategoriju uobičajenih proizvoda.

138. Pojam osnovne funkcionalnosti stoga je neophodan kako bi proizvođač mogao utvrditi primjenjivi sustav ocjenjivanja sukladnosti. Međutim, taj pojam nije izričito definiran u Aktu o kibernetičkoj otpornosti. Proizvodi s digitalnim elementima mogu obavljati niz funkcija, od kojih neke mogu biti pomoćne u odnosu na osnovnu funkcionalnost tog proizvoda i ne bi trebale utjecati na razvrstavanje proizvoda kao uobičajenog proizvoda / važnog proizvoda I. razreda / važnog proizvoda II. razreda / kritičnog proizvoda. Stoga je korisno pružiti više smjernica kako bi se proizvođačima pomoglo da pravilno provode odgovarajuće postupke ocjenjivanja sukladnosti, a tijelima za nadzor tržišta da osiguraju usklađeno izvršavanje Akta o kibernetičkoj otpornosti u cijelom EU-u.

6.1. **Osnovna funkcionalnost**

139. Osnovna funkcionalnost proizvoda s digitalnim elementima odnosi se na glavne značajke i tehničke mogućnosti tog proizvoda, bez kojih ne bi mogao ispuniti svoju namjenu. Može se ocijeniti uzimajući u obzir konkretan kontekst i uvjete upotrebe tog proizvoda, među ostalim informacije koje proizvođač navodi u uputama za upotrebu, promotivnim ili prodajnim materijalima i izjavama te tehničkoj dokumentaciji.

Primjer 57: Softverski proizvod s digitalnim elementima funkcionira kao apstrakcijski sloj na osnovnom hardveru i upravlja izvršenjem softverskih komponenti. Njegove su glavne značajke inicijalizacija hardvera i perifernih uređaja, upravljanje procesima i memorijom, kontrola ulaza i izlaza, raspoređivanje, raspodjela resursa te omogućivanje pristupa uslugama sustava i aplikacijskim programskim sučeljima (API) putem kojih aplikacije ostvaruju interakciju s hardverskim i softverskim resursima uređaja. U tehničkoj dokumentaciji navedeno je da proizvod s digitalnim elementima upravlja računalnim resursima, osigurava funkcioniranje konfiguracija sustava i pruža standardizirana sučelja za softverske module i povezane periferne uređaje. Proizvođač ističe da te mogućnosti omogućuju platformi da služi kao središnje softversko okruženje u kojem se aplikacije mogu pouzdano izvršavati. Proizvod s digitalnim elementima ima osnovnu funkcionalnost operativnog sustava, kako je opisano u točki 11. Priloga I. Provedbenoj uredbi (EU) 2025/2392.

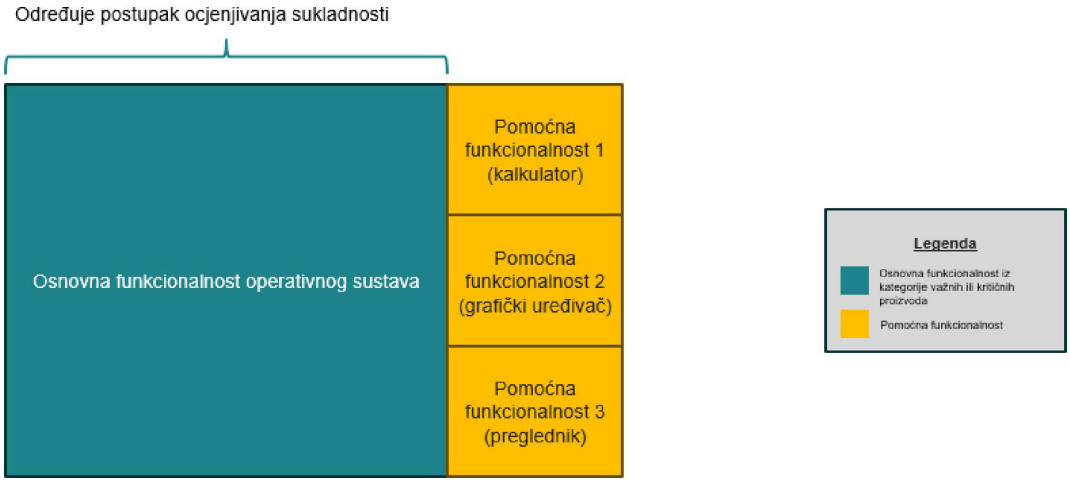
140. Funkcionalnost proizvoda s digitalnim elementima rijetko je ograničena isključivo na njegovu osnovnu funkcionalnost jer proizvodi s digitalnim elementima često, ako ne i uvijek, obavljaju dodatne funkcije koje ne doprinose osnovnoj funkcionalnosti proizvoda. To može uključivati i ugradnju komponenti koje same imaju funkcionalnost drugog važnog ili kritičnog proizvoda s digitalnim elementima. Međutim, činjenica da proizvod s digitalnim elementima obavlja funkcije koje se razlikuju od onih detaljno opisanih u tehničkim opisima važnih ili kritičnih proizvoda s digitalnim elementima ili koje dopunjuju te funkcije sama po sebi ne znači da proizvod ne može imati jednu takvu osnovnu funkcionalnost.

([22]) Kategorija „uobičajenih” proizvoda nije izraz koji je definiran u Aktu o kibernetičkoj otpornosti. Upotreba tog izraza u ovom dokumentu odnosi se na proizvode s digitalnim elementima koji nemaju osnovnu funkcionalnost kategorije proizvoda utvrđene u prilozima III. ili IV. Aktu o kibernetičkoj otpornosti i na koje se stoga primjenjuje sustav ocjenjivanja sukladnosti utvrđen u članku 32. stavku 1.

([23]) Proizvođač ipak uvijek može odabrati primjenu strožeg postupka ocjenjivanja sukladnosti, kako je utvrđeno u članku 32. stavku 1.

Slika 2:

Prikaz načina na koji osnovna funkcionalnost, a ne pomoćne funkcionalnosti, određuje primjenjivi postupak ocjenjivanja sukladnosti



141. Proizvod s digitalnim elementima može imati mogućnost obavljanja funkcija iz kategorije važnih ili kritičnih proizvoda, ali ipak imati osnovnu funkcionalnost drukčiju od funkcionalnosti takve kategorije proizvoda. U tim se slučajevima taj proizvod s digitalnim elementima ne bi smatrao važnim ili kritičnim proizvodom s digitalnim elementima. Kako je izričito navedeno u članku 7. stavku 1. Akta o kibernetičkoj otpornosti za važne proizvode s digitalnim elementima (a ista se logika primjenjuje na kritične proizvode s digitalnim elementima), integracija važnog ili kritičnog proizvoda s digitalnim elementima sama po sebi ne čini proizvod s digitalnim elementima važnim ili kritičnim proizvodom s digitalnim elementima.

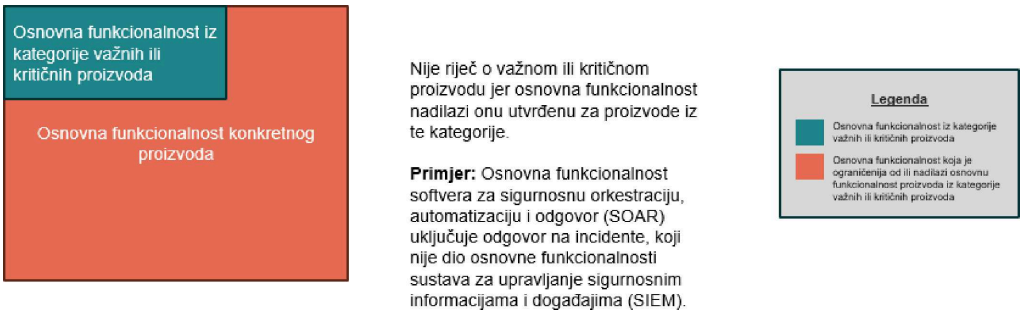
Primjer 58: U pametni telefon integriran je operativni sustav koji ima funkcionalnosti opisane u točki 11. Priloga I. Provedbenoj uredbi (EU) 2025/2392. Dok operativni sustav omogućuje upravljanje hardverskim resursima i izvršavanje softverskih aplikacija, pametni telefon u cjelini ima drukčiju osnovnu funkcionalnost (npr. omogućivanje korisnicima da komuniciraju i pristupaju informacijama i uslugama). Integracija operativnog sustava sama po sebi ne znači da pametni telefon ima osnovnu funkcionalnost operativnog sustava.

142. Neki proizvodi s digitalnim elementima mogu biti slični proizvodima iz kategorije važnih ili kritičnih proizvoda ili pripadati istoj općoj skupini proizvoda, ali njihova osnovna funkcionalnost može znatno nadilaziti osnovnu funkcionalnost iz te kategorije ili biti znatno ograničenija od nje. O takvoj situaciji nije riječ ako proizvod s digitalnim elementima uključuje dodatne funkcionalnosti koje samo dopunjuju ili poboljšavaju osnovnu funkcionalnost, koja sama po sebi odgovara funkcionalnosti iz kategorije važnih ili kritičnih proizvoda; u tim slučajevima proizvod s digitalnim elementima zadržava osnovnu funkcionalnost iz te kategorije i razvrstan je u skladu s tim. Ta bi se procjena trebala temeljiti na glavnim značajkama i tehničkim mogućnostima tog proizvoda, objektivno razmotrenima s obzirom na njegovu namjenu, a ne na načinu na koji je proizvod s digitalnim elementima opisan ili stavljen na tržište, ako taj opis ne odgovara stvarnim tehničkim svojstvima proizvoda.

Primjer 59: Softver za sigurnosnu orkestraciju, automatizaciju i odgovor (SOAR) često može obavljati funkcije proizvoda s digitalnim elementima iz kategorije „sustavi za upravljanje sigurnosnim informacijama i događajima (SIEM)”, odnosno prikupljati podatke iz više izvora, analizirati ih, povezivati i prikazivati kao upotrebljive informacije za sigurnosne potrebe. Međutim, osnovna funkcionalnost softvera znatno nadilazi funkcionalnost SIEM-a jer uključuje usluge kao što je odgovor na incidente kao ključne elemente njegovih tehničkih mogućnosti. Stoga se općenito ne smatra da SOAR ima osnovnu funkcionalnost SIEM-a.

Slika 3:

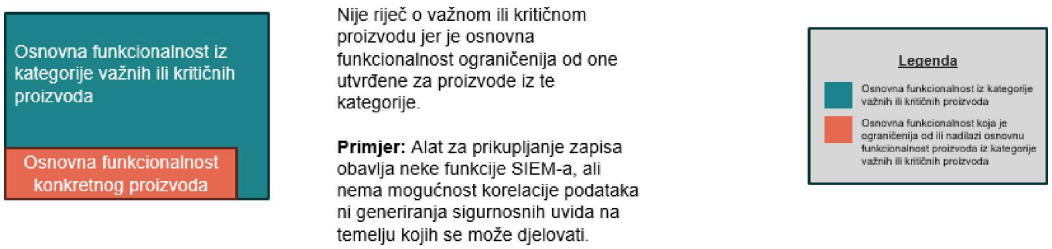
Prikaz osnovne funkcionalnosti proizvoda s digitalnim elementima koja znatno nadilazi funkcionalnosti utvrđene za kategoriju važnih ili kritičnih proizvoda



Primjer 60: Određeni alati za prikupljanje i vizualizaciju zapisa mogu učitavati podatke iz zapisa i izrađivati osnovne nadzorne ploče s pregledom događaja u sustavu. Iako se tim alatima mogu poduprijeti aktivnosti praćenja sigurnosti, njihova osnovna funkcionalnost ograničenija je od funkcionalnosti SIEM-a jer nemaju mogućnost korelacije podataka ni generiranja sigurnosnih uvida na temelju kojih se može djelovati. Stoga se općenito ne smatra da ti alati imaju osnovnu funkcionalnost SIEM-a.

Slika 4:

Prikaz osnovne funkcionalnosti proizvoda s digitalnim elementima koja je znatno ograničenija od funkcionalnosti utvrđene za kategoriju važnih ili kritičnih proizvoda

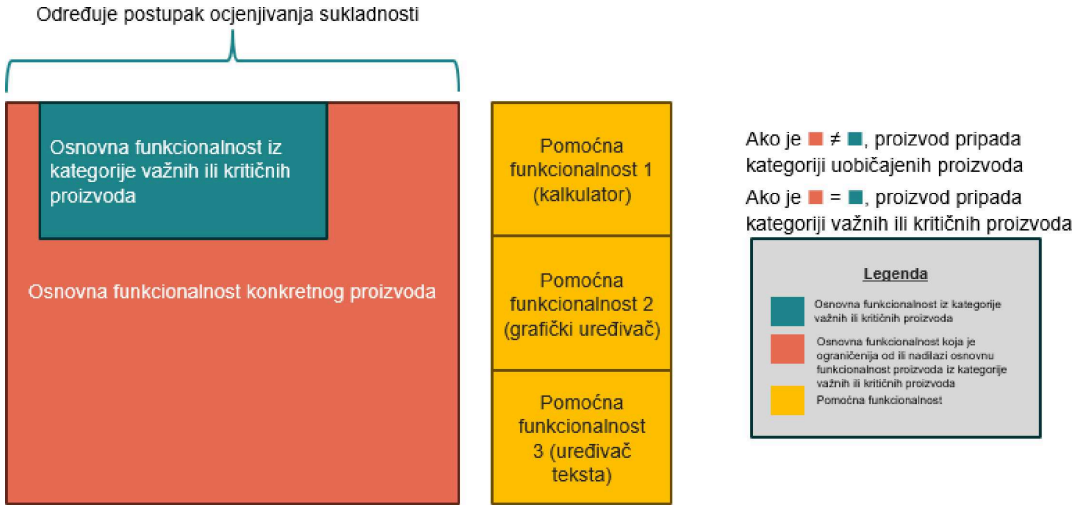


143. Proizvođač ne smije pogrešno prikazivati osnovnu funkcionalnost svojeg proizvoda s digitalnim elementima kako bi izbjegao sustav ocjenjivanja sukladnosti koji se primjenjuje na važne ili kritične proizvode s digitalnim elementima, npr. prikazivanjem uloge određenih funkcionalnosti manjom ili većom nego što stvarno jest kako bi određena osnovna funkcionalnost proizvoda znatno nadilazila ili bila znatno ograničenija od one proizvoda iz odgovarajuće kategorije. Primjer takvog postupanja bilo bi postojanje jasnih nedosljednosti između promotivnih materijala, uputa za upotrebu i tehničke dokumentacije.

144. Proizvod s digitalnim elementima ne smije imati više od jedne osnovne funkcionalnosti za potrebe utvrđivanja primjenjivog sustava ocjenjivanja sukladnosti. U skladu s Prilogom VII. Aktu o kibernetičkoj otpornosti proizvođači su u tehničkoj dokumentaciji proizvoda dužni opisati namjenu svojeg proizvoda s digitalnim elementima i postupak ocjenjivanja sukladnosti koji su proveli. Stoga bi osnovnu funkcionalnost proizvoda trebalo jasno utvrditi. To proizvođačima omogućuje pravilno utvrđivanje primjenjivog sustava ocjenjivanja sukladnosti, a tijelima za nadzor tržišta nadzor i provjeru pravilne primjene Uredbe.

Slika 5:

Prikaz načina na koji osnovna funkcionalnost konkretnog proizvoda s digitalnim elementima određuje razred proizvoda, a time i primjenjivi postupak ocjenjivanja sukladnosti



145. Neki proizvodi s digitalnim elementima stavljaju se na tržište kao pojedinačni proizvodi s digitalnim elementima, ali se sastoje od različitih modula sa zasebnim funkcionalnostima. Ako proizvođač te module na raspolaganje na tržištu stavlja zasebno, na primjer tako da ih nudi za zasebnu kupnju, licenciranje ili pretplatu, ti su moduli sami po sebi samostalni proizvodi s digitalnim elementima. Stoga se razvrstavaju na temelju njihovih osnovnih funkcionalnosti (i na njih se primjenjuje odgovarajući sustav ocjenjivanja sukladnosti određen na temelju osnovne funkcionalnosti svakog modula). To ne vrijedi za module koji se isporučuju isključivo kao komponente integriranog proizvoda s digitalnim elementima i koji nisu zasebno dostupni; u tim se slučajevima osnovna funkcionalnost utvrđuje na razini integriranog proizvoda s digitalnim elementima.

Primjer 61: Proizvođač stavlja na tržište jedinstveni sigurnosni paket u kojem kombinira više modula, uključujući SIEM, sustav za otkrivanje neovlaštenog upada i analitički modul. Te module nudi i uz zasebne pretplate. U tom je scenariju svaki modul zaseban proizvod s digitalnim elementima i razvrstava se na temelju svoje osnovne funkcionalnosti. Na modul za SIEM primjenjuje se sustav ocjenjivanja sukladnosti za važne proizvode s digitalnim elementima I. razreda jer njegova osnovna funkcionalnost odgovara kategoriji „sustavi za upravljanje sigurnosnim informacijama i događajima (SIEM)”. Na sustav za otkrivanje neovlaštenog upada primjenjuje se sustav ocjenjivanja sukladnosti za važne proizvode s digitalnim elementima II. razreda jer njegova osnovna funkcionalnost odgovara kategoriji „vatrozidovi, sustavi za otkrivanje i sprečavanje neovlaštenih upada”. Na analitički modul primjenjuje se sustav ocjenjivanja sukladnosti za „uobičajene” proizvode s digitalnim elementima jer njegova osnovna funkcionalnost nije obuhvaćena kategorijom važnih ili kritičnih proizvoda.

146. Zbog neispunjavanja obveza utvrđenih u članku 32. Akta o kibernetičkoj otpornosti mogu se izreći upravne novčane kazne u skladu s člankom 64. stavkom 3.

6.2. Ocjenjivanje sukladnosti važnih i kritičnih proizvoda s digitalnim elementima

147. Nakon što proizvođač utvrdi osnovnu funkcionalnost svojeg proizvoda s digitalnim elementima, mora provesti jedan od primjenjivih postupaka ocjenjivanja sukladnosti. Mora osigurati da proizvod s digitalnim elementima u cjelini ispunjava bitne zahtjeve, pri čemu, prema potrebi, treba uzeti u obzir sigurnost komponenti ili funkcionalnosti koje su u njega integrirane.

148. Stroži postupak ocjenjivanja sukladnosti, uz sudjelovanje treće strane (na temelju modula B+C, modula H ili programa kibernetičkosigurnosne certifikacije), obvezan je za važne proizvode s digitalnim elementima II. razreda (osim onih koji se smatraju besplatnim softverom otvorenog koda u skladu s člankom 32. stavkom 5.) i za kritične proizvode s digitalnim elementima ([24]). S druge strane, važni proizvodi s digitalnim elementima I. razreda (osim onih koji se smatraju besplatnim softverom otvorenog koda u skladu s člankom 32. stavkom 5.) moraju proći postupak ocjenjivanja sukladnosti koji provodi treća strana samo ako proizvođač nije primijenio ili je samo djelomično primijenio relevantne usklađene norme na koje su upućivanja objavljena u *Službenom listu Europske unije* (dalje u tekstu „usklađene norme"), zajedničke specifikacije ili europske programe kibernetičkosigurnosne certifikacije na barem „znatnoj" razini jamstva ([25]).

149. Stoga, kako bi se na važan proizvod s digitalnim elementima I. razreda mogao primjenjivati postupak unutarnje kontrole, (i) moraju biti ispunjeni svi primjenjivi zahtjevi relevantne usklađene norme; i (ii) područje primjene norme mora obuhvaćati barem sve kibernetičkosigurnosne rizike povezane s osnovnom funkcionalnošću tog proizvoda.

150. Opseg proizvoda s digitalnim elementima može biti širi od opsega predviđenog relevantnom usklađenom normom, a te dodatne funkcije mogu dovesti do drukčijih ili dodatnih kibernetičkosigurnosnih rizika. Proizvođač je uvijek dužan provesti procjenu rizika u skladu s člankom 13. stavkom 2. i stoga bi trebao provjeriti obuhvaća li primjena usklađene norme sve rizike povezane s proizvodom s digitalnim elementima. Ako primjena norme ne obuhvaća sve rizike, proizvođač bi drugim sredstvima trebao osigurati da njegov proizvod s digitalnim elementima ispunjava bitne zahtjeve.

151. Stoga, ako je proizvođač važnog proizvoda s digitalnim elementima I. razreda primijenio relevantnu usklađenu normu koja obuhvaća rizike povezane s osnovnom funkcionalnošću tog proizvoda, može odlučiti primijeniti postupak unutarnje kontrole za dokazivanje sukladnosti svojeg proizvoda. U okviru aktivnosti ocjenjivanja sukladnosti proizvođač će svejedno morati dokazati da su uklonjeni svi rizici koji se odnose na njegov proizvod s digitalnim elementima. Stoga, ako postoji razlika između područja primjene usklađene norme i opsega proizvoda s digitalnim elementima u cjelini, proizvođač svakako mora dokumentirati koje je dodatne mjere proveo za postupanje s tim rizicima.

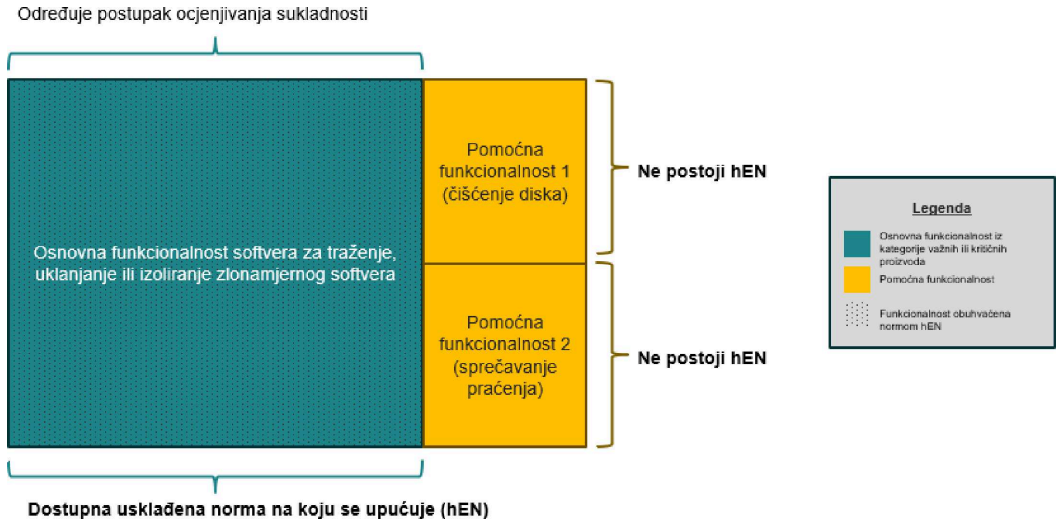
Primjer 62: Antivirusni program ima osnovnu funkcionalnost softvera za traženje, uklanjanje ili izoliranje zlonamjernog softvera, kako je opisano u točki 4. Priloga I. Provedbenoj uredbi (EU) 2025/2392. Taj proizvod s digitalnim elementima ima i dodatne značajke, odnosno funkciju čišćenja diska i funkciju sprečavanja praćenja koja štiti korisnika pri pretraživanju interneta. Proizvođač provodi procjenu rizika kojom je obuhvaćen proizvod s digitalnim elementima u cjelini, uključujući osnovnu funkcionalnost antivirusnog programa, funkciju čišćenja diska i funkciju sprečavanja praćenja. Primjenjuje usklađenu normu koja obuhvaća rizike povezane s osnovnom funkcionalnošću antivirusnog programa i dodatne mjere za uklanjanje rizika koji proizlaze iz dodatnih funkcija. Za ocjenjivanje sukladnosti proizvođač smije primijeniti postupak unutarnje kontrole koji obuhvaća proizvod s digitalnim elementima u cjelini, uključujući funkcije čišćenja diska i sprečavanja praćenja.

([24]) To vrijedi i za primjenu europskog programa kibernetičkosigurnosne certifikacije na barem „znatnoj" razini jamstva jer je potrebno sudjelovanje certifikacijskog tijela treće strane.

([25]) Radi sažetosti u ostatku ovog odjeljka spominju se samo usklađene norme na koje su upućivanja objavljena u *Službenom listu Europske unije*. Međutim, iste se smjernice odnose i na zajedničke specifikacije donesene u skladu s člankom 27. stavkom 2. i na europske programe kibernetičkosigurnosne certifikacije ako ih Komisija utvrdi delegiranim aktima u skladu s člankom 27. stavkom 9.

Slika 6:

Prikaz načina na koji primjena navedene usklađene norme koja obuhvaća samo osnovnu funkcionalnost određuje primjenjivi postupak ocjenjivanja sukladnosti



152. To vrijedi i ako je u proizvod s digitalnim elementima integrirana dodatna funkcija koja je i sama funkcija drugog važnog ili kritičnog proizvoda s digitalnim elementima. Naime, osnovna funkcionalnost proizvoda s digitalnim elementima u cjelini, a ne funkcionalnost pojedinačnih integriranih komponenti, određuje pripada li proizvod s digitalnim elementima kategoriji važnih ili kritičnih proizvoda (a time i koji se sustav ocjenjivanja sukladnosti primjenjuje). Na primjer, ako proizvod s digitalnim elementima ima osnovnu funkcionalnost važnog proizvoda s digitalnim elementima I. razreda, na taj se proizvod u cjelini primjenjuje sustav ocjenjivanja sukladnosti koji se primjenjuje na važne proizvode s digitalnim elementima I. razreda, iako sadržava komponentu koja je sama po sebi kritični proizvod s digitalnim elementima. U tim slučajevima, ako proizvođač primjenjuje usklađenu normu koja obuhvaća rizike povezane s osnovnom funkcionalnošću tog proizvoda, smije primijeniti postupak unutarnje kontrole.

Primjer 63: Hardverski proizvod s digitalnim elementima ima osnovnu funkcionalnost rutera, kako je opisano u točki 12. Priloga I. Provedbenoj uredbi (EU) 2025/2392. Taj proizvod s digitalnim elementima ima i dodatne funkcionalnosti, uključujući mogućnosti vatrozida, jer sadržava komponentu vatrozida. Proizvođač provodi procjenu rizika koja obuhvaća proizvod s digitalnim elementima u cjelini, uključujući osnovnu funkcionalnost rutera i funkcionalnost vatrozida. Primjenjuje usklađenu normu koja obuhvaća rizike povezane s osnovnom funkcionalnošću rutera i dodatne mjere za uklanjanje rizika koji proizlaze iz dodatnih funkcija. Na primjer, proizvođač može primijeniti usklađenu normu za vatrozidove kako bi obuhvatio rizike povezane s funkcionalnošću vatrozida. Za ocjenjivanje sukladnosti proizvođač smije primijeniti postupak unutarnje kontrole koji obuhvaća proizvod s digitalnim elementima u cjelini, uključujući funkcionalnost vatrozida.

6.3. Značenje za pretpostavku sukladnosti

153. Člankom 27. stavkom 1. Akta o kibernetičkoj otpornosti utvrđeno je da se 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 da su sukladni s bitnim zahtjevima Akta o kibernetičkoj otpornosti obuhvaćenima tim normama ili njihovim dijelovima ([26]). Člankom 27. stavkom 5. ta se

([26]) Kao što je jasno navedeno u točki 4.1.2.2. Plavog vodiča, „[u] zakonodavnim propisima za usklađivanje povezanima s rizikom […] proizvođači uvijek, čak i ako upotrebljavaju usklađene norme s upućivanjima objavljenima u Dzienniku Urzędowym Unii Europejskiej-u, snose potpunu odgovornost za procjenu svih rizika svojih proizvoda kako bi utvrdili koji su temeljni (ili ostali) zahtjevi relevantni. Nakon te procjene proizvođač može odlučiti o primjeni tehničkih specifikacija navedenih u usklađenim normama s upućivanjima objavljenima u Dzienniku Urzędowym Unii Europejskiej-u za provedbu ‚mjera za smanjenje rizika' koje su navedene u usklađenim normama."

pretpostavka sukladnosti proširuje na proizvode s digitalnim elementima i procese koje je proizvođač uspostavio i koji su sukladni sa zajedničkim specifikacijama koje je Komisija donijela provedbenim aktima, a člankom 27. stavkom 8. utvrđuje se pretpostavka sukladnosti za proizvode s digitalnim elementima i procese koje je uspostavio proizvođač i za koje su izdani EU izjava o sukladnosti ili certifikat u okviru europskog programa kibernetičkosigurnosne certifikacije donesenog u skladu s Uredbom (EU) 2019/881, ako je to utvrđeno u delegiranim aktima u skladu s člankom 27. stavkom 9. ([27])

154. Stoga, ako je proizvođač primijenio usklađenu normu na koju su upućivanja objavljena u Službenom listu, na njega se primjenjuje pretpostavka sukladnosti za rizike obuhvaćene tom normom. O takvoj je situaciji riječ, na primjer, ako usklađena norma na koju se upućuje obuhvaća sve rizike povezane s osnovnom funkcionalnošću proizvoda s digitalnim elementima i ako ne postoje dodatne funkcionalnosti koje mogu dovesti do kibernetičkosigurnosnih rizika. Na primjer, očekuje se da će se primjenom usklađene norme za rutere ukloniti barem rizici povezani s osnovnom funkcionalnošću tih proizvoda s digitalnim elementima. Ako takav proizvod ne sadržava dodatne funkcionalnosti ili ako te dodatne funkcionalnosti ne mogu dovesti do rizika koji nisu obuhvaćeni normom, na proizvod s digitalnim elementima može se primjenjivati pretpostavka sukladnosti.

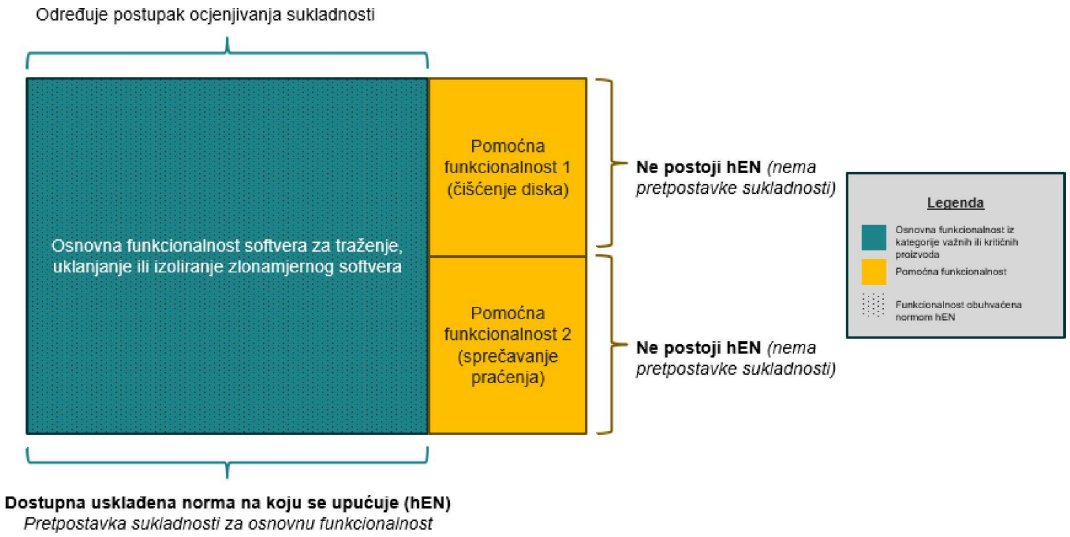
155. U slučajevima navedenima u točkama 151. i 152. proizvođač smije primijeniti postupak unutarnje kontrole jer usklađena norma obuhvaća rizike povezane s osnovnom funkcionalnošću proizvoda s digitalnim elementima. Međutim, proizvodi s digitalnim elementima opisani u tim primjerima mogu imati širi opseg od područja primjene usklađenih normi, a dodatne funkcionalnosti mogu dovesti do kibernetičkosigurnosnih rizika koji nisu obuhvaćeni relevantnom usklađenom normom. Stoga se na te proizvode s digitalnim elementima možda neće primjenjivati pretpostavka sukladnosti za te dodatne funkcionalnosti.

Primjer 64: Antivirusni program ima osnovnu funkcionalnost softvera za traženje, uklanjanje ili izoliranje zlonamjernog softvera, a rizici povezani s tom osnovnom funkcionalnošću obuhvaćeni su usklađenom normom. Taj proizvod s digitalnim elementima ima i dodatne funkcionalnosti, odnosno funkciju čišćenja diska i funkciju sprečavanja praćenja koja štiti korisnika pri pretraživanju interneta, čiji rizici nisu obuhvaćeni usklađenom normom. Ako se primjenjuje usklađena norma, proizvođač za ocjenjivanje sukladnosti smije primijeniti postupak unutarnje kontrole. Na njega će se primjenjivati pretpostavka sukladnosti za rizike povezane s osnovnom funkcionalnošću tog proizvoda, ali ne i za rizike povezane s dodatnim funkcionalnostima.

([27]) Kao što je prethodno navedeno, radi sažetosti u ostatku ovog odjeljka spominju se samo usklađene norme na koje su upućivanja objavljena u Službenom listu. Međutim, iste se smjernice odnose i na zajedničke specifikacije i europske programe kibernetičkosigurnosne certifikacije.

Slika 7:

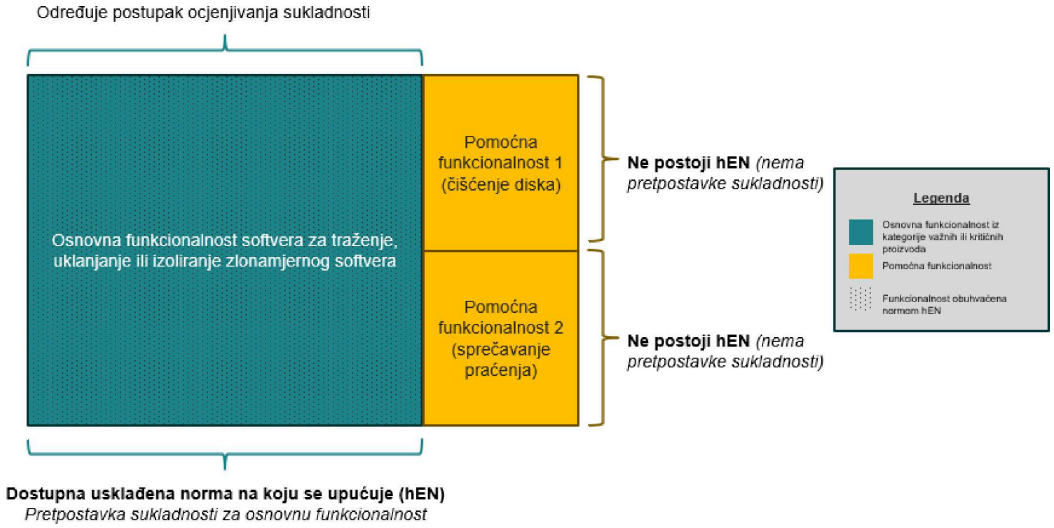
Usklađena norma omogućuje primjenu pretpostavke sukladnosti za osnovnu funkcionalnost jer obuhvaća sve rizike povezane s tom osnovnom funkcionalnošću, ali ne i za pomoćne funkcionalnosti



Primjer 65: U istom scenariju kao u prethodnom primjeru usklađena norma sad je ažurirana kako bi se obuhvatili i rizici povezani s jednom od dodatnih funkcionalnosti, odnosno funkcijom čišćenja diska, ali ne i drugom funkcijom (tj. funkcijom sprečavanja praćenja). Ako se primjenjuje usklađena norma, proizvođač za ocjenjivanje sukladnosti smije primijeniti postupak unutarnje kontrole. Na njega će se primjenjivati pretpostavka sukladnosti za rizike povezane s osnovnom funkcionalnošću tog proizvoda i funkcionalnošću čišćenja diska, ali ne i za rizike povezane s funkcionalnošću sprečavanja praćenja.

Slika 8:

Usklađena norma omogućuje primjenu pretpostavke sukladnosti za osnovnu funkcionalnost i pomoćnu funkcionalnost 1 jer obuhvaća sve rizike povezane s te dvije funkcionalnosti, ali ne i za pomoćnu funkcionalnost 2.



7. **PROCJENA KIBERNETIČKOSIGURNOSNIH RIZIKA I INTEGRACIJA PROIZVODA S DIGITALNIM ELEMENTIMA I KOMPONENTI**

7.1. **Procjena i postupanje s kibernetičkosigurnosnim rizicima**

156. U okviru procjene kibernetičkosigurnosnih rizika iz članka 13. stavka 2. Akta o kibernetičkoj otpornosti proizvođač je dužan utvrditi relevantne rizike i procijeniti njihov mogući učinak na proizvod s digitalnim elementima. Proizvođači moraju provesti i odgovarajuće mjere za uklanjanje tih rizika u skladu s bitnim zahtjevima iz Priloga I.

157. U kontekstu organizacijskog upravljanja rizicima rizici se obično procjenjuju na temelju kriterija prihvatljivosti koji proizlaze iz unutarnjih ciljeva organizacije ili njezine sklonosti preuzimanju rizika. Međutim, na temelju Akta o kibernetičkoj otpornosti preostali kibernetički sigurnosni rizik trebalo bi procijeniti s obzirom na zahtjev da proizvod s digitalnim elementima koji je stavljen na tržište jamči odgovarajuću razinu kibernetičke sigurnosti na temelju rizika, pri čemu treba uzeti u obzir njegovu namjenu i razumno predvidljivu upotrebu.

158. U skladu s tim, proizvođačeva unutarnja tolerancija na rizik, poslovna strategija ili aspekti troškova nisu relevantni za utvrđivanje toga jesu li rizici uklonjeni. Za potrebe članka 13. stavaka 2. i 3. proizvođači moraju moći utvrditi jesu li utvrđeni kibernetičkosigurnosni rizici u dovoljnoj mjeri uklonjeni primjenom bitnih zahtjeva iz dijela I. Priloga I. s obzirom na namjenu, razumno predvidljivu upotrebu i uvjete upotrebe, uključujući, prema potrebi, operativno okruženje (npr. predviđeni korisnici proizvoda s digitalnim elementima) i sredstva koja treba zaštititi, pri čemu treba uzeti u obzir očekivano trajanje upotrebe proizvoda s digitalnim elementima.

159. Preostali kibernetički sigurnosni rizik sastavni je rezultat procjene rizika i postupanja s rizicima. Poznato je da se kibernetičkosigurnosni rizici u praksi ne mogu u potpunosti ukloniti. Međutim, postojanje preostalog rizika ne znači da proizvođač može prema vlastitom nahođenju prihvatiti bilo koji rizik. Proizvod s digitalnim elementima može se staviti na tržište samo ako su preostali rizici, nakon što se poduzmu odgovarajuće mjere, u dovoljnoj mjeri uklonjeni primjenom bitnih zahtjeva, s obzirom na namjenu i razumno predvidljivu upotrebu proizvoda s digitalnim elementima.

160. U skladu s člankom 13. stavkom 3., ako se utvrde kibernetičkosigurnosni rizici, proizvođači su dužni na njih odgovoriti odgovarajućim mjerama, među ostalim na razini proizvoda. Ovisno o okolnostima, to može uključivati, na primjer, smanjenje površine napada, provedbu tehničkih zaštitnih mjera, ograničavanje ili prilagodbu funkcionalnosti ili preciznije definiranje namjene proizvoda s digitalnim elementima. Proizvođači mogu poduzeti i korake za oblikovanje razumno predvidljive upotrebe proizvoda s digitalnim elementima, na primjer obavješćivanjem o riziku, smjernicama za korisnike ili projektiranjem korisničkog sučelja, kako bi usmjerili ponašanje korisnika prema sigurnim obrascima upotrebe.

161. Aktom o kibernetičkoj otpornosti ne predviđa se prijenos kibernetičkosigurnosnog rizika ili odgovornosti na korisnike ili treće strane kako bi se nadoknadili nedostaci u projektiranju proizvoda ili opravdalo neuklanjanje kibernetičkosigurnosnih rizika. Obveza stavljanja na tržište sigurnog proizvoda s digitalnim elementima i dokazivanja sukladnosti s bitnim zahtjevima ostaje na proizvođaču.

162. Informacije i upute koje se pružaju korisnicima mogu se upotrebljavati za potporu sigurnom uvođenju i radu proizvoda s digitalnim elementima, među ostalim ako je proizvođač odlučio ograničiti namjenu tog proizvoda na pouzdana okruženja, te za informiranje korisnika o preostalim rizicima na način koji je primjeren prirodi proizvoda s digitalnim elementima i njegovim predviđenim korisnicima.

Primjer 66: Proizvođač razvija industrijski senzor za upotrebu u pouzdanim okruženjima. Za potrebe pravilnog funkcioniranja senzora proizvođač ne provodi mjere za zaštitu samog senzora od fizičkih napada. Kako bi se ublažili povezani rizici utvrđeni u procjeni rizika, proizvođač ograničava namjenu senzora na upotrebu isključivo u pouzdanim okruženjima u kojima je onemogućen neovlašten fizički pristup proizvodu s digitalnim elementima. U informacijama i uputama za korisnike jasno se navode ta ograničenja upotrebe senzora na način koji je primjeren prirodi proizvoda s digitalnim elementima i njegovim predviđenim korisnicima.

Primjer 67: Proizvođač razvija softversku aplikaciju za profesionalnu upotrebu na stolnim i mobilnim uređajima kojima se upravlja. Aplikacija obrađuje lokalno pohranjene osjetljive podatke i sadržaj koji su izradili korisnici. U okviru procjene rizika proizvođač utvrđuje rizik od neovlaštenog pristupa tim podacima ako su pohranjeni na uređaju u nešifriranom obliku. Umjesto projektiranja i implementacije vlastitog mehanizma šifriranja unutar same aplikacije, proizvođač se odlučuje osloniti na funkcije šifriranja i upravljanja ključevima koje izvorno pruža operativni sustav u kojem bi aplikacija trebala raditi jer su ugrađene kriptografske usluge tog operativnog sustava pouzdane i redovito se održavaju.

163. Ako se u okviru procjene kibernetičkosigurnosnih rizika utvrde rizici koji se ne mogu adekvatno ukloniti odgovarajućim mjerama, za usklađenost s Aktom o kibernetičkoj otpornosti mogu biti potrebne promjene u projektiranju, funkcionalnostima ili namjeni proizvoda s digitalnim elementima. Aspekti koji se odnose isključivo na troškove ili komercijalnu izvedivost nisu dovoljna osnova za neuklanjanje tih rizika ako bi se time spriječilo da proizvod s digitalnim elementima ispuni bitne zahtjeve.

7.2. Projektiranje, razvoj i proizvodnja proizvoda s digitalnim elementima tako da osiguravaju odgovarajuću razinu kibernetičke sigurnosti na temelju rizika

164. Bitnim zahtjevom u pogledu kibernetičke sigurnosti iz dijela I. točke 1. Priloga I. Aktu o kibernetičkoj otpornosti predviđa se da se proizvodi s digitalnim elementima projektiraju, razvijaju i proizvode tako da osiguravaju odgovarajuću razinu kibernetičke sigurnosti na temelju rizika.

165. Svrha je tog bitnog zahtjeva uklanjanje svih kibernetičkosigurnosnih rizika koji su utvrđeni u okviru procjene takvih rizika. To prije svega uključuje kibernetičkosigurnosne rizike koji nisu na odgovarajući način uzeti u obzir u okviru primjene drugih bitnih zahtjeva iz dijela I. Priloga I. osim onih iz točke 1. Taj se bitni zahtjev razlikuje od pravne obveze provedbe procjene kibernetičkosigurnosnih rizika, koju treba provesti u skladu s člankom 13. stavkom 2.

166. Ako se sa svim relevantnim kibernetičkosigurnosnim rizicima povezanima s proizvodom s digitalnim elementima postupa tako da se provode odgovarajuće mjere za ispunjavanje primjenjivih drugih bitnih zahtjeva osim onih iz točke 1., bitni zahtjev iz dijela I. točke 1. Priloga I. smatra se ispunjenim. S druge strane, ako se u okviru procjene kibernetičkosigurnosnih rizika utvrde dodatni rizici koji nisu u potpunosti obuhvaćeni takvim mjerama, proizvođači su dužni provesti odgovarajuće mjere za proizvod s digitalnim elementima kako bi uklonili te rizike i ispunili bitni zahtjev iz dijela I. točke 1. Priloga I. U praksi se u većini slučajeva očekuje da će ispunjavanje drugih bitnih zahtjeva rezultirati ispunjavanjem i tog zahtjeva.

7.3. Procjena rizika i dužna pažnja u kontekstu vanjskih ovisnosti i integriranih komponenti

167. Aktom o kibernetičkoj otpornosti utvrđuju se dvije različite, ali komplementarne obveze proizvođača u pogledu upravljanja kibernetičkim sigurnosnim rizicima. Prvo, u skladu s člankom 13. stavkom 2. proizvođač je dužan provesti procjenu kibernetičkosigurnosnih rizika za sam proizvod s digitalnim elementima. Drugo, člankom 13. stavkom 5. uvodi se obveza postupanja s dužnom pažnjom u pogledu integriranih komponenti. Svrha je tih dviju obveza zajedno zajamčiti sigurnost proizvoda s digitalnim elementima, među ostalim i u slučajevima u kojima se oslanja na rješenja za daljinsku obradu podataka, usluge na daljinu ili softverske ili hardverske komponente trećih strana.

168. Procjena kibernetičkosigurnosnih rizika odnosi se na utvrđivanje i upravljanje relevantnim rizicima koji mogu utjecati na proizvod s digitalnim elementima, uključujući rizike koji potječu izvan samog proizvoda, kao što su vanjske mreže, čimbenici iz okruženja ili drugi vanjski aspekti koji mogu utjecati na proizvod s digitalnim elementima ili na koje se proizvod oslanja. Kad je riječ o takvim vanjskim rizicima, Aktom o kibernetičkoj otpornosti ne uvodi se obveza za proizvođače da kontroliraju ili upravljaju vanjskim okruženjem. Umjesto toga, proizvođači su dužni utvrditi takve rizike i ublažiti ih u okviru projektiranja i razvoja samog proizvoda s digitalnim elementima. To uključuje primjenu odgovarajućih bitnih zahtjeva utvrđenih u dijelu I. Priloga I. i, prema potrebi, pružanje informacija i uputa korisnicima o rizicima povezanima s integracijom ili uvođenjem.

169. Na primjer, proizvođač može utvrditi rizik od toga da bi neovlaštene osobe mogle dobiti pristup pozadinskim sustavima koji nisu dio samog proizvoda s digitalnim elementima dok je proizvod u radu te pokušati poslati zlonamjerne naredbe proizvodu s digitalnim elementima. Takvi pozadinski sustavi, ako ih nije projektirao i razvio proizvođač ili ako nisu pod njegovom odgovornošću ili ako ne podržavaju jednu od funkcija proizvoda s digitalnim elementima, ne predstavljaju rješenja za daljinsku obradu podataka i stoga nisu obuhvaćeni opsegom proizvoda s digitalnim elementima za potrebe Akta o kibernetičkoj otpornosti. Međutim, u skladu s Aktom o kibernetičkoj otpornosti proizvođač je dužan ukloniti rizik koji oni mogu predstavljati mjerama na razini proizvoda, kao što su zahtijevanje kriptografske autentifikacije naredbi poslanih na daljinu, provjera cjelovitosti promjena konfiguracije ili generiranje zapisa ili upozorenja relevantnih za sigurnost ako se otkrije neuobičajeno ponašanje. Slično tomu, ako proizvođač utvrdi rizik koji proizlazi iz nedostupnosti takve vanjske usluge, na primjer zbog prekida napajanja ili kvarova infrastrukture, u skladu s Aktom o kibernetičkoj otpornosti može biti potrebna provedba mjera ublažavanja takvih kibernetičkosigurnosnih rizika na razini proizvoda, npr. osiguravanje da zbog prekida napajanja ne dođe do prelaska proizvoda s digitalnim elementima u nesigurna stanja. U tim slučajevima Aktom o kibernetičkoj otpornosti uređuje se način na koji proizvod s digitalnim elementima odgovara na te vanjske rizike; njime se ne uvode obveze u pogledu organizacije pozadinske infrastrukture, osiguravanja osoblja za nju i njezina rada niti se ta infrastruktura smatra dijelom proizvoda s digitalnim elementima.

170. Dužna pažnja odnosi se na elemente koji čine dio samog proizvoda s digitalnim elementima, konkretno na integrirane softverske ili hardverske komponente koje isporučuje treća strana. Proizvođači su dužni poduzeti odgovarajuće mjere kako bi osigurali da te komponente ne ugrožavaju usklađenost proizvoda s digitalnim elementima s bitnim zahtjevima. To se može postići samo utvrđivanjem zahtjeva koje komponente proizvoda s digitalnim elementima moraju ispunjavati kako bi on ostvario svoje ciljeve u području kibernetičke sigurnosti i provjerom, na temelju rizika, jesu li te komponente u skladu s potrebama proizvoda, kako je navedeno i u uvodnoj izjavi 34.

171. Proizvođač mora na temelju procjene kibernetičkosigurnosnih rizika utvrditi zahtjeve koje bi integrirana komponenta trebala ispunjavati. Na primjer, ako se proizvod s digitalnim elementima oslanja na kriptografske funkcije, mehanizme ažuriranja ili sigurnu komunikaciju koje pruža komponenta, proizvođač mora u okviru postupanja s dužnom pažnjom utvrditi te potrebe i provjeriti zadovoljava li komponenta te potrebe. Dokaz u tu svrhu može biti dokumentacija dobivena od proizvođača komponente, kao što su tehničke specifikacije, sigurnosna dokumentacija ili relevantna dokumentacija o sukladnosti ili jamstvu. Proizvođač prema potrebi može provesti i ispitivanja kako bi provjerio obavljaju li te komponente odgovarajuće funkcije. Iako je dužna pažnja zasebna pravna obveza, ona omogućuje i olakšava proizvođaču da dokaže usklađenost s bitnim zahtjevima za proizvod s digitalnim elementima u cjelini.

172. Pri procjeni rizika za proizvod s digitalnim elementima u cjelini, elementi izvan proizvoda, kao što su elementi iz okruženja, vanjska infrastruktura, drugi sustavi ili mreže, moraju se uzeti u obzir u procjeni kibernetičkosigurnosnih rizika i prema potrebi obuhvatiti mjerama na razini proizvoda kako bi se osigurala usklađenost proizvoda s digitalnim elementima s bitnim zahtjevima. Komponente koje su fizički ili logički integrirane u proizvod s digitalnim elementima, ali potječu od trećih strana, također se moraju smatrati dijelom procjene rizika. Međutim, za potrebe usklađenosti proizvođač bi s tim komponentama trebao postupati kao s komponentama koje isporučuju vanjski dobavljači čija se svojstva provjeravaju u okviru dužne pažnje pri integraciji jer ih proizvođač možda nije ponovno projektirao ili razvio.

173. Ista se logika primjenjuje tijekom razvoja i integracije komponenti. Ako proizvođač sam razvija funkcionalnosti, mora izravno ispuniti bitne zahtjeve. Ako proizvođač integrira komponente koje su razvili drugi, mora dužnom pažnjom osigurati da se te komponente mogu upotrebljavati na način koji omogućuje usklađenost proizvoda s digitalnim elementima u cjelini. U oba slučaja cilj ostaje isti: da proizvod s digitalnim elementima kako je stavljen na tržište postiže odgovarajuću razinu kibernetičke sigurnosti u skladu s Aktom o kibernetičkoj otpornosti, uzimajući u obzir rizike utvrđene u procjeni kibernetičkosigurnosnih rizika.

7.4. **Ponovna upotreba procjena rizika i dokumentacije o sukladnosti za skupine proizvoda s digitalnim elementima**

174. Proizvođači mogu na tržište staviti proizvode s digitalnim elementima koji su slični, na primjer različite inačice, modele ili konfiguracije iste skupine proizvoda. Ako ti proizvodi s digitalnim elementima imaju istu arhitekturu, značajke relevantne za sigurnost i namjenu te su izloženi istim kibernetičkosigurnosnim rizicima, Aktom o kibernetičkoj otpornosti od proizvođača se ne zahtijeva da svaku inačicu smatraju potpuno zasebnim proizvodom s digitalnim elementima za potrebe procjene rizika i ocjenjivanja sukladnosti.

175. U tim slučajevima, pod uvjetom da su sve predmetne inačice obuhvaćene na odgovarajući način u smislu relevantnih rizika i bitnih zahtjeva, proizvođačima mogu biti dovoljni: (i) jedna procjena kibernetičkosigurnosnih rizika provedena u skladu s člankom 13. stavkom 2. Akta o kibernetičkoj otpornosti; (ii) jedna tehnička dokumentacija; i (iii) jedan postupak ocjenjivanja sukladnosti. To omogućuje i izdavanje jedne EU izjave o sukladnosti za skupinu proizvoda s digitalnim elementima, pod uvjetom da se jasno utvrde inačice proizvoda na koje se ona odnosi.

176. Odlučujući je čimbenik to jesu li razlike među inačicama relevantne za kibernetičku sigurnost. Za razlike koje ne utječu na kibernetičkosigurnosna svojstva proizvoda s digitalnim elementima, kao što su razlike u boji, obliku, veličini memorije ili drugim značajkama koje nisu relevantne za sigurnost, nisu potrebne zasebne procjene rizika ili ocjenjivanja sukladnosti. S druge strane, u nekim se slučajevima inačice mogu razlikovati na načine koji utječu na primjenu bitnih zahtjeva, na primjer zbog različitih komunikacijskih sučelja, softverskih stogova, mehanizama ažuriranja ili daljinske povezivosti. U tim se slučajevima te razlike moraju uzeti u obzir u procjeni rizika i, prema potrebi, u ocjenjivanju sukladnosti i tehničkoj dokumentaciji.

177. Proizvođači su i dalje odgovorni za to da procjena rizika i povezana dokumentacija točno odgovaraju proizvodima s digitalnim elementima stavljenima na tržište. Ako nova inačica dovodi do novih kibernetičkosigurnosnih rizika ili mijenja način primjene bitnih zahtjeva, postojeća procjena rizika i dokumentacija o sukladnosti moraju se na odgovarajući način ažurirati. Oslanjanje na jedno ocjenjivanje sukladnosti moguće je samo ako se proizvodi s digitalnim elementima ne razlikuju po kibernetičkosigurnosnim svojstvima.

8. **DALJINSKA OBRADA PODATAKA**

178. U članku 3. točki 1. Akta o kibernetičkoj otpornosti proizvod s digitalnim elementima definiran je kao „softverski ili hardverski proizvod i njegova rješenja za daljinsku obradu podataka, uključujući softverske ili hardverske komponente koje se zasebno stavljaju na tržište”. S obzirom na to, proizvođač mora promatrati proizvod s digitalnim elementima u cjelini, uključujući njegova rješenja za daljinsku obradu podataka (RDPS). Na primjer, pri dokazivanju da proizvod s digitalnim elementima ispunjava bitne zahtjeve utvrđene u Prilogu I., RDPS se mora uzeti u obzir počevši od procjene rizika (članak 13. stavak 2.). Isto vrijedi i za obveze tijekom životnog ciklusa, kao što je izvješćivanje o iskorištenim ranjivostima i značajnim incidentima (članak 14.).

179. Svrha je ovih smjernica dodatno olakšati proizvođačima da utvrde ima li njihov proizvod s digitalnim elementima RDPS kako je definiran u Aktu o kibernetičkoj otpornosti i da ispune svoje obveze usklađenosti u tom pogledu. Nakon početne analize definicija i uvodnih izjava iz Akta o kibernetičkoj otpornosti u ovim će se smjernicama navesti pitanja koja si proizvođači mogu postaviti kako bi utvrdili sadržava li njihov proizvod s digitalnim elementima RDPS (vidjeti odjeljak *8.1.* – Što se smatra rješenjem za daljinsku obradu podataka za proizvod s digitalnim elementima?). Zatim će se razraditi tehničke implikacije RDPS-a i način ocjene usklađenosti s Aktom o kibernetičkoj otpornosti (vidjeti odjeljak *8.2.* – Praktične i tehničke implikacije rješenja za daljinsku obradu podataka i oslanjanje na rješenja trećih strana).

180. U članku 3. točki 2. pojam „daljinska obrada podataka” definira se kao „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”. RDPS je stoga definiran kao softverski elementi („dio elektroničkog informacijskog sustava koji se sastoji od računalnog koda”, kako je definiran u članku 3. točki 4.) obrade podataka na daljinu. Nije predviđeno da se u opseg proizvoda s digitalnim elementima uključi hardver koji se može koristiti pri daljinskoj obradi podataka.

181. U uvodnim izjavama 11. i 12. navedena su dodatna objašnjenja toga kako bi taj pojam trebalo tumačiti. U uvodnoj izjavi 11. pojašnjava se da je cilj obuhvaćanja rješenja za daljinsku obradu podataka to 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”. Navedeno je i da „[z]ahtjevi 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”.

182. Stoga iz uvodne izjave 11. proizlazi da namjera nije da zahtjevi iz Akta o kibernetičkoj otpornosti obuhvaćaju cjelokupnu informatičku infrastrukturu organizacije, nego samo softverske komponente koje omogućuju izvršenje rješenja za obradu podataka. Na primjer, unutarnji sustavi povezani s ljudskim resursima proizvođača, obračunima plaća, upravljanjem odnosima s klijentima, kontinuiranom integracijom / kontinuiranom isporukom te distribucijom sigurnosnih ažuriranja na rubnim lokacijama ne bi se trebali smatrati RDPS-om. Isto tako, sustavi povezani s aktivnostima revizije i ispitivanja, kao što su penetracijsko testiranje, traženje prijetnji i simulacija napada, nisu obuhvaćeni opsegom proizvoda s digitalnim elementima u smislu Akta o kibernetičkoj otpornosti. Važno je napomenuti da, iako je primjena djelotvornih i redovitih ispitivanja i preispitivanja sigurnosti proizvoda s digitalnim elementima bitan zahtjev utvrđen u dijelu II. točki 3. Priloga I. Aktu o kibernetičkoj otpornosti, to ne znači da se takve aktivnosti trebaju smatrati RDPS-om za proizvod s digitalnim elementima.

183. Uvodna izjava 12. primarno se bavi uslugama računalstva u oblaku i u njoj se navode okolnosti u kojima bi se usluge računalstva u oblaku mogle smatrati RDPS-om. U toj uvodnoj izjavi podsjeća se na to da su usluge računalstva u oblaku i modeli usluga u oblaku obuhvaćeni područjem primjene Direktive (EU) 2022/2555 (NIS 2) ([28]), kojom se utvrđuju zahtjevi za upravljanje kibernetičkim sigurnosnim rizicima za pružatelje usluga računalstva u oblaku. Ti su zahtjevi podrobnije utvrđeni u Provedbenoj uredbi Komisije (EU) 2024/2690 ([29]).

8.1. **Što se smatra rješenjem za daljinsku obradu podataka za proizvod s digitalnim elementima?**

184. Definicija daljinske obrade podataka utvrđena u članku 3. točki 2. temelji se na tri elementa: (i) obrađuju li se podaci „na daljinu”; (ii) bi li nepostojanje takve obrade podataka onemogućilo proizvodu s digitalnim elementima obavljanje neke od njegovih funkcija; i (iii) je li softver projektirao i razvio proizvođač ili je to učinjeno pod njegovom odgovornošću. U sljedeća tri pododjeljka detaljnije se obrađuje svaki od tih elemenata.

([28]) 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., ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27.

([29]) Provedbena uredba Komisije (EU) 2024/2690 od 17. listopada 2024. o utvrđivanju pravila za primjenu Direktive (EU) 2022/2555 u pogledu tehničkih i metodoloških zahtjeva za mjere upravljanja kibernetičkosigurnosnim rizicima te dodatnih specifikacija slučajeva u kojima se incident smatra značajnim za pružatelje usluga DNS-a, registre naziva vršnih domena, pružatelje usluga računalstva u oblaku, pružatelje usluga podatkovnog centra, pružatelje mreža za isporuku sadržaja, pružatelje upravljanih usluga, pružatelje upravljanih sigurnosnih usluga, pružatelje internetskih tržišta, internetskih tražilica i platformi za usluge društvenih mreža te pružatelje usluga povjerenja, SL L, 2024/2690, 18.10.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj.

8.1.1. *Pojam „na daljinu”*

185. Pojam „na daljinu” iz članka 3. točke 2. relevantan je, ali nije dovoljan za utvrđivanje sadržava li proizvod s digitalnim elementima RDPS. Nadalje, s obzirom na raznolikost rješenja koja bi mogla biti obuhvaćena tim pojmom, nije moguće dati iscrpnu definiciju pojma „na daljinu”. Proizvođač treba provesti procjenu za svaki pojedini slučaj.

186. U uvodnoj izjavi 11. Akta o kibernetičkoj otpornosti razlikuju se podaci koje „proizvođač [obrađuje ili pohranjuje] na daljinu” i podaci koji se obrađuju ili pohranjuju „lokalno na uređaju korisnika”. Daljinska obrada podataka obično se odvija izvan korisničkog okruženja proizvoda s digitalnim elementima ili operativnog okruženja organizacije (u slučaju profesionalnog korisnika). Međutim, to ne sprečava da se obrada odvija i u blizini uređaja („na rubu”). Prijenos podataka može biti žični (npr. Ethernet kabel) ili bežični (npr. Wi-Fi, Bluetooth). Računalstvo u oblaku, uključujući računalstvo na rubu mreže, tipičan je primjer obrade podataka koja se odvija „na daljinu”. Na primjer, u slučaju funkcije u oblaku kojoj korisnik pristupa iz mobilne aplikacije, dio obrade podataka odvija se u oblaku, izvan okruženja korisnika.

187. Važno je napomenuti da RDPS ne mora nužno raditi na infrastrukturi oblaka trećih strana. RDPS-om se može smatrati i daljinska obrada podataka koja se odvija na lokalnim poslužiteljima u prostorima proizvođača. Drugim riječima, rješenje koje se izvršava u poslovnim prostorima i u privatnom oblaku može se smatrati RDPS-om jednako kao i rješenje koje se izvršava u javnom oblaku i izvan poslovnih prostora.

188. Dva odlučujuća i kumulativna pitanja na temelju kojih se utvrđuje je li obrada podataka obuhvaćena Aktom o kibernetičkoj otpornosti kao rješenje za daljinsku obradu podataka navedena su u nastavku, u odjeljcima *8.1.2.*, i *8.2*. Ako je odgovor na oba pitanja potvrdan, daljinska obrada podataka smatra se RDPS-om.

8.1.2. *Bi li nepostojanje takve obrade podataka onemogućilo proizvodu s digitalnim elementima obavljanje neke od njegovih funkcija?*

189. Kako je utvrđeno u definiciji pojma „daljinska obrada podataka” iz članka 3. točke 2., da bi se obrada podataka na daljinu smatrala RDPS-om, njezino nepostojanje trebalo bi onemogućiti da proizvod s digitalnim elementima obavlja neku od svojih funkcija. Pojam „funkcije” uključen u tu definiciju nije ograničen na „osnovnu funkcionalnost” ili „namjenu” proizvoda s digitalnim elementima jer se Aktom o kibernetičkoj otpornosti ne uvodi takvo ograničenje. Funkcije obuhvaćene područjem primjene Akta o kibernetičkoj otpornosti jesu funkcije koje izravno ispunjavaju namjenu proizvoda s digitalnim elementima iz perspektive korisnika i funkcije koje doprinose ukupnim performansama proizvoda.

190. Primjeri funkcija u kojima se podaci mogu obrađivati na daljinu i koje bi onemogućile da proizvod s digitalnim elementima obavlja neku od svojih funkcija uključuju: (i) slanje naredbi uređaju; (ii) sinkronizaciju datoteka; (iii) uključivanje korisnika; (iv) konfiguraciju (personalizacija proizvoda s digitalnim elementima); (v) automatiziranu distribuciju ažuriranja, uključujući ažuriranje značajki i sigurnosne zakrpe; (vi) upravljanje identitetom i pristupom.

191. U nekim slučajevima korisnik može koristiti funkciju i na daljinu i ručno (npr. uključivanje i isključivanje žarulje preko aplikacije ili ručno). Ta mogućnost ne znači da se obrada podataka povezana s daljinskim obavljanjem funkcije ne može smatrati RDPS-om. Obavljanje te funkcije na daljinu također se smatra dijelom funkcija koje nudi proizvod s digitalnim elementima.

192. S druge strane, ako nepostojanje određene obrade podataka ne onemogućuje da proizvod s digitalnim elementima obavlja neku od svojih funkcija, takva se obrada ne smatra RDPS-om u smislu Akta o kibernetičkoj otpornosti. To uključuje, na primjer, daljinsku analizu telemetrijskih podataka prikupljenih isključivo u statističke svrhe ili za budući razvoj proizvoda.

193. Međutim, čak i ako obrada podataka ne doprinosi obavljanju funkcije proizvoda s digitalnim elementima, proizvođači će u okviru procjene kibernetičkosigurnosnih rizika možda morati razmotriti dovode li te daljinske komponente do rizika za proizvod s digitalnim elementima (npr. s obzirom na operativno okruženje proizvoda) i na odgovarajući način ublažiti te rizike (npr. ublažavanjem na razini proizvoda).

194. Internetske stranice poseban su slučaj koji je potrebno dodatno pojasniti, kako je navedeno i u odjeljku *2.1.* – Stavljanje na tržište. Internetske stranice nisu obuhvaćene opsegom RDPS-a ako ne doprinose obavljanju funkcije proizvoda s digitalnim elementima, kako je objašnjeno u uvodnoj izjavi 11. Akta o kibernetičkoj otpornosti. Sama činjenica da internetske stranice sadržavaju informacije o proizvodu s digitalnim elementima nije dovoljna da bi se one smatrale obuhvaćenima opsegom RDPS-a, čak i ako proizvod preusmjerava korisnika na te internetske stranice. Na primjer, preusmjeravanje korisnika na vanjsku internetsku stranicu s informacijama i uputama za korisnike nije RDPS. S druge strane, internetske stranice mogu biti obuhvaćene opsegom RDPS-a ako omogućuju ili doprinose obavljanju funkcije proizvoda s digitalnim elementima. Na primjer, portal za autentifikaciju koji izdaje vjerodajnice ili tokene potrebne za rad proizvoda s digitalnim elementima smatrao bi se RDPS-om (pod uvjetom da su ispunjeni i drugi kriteriji iz definicije).

8.1.3. *Je li proizvođač projektirao i razvio softver odnosno je li to učinjeno pod njegovom odgovornošću?*

195. U definiciji pojma „daljinska obrada podataka” iz članka 3. točke 2. Akta o kibernetičkoj otpornosti dodatno se navodi da softver za tu obradu podataka na daljinu mora projektirati i razviti proizvođač ili se mora projektirati i razviti pod njegovom odgovornošću. Softver za daljinsku obradu podataka koji je u cijelosti razvio i projektirao proizvođač (interno) nedvojbeno bi se smatrao RDPS-om. To vrijedi i ako se proizvođači oslanjaju na vanjskog pružatelja usluga za razvoj i projektiranje rješenja (tj. „pod njegovom odgovornošću”). Izraz „pod odgovornošću proizvođača” odnosi se na rješenja za daljinsku obradu koja su prilagođena proizvođaču. Riječ je o slučajevima u kojima proizvođač nije samo davatelj licencije za postojeći proizvod s digitalnim elementima ili uslugu koje pružatelj usluga nudi svojim kupcima ili njihove neznatno izmijenjene verzije. „[P]od odgovornošću proizvođača” znači da je softver izradio isključivo proizvođač ili je izrađen u njegovo ime, na temelju projekata i specifikacija koje je on osigurao.

196. Pri utvrđivanju je li riječ o RDPS-u pitanje „tko upravlja rješenjem” nije odlučujuće jer se u definiciji iz Akta o kibernetičkoj otpornosti spominju samo projektiranje i razvoj RDPS-a. To je u skladu s pristupom iz Akta o kibernetičkoj otpornosti prema kojem se zahtjevi i obveze odnose na proizvođače, a ne na rad proizvoda s digitalnim elementima. Ako proizvođači projektiraju i razvijaju rješenja kojima zatim upravlja treća strana, oni su i dalje odgovorni za ispunjavanje bitnih zahtjeva iz Akta o kibernetičkoj otpornosti za proizvod s digitalnim elementima koji stavljaju na tržište.

197. Treba razlikovati slučajeve u kojima projektiranje i razvoj provode proizvođači (ili se oni provode pod njihovom odgovornošću) od slučajeva u kojima se oslanjaju na rješenja trećih strana koja proizvođači nisu projektirali i razvili (ili to nije učinjeno pod njihovom odgovornošću). Na primjer, korisno je promotriti najčešće modele usluga u oblaku koji predviđaju različite stupnjeve kontrole korisnika i koji su navedeni i u uvodnoj izjavi 12. Akta o kibernetičkoj otpornosti, a to su softver kao usluga (SaaS), platforma kao usluga (PaaS) i infrastruktura kao usluga (IaaS).

198. Kad je riječ o rješenju treće strane za IaaS, proizvođač ne kontrolira niti upravlja osnovnim fizičkim i virtualnim resursima (kao što su osnovni hardver i hipervizor pružatelja usluga računalstva u oblaku), ali može uvesti i izvršavati proizvoljan softver pomoću takvih resursa, kao što su operativni sustavi i aplikacije. Takav je softver projektirao i razvio proizvođač ili je on projektiran i razvijen pod njegovom odgovornošću te se stoga može smatrati RDPS-om (ako ispunjava druge kriterije iz definicije).

199. Kad je riječ o rješenju treće strane za PaaS, proizvođač uvodi vlastitu aplikaciju (koju je sam razvio ili nabavio) koristeći programske jezike i okruženja za izvršavanje koje osigurava pružatelj usluga računalstva u oblaku te integrira aplikaciju u svoj proizvod s digitalnim elementima. Proizvođač ima kontrolu nad aplikacijom i eventualno nad konfiguracijskim postavkama za okruženje za izvršavanje. Aplikaciju je stoga projektirao i razvio proizvođač ili je ona projektirana i razvijena pod njegovom odgovornošću te se stoga može smatrati RDPS-om (ako ispunjava druge kriterije iz definicije).

200. Kad je riječ o rješenju treće strane za SaaS, pružatelj SaaS-a nudi proizvođaču potpuno razvijenu aplikaciju za potrebe integracije u proizvođačev proizvod s digitalnim elementima. Proizvođač ima ograničenu mogućnost upravljanja konfiguracijskim postavkama aplikacije specifičnima za korisnika. Aplikaciju stoga nije projektirao i razvio proizvođač odnosno ona nije projektirana i razvijena pod njegovom odgovornošću.

201. Međutim, ako se određeni elementi ne smatraju RDPS-om (npr. hipervizor u slučaju infrastrukture u okviru IaaS-a treće strane, operativni sustav u slučaju rješenja za PaaS treće strane ili aplikacije treće strane u modelu SaaS), ali su integrirani u proizvod s digitalnim elementima na način koji utječe na njegovu sigurnost, ta rješenja trebalo bi smatrati sličnima komponentama treće strane. Proizvođač je dužan utvrditi i procijeniti rizike povezane s integracijom tih elemenata te ih ukloniti primjenom bitnih zahtjeva za sam proizvod s digitalnim elementima. To se, prema potrebi, može postići pomoću sigurnosnih funkcija koje pružatelj usluga računalstva u oblaku stavlja na raspolaganje u okviru svojeg modela zajedničke odgovornosti, pri čemu proizvođač upotrebljava ili konfigurira te funkcije kako bi uklonio utvrđene rizike. Osim toga, očekuje se da će proizvođač ispuniti obvezu sličnu obvezi postupanja s dužnom pažnjom iz članka 13. stavka 5. koja se odnosi na sigurnost tih komponenti, i to na način koji je razmjeran riziku koji rješenje za daljinsku obradu predstavlja za sigurnost proizvoda s digitalnim elementima.

202. Stoga se može zaključiti sljedeće:

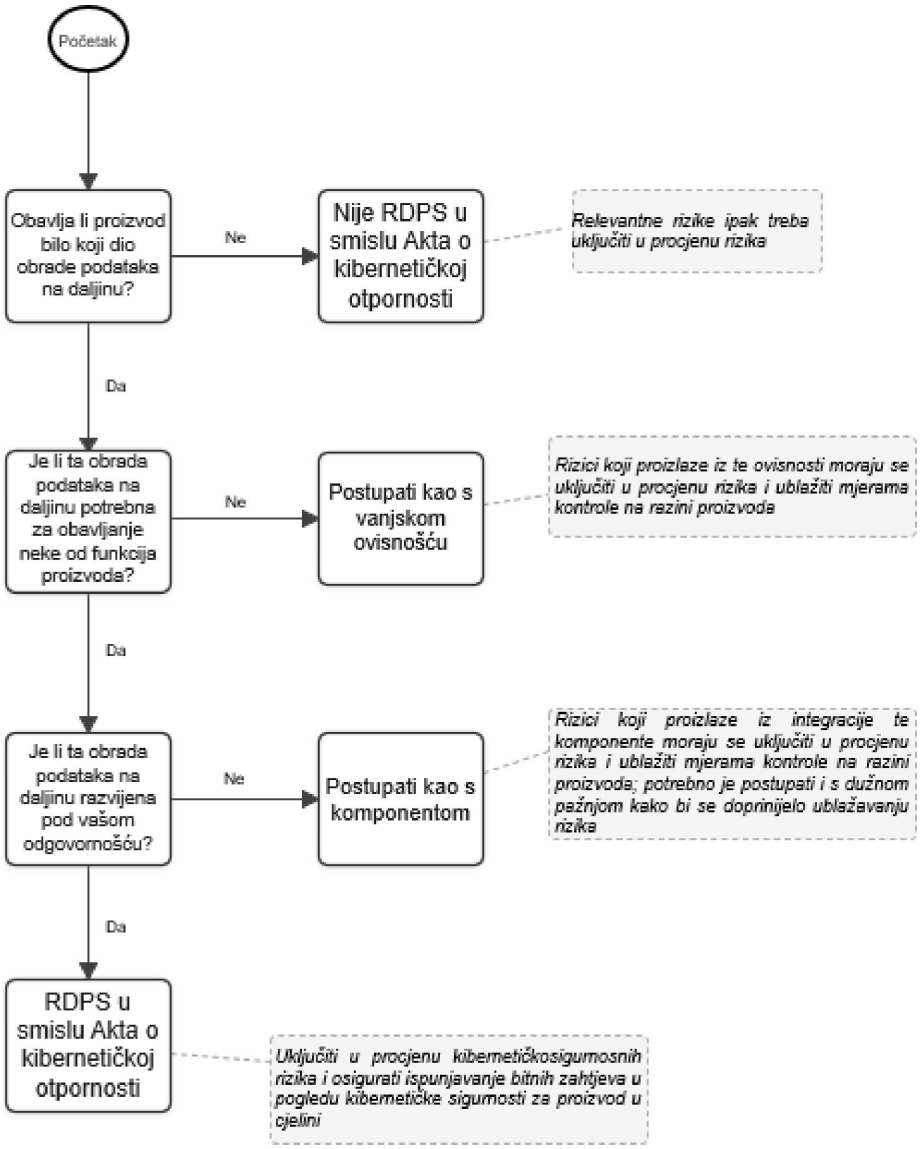
(a) Kako bi se obrada podataka smatrala RDPS-om, odgovor na oba pitanja postavljena u odjeljcima *8.1.2.* – Bi li nepostojanje takve obrade podataka onemogućilo proizvodu s digitalnim elementima obavljanje neke od njegovih funkcija? i *8.1.3.* – Je li proizvođač projektirao i razvio softver odnosno je li to učinjeno pod njegovom odgovornošću? mora biti potvrdan.

(b) Ako je odgovor na pitanje u odjeljku *8.1.2.* – Bi li nepostojanje takve obrade podataka onemogućilo proizvodu s digitalnim elementima obavljanje neke od njegovih funkcija? niječan, proizvođači bi u okviru procjene rizika trebali procijeniti rizike koji proizlaze iz postojanja takve obrade podataka.

(c) Ako je odgovor na pitanje u odjeljku *8.1.2.* – Bi li nepostojanje takve obrade podataka onemogućilo proizvodu s digitalnim elementima obavljanje neke od njegovih funkcija? potvrdan, ali je odgovor na pitanje u odjeljku *8.1.3.* – Je li proizvođač projektirao i razvio softver odnosno je li to učinjeno pod njegovom odgovornošću? niječan, proizvođači bi s rješenjem treće strane trebali postupati kao s komponentom. U okviru procjene rizika proizvođači bi trebali procijeniti rizike koji proizlaze iz integracije takvog rješenja i na odgovarajući ih način ublažiti. Osim toga, proizvođači bi trebali postupati s dužnom pažnjom.

Slika 9:

Stilizirani dijagram toka koji prikazuje postupak utvrđivanja sadržava li proizvod s digitalnim elementima RDPS



8.2. Praktične i tehničke implikacije rješenja za daljinsku obradu podataka i oslanjanje na rješenja trećih strana

203. U Aktu o kibernetičkoj otpornosti primjenjuje se pristup koji se temelji na riziku, utvrđen u članku 13. stavcima 2. i 3. te u prvom bitnom zahtjevu iz dijela I. Priloga I., prema kojem se „proizvodi s digitalnim elementima projektiraju […], razvijaju i proizvode tako da osiguravaju odgovarajuću razinu kibernetičke sigurnosti na temelju rizika”. Stoga bi pri primjeni zahtjeva iz Akta o kibernetičkoj otpornosti na RDPS i postupanje s rizicima koji proizlaze iz usluga trećih strana integriranih u proizvod s digitalnim elementima trebalo razmotriti pristup koji se temelji na riziku.

204. Prvo, proizvođači bi trebali (i) u tehničkoj dokumentaciji navesti da njihov proizvod s digitalnim elementima sadržava RDPS ili se oslanja na rješenja na daljinu trećih strana te (ii) opisati ta rješenja. Ako isti RDPS doprinosi radu više proizvoda s digitalnim elementima, RDPS se mora navesti u tehničkoj dokumentaciji svakog proizvoda. Dokumentacija o RDPS-u koji opslužuje više proizvoda s digitalnim elementima može se ponovno upotrijebiti pri ocjeni sukladnosti drugih proizvoda.

205. Kao što je navedeno u uvodnoj izjavi 11., RDPS-i koji su dio proizvoda s digitalnim elementima i stoga su obuhvaćeni ocjenjivanjem sukladnosti tog proizvoda trebali bi biti ograničeni na softverske module koji su odgovorni za funkcionalnost proizvoda s digitalnim elementima i na sučelja koja ti moduli koriste za povezivanje s vanjskim uslugama. Dodatni pozadinski sustavi koji provode daljnju obradu i s kojima proizvod s digitalnim elementima nije u izravnoj interakciji ne smatraju se RDPS-om.

206. Međutim, ti pozadinski sustavi i dalje predstavljaju vanjske ovisnosti koje se moraju procijeniti u okviru procjene kibernetičkosigurnosnih rizika te koje je potrebno ublažiti mjerama na razini proizvoda. U procjeni rizika koju provodi proizvođač trebalo bi uzeti u obzir: (i) rizike povezane s RDPS-om; (ii) rizike povezane s oslanjanjem na rješenja na daljinu trećih strana (slično komponentama trećih strana); i (iii) rizike povezane s okruženjem proizvoda (npr. osnovni hardver). Proizvođači bi trebali u sam proizvod s digitalnim elementima uključiti sigurnosne kontrole kako bi ublažili te rizike.

207. Nadalje, proizvođač u okviru ocjenjivanja sukladnosti i/ili ispunjavanja obveza dužne pažnje povezanih s uslugama na daljinu trećih strana može ponovno upotrijebiti dokazne materijale s netaksativnog popisa navedenog u nastavku:

(a) dokaz o ispunjavanju obveza na temelju Provedbene uredbe Komisije (EU) 2024/2690;

(b) dokaz o ispunjavanju obveza na temelju Uredbe (EU) 2022/2554 (DORA);

(c) izjava o sukladnosti ili certifikat dobiven u okviru europskog programa kibernetičkosigurnosne certifikacije (donesen na temelju Uredbe (EU) 2019/881 – Akt o kibernetičkoj sigurnosti);

(d) dokaz o sukladnosti s normom ISO/IEC 27017:2015 ili ISO/IEC 27001:2022.

208. Naposljetku, u svojim interakcijama s trećim stranama pružateljima usluga na daljinu proizvođači moraju provesti najprikladnije sigurnosne mjere na temelju procjene rizika (i, prema potrebi, pomoću modela zajedničke odgovornosti pružatelja usluga). Te mjere ublažavanja trebale bi uključivati sigurnosne kontrole za njihove proizvode s digitalnim elementima i provjeru sigurnosnih mjera koje same provode treće strane pružatelji usluga (dužna pažnja). Način za ublažavanje tih rizika može biti uključivanje sigurnosnih jamstava u njihove sporazume o razini usluga s trećim stranama pružateljima usluga, uključujući jamstva da pružatelji usluga na odgovarajući način postupaju s ranjivostima. Velika promjena u rješenjima koja osiguravaju treće strane pružatelji usluga na daljinu ne bi se trebala smatrati bitnom izmjenom proizvoda s digitalnim elementima jer za te elemente nije odgovoran proizvođač. Međutim, u okviru svojih obveza dužne pažnje i kako bi se pravilno ublažili rizici koji proizlaze iz suradnje s trećim stranama pružatelja usluga, proizvođače se potiče da osiguraju da ih njihove treće strane pružatelji usluga računalstva u oblaku na odgovarajući način obavješćuju o promjenama koje uvode u svojim rješenjima. Na temelju tih informacija proizvođači će možda morati revidirati svoju procjenu rizika. U ažuriranoj procjeni rizika trebalo bi uzeti u obzir pružaju li treće strane pružatelji usluga i dalje dostatna jamstva u pogledu kibernetičke sigurnosti te jesu li sigurnosne kontrole na razini proizvoda i dalje primjerene. U nekim će slučajevima proizvođači možda morati izmijeniti te kontrole ili promijeniti treće strane pružatelje usluga.

8.3. **Primjeri upotrebe rješenja za daljinsku obradu podataka**

Kako bi se proizvođačima pružile dodatne praktične smjernice, u ovom se odjeljku navodi niz fiktivnih primjera upotrebe u kojima se opisuju tipični proizvodi s digitalnim elementima koji se oslanjaju na daljinsku obradu podataka i objašnjava može li se takva obrada smatrati rješenjem za daljinsku obradu podataka u smislu Akta o kibernetičkoj otpornosti.

8.3.1. *Aplikacija za mobilno bankarstvo*

Financijski subjekt stavlja aplikaciju za mobilno bankarstvo na tržište. Pozadinski sustavi aplikacije podržavaju, među ostalim, autentifikaciju, autorizaciju, upravljanje računima i plaćanja. Financijski subjekt primjenjuje hibridnu strategiju koja se oslanja na internu infrastrukturu i rješenja na daljinu trećih strana kako bi omogućio rad funkcionalnosti aplikacije. To su među ostalim:

Infrastruktura s vlastitim hostingom koju je razvio financijski subjekt:

— Klijent otvara aplikaciju za mobilno bankarstvo i autentificira se na sučelju za bankarstvo, rješenju s vlastitim hostingom koje je razvio financijski subjekt, koje prima zahtjeve aplikacije i vraća odgovarajuće odgovore. Preko sučelja za bankarstvo provjerava se identitet klijenta pretraživanjem sustava za upravljanje računima i odobrava pristup aplikaciji.

— Klijent preko aplikacije inicira prijenos. Aplikacija prosljeđuje nalog sučelju za bankarstvo, koje zatim upućuje odgovarajući zahtjev sustavu za evidenciju transakcija.

— Transakcija se bilježi u sustavu za upravljanje računima i sustavu za evidenciju transakcija, koji oba imaju vlastiti hosting, ali su logički odvojeni od sučelja za bankarstvo.

— Sustav za evidenciju transakcija vraća status transakcije sučelju za bankarstvo, koje klijentu prikazuje rezultat.

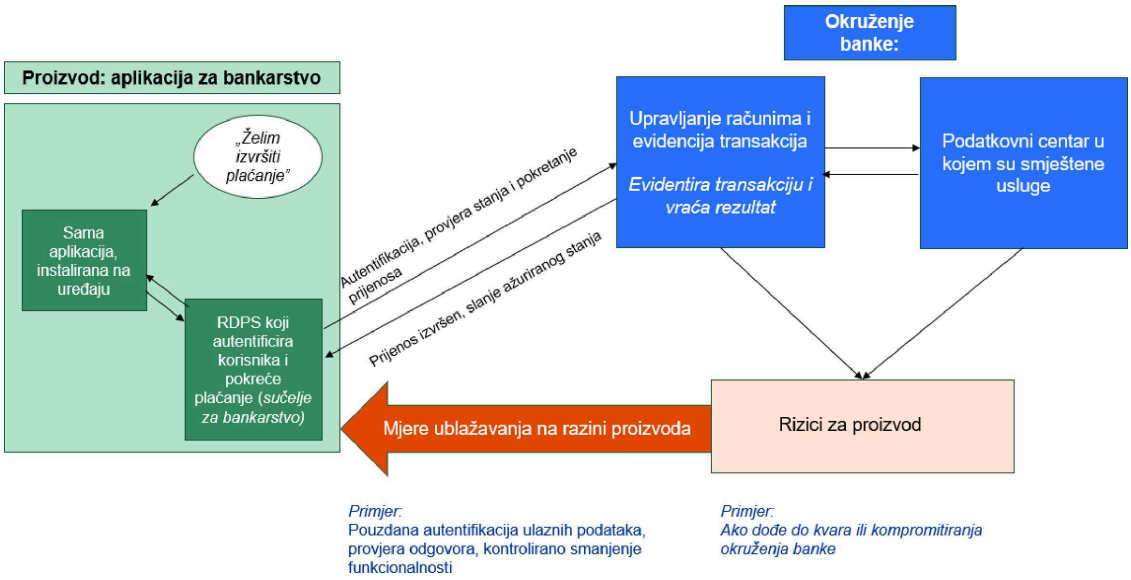
Što to znači za RDPS:

— Sučelje za bankarstvo nužno je kako bi aplikacija mogla obavljati svoje funkcije, odnosno autentifikaciju klijenta, dostavljanje klijentovih naloga, uključujući naloge za plaćanje i prijenos, te vraćanje nastalog statusa. Sučelje za bankarstvo projektirano je i razvijeno pod odgovornošću proizvođača. Budući da je odgovor na oba pitanja iznesena u prethodnim odjeljcima potvrdan, sučelje za bankarstvo treba smatrati RDPS-om. Stoga se ono mora uključiti u procjenu kibernetičkosigurnosnih rizika i primjenu bitnih zahtjeva za proizvod s digitalnim elementima u cjelini. Kasnija obrada naloga nakon što je podnesen, konkretno evidentiranje transakcije u sustavu za upravljanje računima i sustavu za evidenciju transakcija, namira i poravnanje, provodi se u okviru sustava s kojima aplikacija nije u izravnoj interakciji i stoga nije riječ o RDPS-u.

— Sustav za upravljanje računima i sustav za evidenciju transakcija ne smatraju se RDPS-om za aplikaciju za bankarstvo. Aplikacija s njima nije u izravnoj interakciji (interakcija se odvija sa sučeljem za bankarstvo, koje se na njih oslanja). Iako njihova dostupnost može biti potrebna za obavljanje određene funkcije, Akt o kibernetičkoj otpornosti obuhvaća samo one dijelove sustava koji su u izravnoj interakciji s proizvodom s digitalnim elementima. Stoga nisu obuhvaćeni definicijom RDPS-a za potrebe tog akta. Međutim, ti sustavi i dalje predstavljaju vanjske ovisnosti koje proizvod s digitalnim elementima mogu izložiti znatnim kibernetičkosigurnosnim rizicima. Na primjer, kompromitiranje sustava za evidenciju transakcija moglo bi napadaču omogućiti da utječe na rezultate transakcije koji se kasnije prikazuju u aplikaciji. Proizvođač je stoga dužan utvrditi i procijeniti te rizike u okviru procjene kibernetičkosigurnosnih rizika te ih ublažiti mjerama na razini proizvoda, kao što su pouzdana autentifikacija pozadinskih sučelja, zaštita cjelovitosti podataka o transakcijama, sigurni komunikacijski kanali i provjera odgovora koje aplikacija prima.

Slika 10:

Stilizirani prikaz aplikacije za bankarstvo koja se oslanja na RDPS



SaaS treće strane za korisničku podršku:

— Financijski subjekt u svoju aplikaciju integrira rješenje za korisničku podršku u obliku razgovora koje je razvila i kojim upravlja treća strana pružatelj usluga; treća strana pružatelj usluga napisala je kôd poslužitelja za razgovor, izradila korisničko sučelje i upravlja infrastrukturom na kojoj se razgovor izvršava (tj. model SaaS).

— Kad klijent zatraži podršku, aplikacija ga povezuje s uslugom treće strane kako bi se mogla pokrenuti sesija razgovora i odviti razmjena poruka, pri čemu se trećoj strani ne omogućuje pristup osnovnim sustavima za bankarstvo.

Što to znači za RDPS:

— Rješenje za korisničku podršku u obliku razgovora potrebno je kako bi proizvod s digitalnim elementima obavljao jednu od svojih funkcija, ali ga financijski subjekt nije projektirao ni razvio niti je to učinjeno pod njegovom odgovornošću; stoga nije riječ o RDPS-u. Međutim, s njim bi trebalo postupati kao s komponentom treće strane. Oslanjanje na tu uslugu treće strane može dovesti do kibernetičkosigurnosnih rizika za aplikaciju za bankarstvo, na primjer ako bi napadač upotrijebio kanal za razgovor kako bi se lažno predstavljao kao banka ili isporučio zlonamjerni sadržaj korisnicima. Financijski subjekt mora te rizike uzeti u obzir u svojoj procjeni kibernetičkosigurnosnih rizika i ublažiti ih mjerama na razini proizvoda, kao što su izolacija funkcije razgovora od temeljnih značajki bankarstva, kontrola protoka podataka i validacija sadržaja. Osim toga, u pogledu SaaS-a trebalo bi postupati s dužnom pažnjom.

8.3.2. *Pametni termostat*

Pametni termostat omogućuje korisnicima da pomoću mobilne aplikacije kontroliraju temperaturu u svojem domu. Mobilna aplikacija i pametni termostat oslanjaju se na daljinsku obradu podataka za potrebe razmjene podataka (npr. zahtjev za povećanje temperature) i pohrane podataka (npr. preferencije korisnika). Te su funkcije razvijene i projektirane pod odgovornošću proizvođača, ali rade na osnovnoj fizičkoj i virtualnoj infrastrukturi koju osigurava treća strana (IaaS treće strane).

Pametni termostat bez te daljinske obrade podataka ne bi mogao obavljati svoje pametne funkcionalnosti, što znači da bi njezino nepostojanje proizvodu s digitalnim elementima onemogućilo da obavlja jednu ili više svojih funkcija. Osim toga, softver je razvijen i projektiran pod odgovornošću proizvođača pametnog termostata. Stoga se daljinska obrada podataka smatra RDPS-om kako je definiran u Aktu o kibernetičkoj otpornosti.

Za potrebe usklađenosti s Aktom o kibernetičkoj otpornosti proizvođač pametnog termostata u tehničkoj dokumentaciji proizvoda s digitalnim elementima treba navesti da proizvod sadržava RDPS te da se oslanja na IaaS treće strane, uključujući pojedinosti o ugovorenoj usluzi. Proizvođač te elemente treba uzeti u obzir u procjeni rizika, koja obuhvaća namjenu i razumno predvidljivu upotrebu proizvoda s digitalnim elementima. Proizvođač primjenjuje bitne zahtjeve iz Akta o kibernetičkoj sigurnosti na temelju rizika koji proizlaze iz RDPS-a. Kad je riječ o IaaS-u treće strane, proizvođač mora osigurati da su sigurnosne mjere koje provodi treća strana pružatelj usluga primjerene i/ili poduzeti odgovarajuće mjere u pogledu infrastrukture. Na primjer, u prvom bi slučaju proizvođač mogao zatražiti dokaz da su ispunjene obveze iz Direktive NIS 2.

8.3.3. *e-čitač*

Proizvođač softvera za e-čitač koristi uslugu pohrane treće strane u modelu SaaS kako bi pohranio elektroničke knjige koje su kupili korisnici i omogućio im pristup njihovim knjigama. Bez te usluge pohrane proizvod s digitalnim elementima ne bi mogao obavljati jednu od svojih funkcija, ali uslugu pohrane treće strane u modelu SaaS nije razvio proizvođač niti je ona razvijena pod njegovom odgovornošću; pružatelj SaaS-a stavlja ga na raspolaganje korisnicima za svaki slučaj upotrebe.

Usluga pohrane u modelu SaaS ne odgovara definiciji RDPS-a. Međutim, proizvođač e-čitača oslanja se na tu vanjsku uslugu za funkcioniranje svojeg proizvoda s digitalnim elementima te stoga u svojoj procjeni kibernetičko-sigurnosnih rizika mora uzeti u obzir povezane rizike. Proizvođač e-čitača trebao bi sa SaaS-om postupati kao s komponentom. Proizvođač mora provesti odgovarajuće sigurnosne mjere na razini proizvoda, kao što su sigurna autentifikacija, šifriranje i zaštita cjelovitosti komunikacije s uslugom pohrane. Dužna pažnja pri odabiru i integraciji pružatelja SaaS-a doprinijet će i ispunjavanju obveza proizvođača kako bi proizvod s digitalnim elementima u cjelini mogao ispunjavati bitne zahtjeve.

8.3.4. *Industrijski robot*

Industrijski robot ima zadaću preuzimati dijelove. Robot šalje informacije prikupljene kamerama usluzi na daljinu koju je projektirao i razvio proizvođač. Ta usluga radi na osnovnoj fizičkoj i virtualnoj infrastrukturi koju osigurava treća strana pružatelj usluga (IaaS treće strane). Usluga računalstva u oblaku izračunava položaj dijela na temelju snimki s kamera i robotu šalje naredbe za preuzimanje dijelova.

Bez te obrade podataka industrijski robot ne bi mogao preuzeti dijelove, a stoga ni obavljati jednu od svojih funkcija. Nadalje, proizvođač je projektirao i razvio softver koji se izvršava u okviru infrastrukture. Softver koji je projektirao i razvio proizvođač odgovara definiciji RDPS-a.

Proizvođač industrijskog robota u tehničkoj dokumentaciji proizvoda s digitalnim elementima treba navesti da proizvod sadržava RDPS te da se oslanja na IaaS treće strane (uključujući pojedinosti o ugovorenoj usluzi). Proizvođač te elemente treba uzeti u obzir i u procjeni rizika, koja obuhvaća namjenu i razumno predvidljivu upotrebu proizvoda s digitalnim elementima. Proizvođač na temelju rizika primjenjuje bitne zahtjeve iz Akta o kibernetičkoj otpornosti za proizvod s digitalnim elementima, uključujući njegov RDPS. Dužna pažnja pri odabiru pružatelja IaaS-a doprinijet će i ispunjavanju obveza proizvođača. Na primjer, proizvođač bi mogao zatražiti dokaz da su ispunjene obveze iz Direktive NIS 2.

8.3.5. *Mobilna radiotelefonska mreža*

Pametni telefon oslanja se na 5G mrežu kako bi korisnicima omogućio internetsku vezu, telefonske pozive i poruke (mobilna povezivost). Mobilnu radiotelefonsku mrežu razvijaju i projektiraju telekomunikacijski operateri. Mreža obuhvaća male ćelije i odašiljače te drugu mrežnu opremu.

Proizvod s digitalnim elementima trebao bi se moći pravilno povezati s mrežom; to je jedna od njegovih funkcija. Međutim, pitanje je li ta mreža u funkciji nije relevantno za utvrđivanje radi li proizvod s digitalnim elementima pravilno. Mreža je samo komunikacijski kanal i nije potrebna kako bi proizvod s digitalnim elementima mogao obavljati svoju funkciju „pravilnog povezivanja s mrežom”. Isto tako, Ethernet kabel, ruter ili Wi-Fi signal ne smatraju se rješenjima za obradu podataka čije bi nepostojanje onemogućilo da proizvod s digitalnim elementima obavlja neku od svojih funkcija, već služe za ostvarivanje komunikacije/povezivosti.

Stoga mobilna radiotelefonska mreža ne odgovara definiciji RDPS-a. Mrežu ne bi trebalo smatrati komponentom treće strane jer u proizvod s digitalnim elementima nije integriran softver, nego se proizvod samo oslanja na tu mrežu. Stoga proizvođač nema obveze dužne pažnje prema pružatelju mrežnih usluga.

9. **DODATNI ELEMENTI**

9.1. **Obveze u pogledu izvješćivanja**

209. U skladu s člankom 14. stavcima 1. i 3. Akta o kibernetičkoj otpornosti proizvođač je dužan istodobno obavijestiti CSIRT koji je imenovan koordinatorom i ENISA-u o (i) svakoj iskorištenoj ranjivosti njegova proizvoda s digitalnim elementima za koju dozna; i (ii) svakom značajnom incidentu koji utječe na sigurnost proizvoda s digitalnim elementima za koji dozna.

210. U skladu s člankom 69. stavkom 3. i člankom 71. stavkom 2. drugom rečenicom obveza utvrđena u članku 14. primjenjuje se od 11. rujna 2026. na sve proizvode s digitalnim elementima obuhvaćene područjem primjene Akta o kibernetičkoj otpornosti, uključujući proizvode s digitalnim elementima stavljene na tržište prije 11. prosinca 2027. Nadalje, za razliku od obveza postupanja s ranjivostima, koje traju samo tijekom razdoblja potpore za proizvod, obveze u pogledu izvješćivanja i dalje se primjenjuju nakon što se za proizvod s digitalnim elementima više ne pruža potpora. Ako je proizvod s digitalnim elementima stavljen na tržište prije 11. prosinca 2027. ili ako je njegovo razdoblje potpore završilo, proizvođač nije dužan ispuniti obveze postupanja s ranjivostima utvrđene u dijelu II. Priloga I.

211. Valja podsjetiti na to da se obveza obavješćivanja o tim događajima primjenjuje nakon što proizvođač dozna da se ranjivost aktivno iskorištava ili da je došlo do značajnog incidenta zbog kojeg je ugrožena sigurnost njegova proizvoda s digitalnim elementima. Stoga bi smjernice o tome kad se smatra da je proizvođač doznao za njih trebale pomoći proizvođačima da odrede trenutak od kojeg počinju teći primjenjivi rokovi za obavješćivanje.

212. Proizvođači mogu imati usporedive obveze u pogledu izvješćivanja na temelju više akata EU-a. Kako bi se pojam „doznati” dosljedno tumačio i kako bi se proizvođačima olakšalo ispunjavanje tih obveza, ove su smjernice usklađene s uvodnom izjavom 31. Provedbene uredbe Komisije (EU) 2024/2690 i odjeljkom II. točkom A Smjernica 9/2022 o obavješćivanju o povredi osobnih podataka na temelju Opće uredbe o zaštiti podataka.

213. U nekim slučajevima proizvođač može otkriti sumnjiv događaj ili mu treća strana, kao što je pojedinac, kupac, subjekt, tijelo, medijska organizacija ili drugi izvor, može skrenuti pozornost na potencijalni incident ili ranjivost. U tim slučajevima proizvođač bi trebao odmah procijeniti sumnjivi događaj kako bi utvrdio predstavlja li on aktivno iskorištenu ranjivost ili značajan incident koji utječe na sigurnost proizvoda s digitalnim elementima. Stoga se smatra da je proizvođač doznao za njih kad nakon takve početne procjene može biti razumno siguran: (i) da se aktivno iskorištava ranjivost njegova proizvoda s digitalnim elementima; ili (ii) da se dogodio značajan incident zbog kojeg je ugrožena sigurnost njegova proizvoda s digitalnim elementima.

214. Stoga trenutak u kojem se može smatrati da je proizvođač doznao za te situacije ovisi o okolnostima konkretne aktivno iskorištene ranjivosti ili značajnog incidenta. U nekim slučajevima od samog početka može biti relativno jasno da se ranjivost aktivno iskorištava ili da na sigurnost proizvoda s digitalnim elementima utječe značajan incident. U drugima će možda trebati neko vrijeme da se utvrdi utječe li ranjivost na proizvod s digitalnim elementima i iskorištava li tu ranjivost zlonamjerni akter odnosno utječe li na sigurnost proizvoda s digitalnim elementima neki incident. Međutim, u prvom bi planu trebalo biti brzo poduzimanje mjera za provedbu početne procjene kako bi se utvrdilo jesu li ti uvjeti doista ispunjeni, posebno ako ranjivost može predstavljati znatan rizik, te, ako može, poduzimanje korektivnih mjera i obavješćivanje u skladu s Aktom o kibernetičkoj otpornosti.

215. Nadalje, zbog strukture obveza u pogledu izvješćivanja proizvođači moraju postupno ažurirati svoje obavijesti na temelju napretka unutarnjih istraga i detaljnijih saznanja o aktivno iskorištenoj ranjivosti ili incidentu. Konkretno, proizvođači su dužni rano upozorenje s ograničenim informacijama dostaviti bez nepotrebne odgode, a u svakom slučaju u roku od 24 sata nakon što za njih doznaju. Dodatne informacije dužni su dostaviti kasnije, kao dio obavijesti koja se dostavlja bez nepotrebne odgode, a u svakom slučaju u roku od 72 sata nakon što za njih doznaju („obavijest u roku od 72 sata”). Potpuno izvješće mora se dostaviti u roku od 14 dana nakon što bude dostupna korektivna mjera ili mjera ublažavanja za aktivno iskorištene ranjivosti ili u roku od mjesec dana od obavijesti o značajnim incidentima koja je dostavljena u roku od 72 sata.

216. Kako je navedeno i u odjeljku *3.3.1.* – Kontinuirana potpora i osiguravanje održivosti FOSS-a, upravitelji softvera otvorenog koda također su dužni obavijestiti o aktivno iskorištenim ranjivostima u skladu s člankom 24. stavkom 3. ([30]) Ta se obveza primjenjuje nakon što doznaju za aktivno iskorištenu ranjivost, a ne samo zbog postojanja ranjivosti u bazi koda FOSS-a čiji je taj subjekt upravitelj. U praksi, s obzirom na to da se komponente FOSS-a niže u lancu opskrbe obično integriraju u druge proizvode s digitalnim elementima, upravitelj će za aktivno iskorištavanje vjerojatno doznati iz izvješća trećih strana u kojima se navodi iskorištavanje komponenti FOSS-a integriranih u druge proizvode s digitalnim elementima. Do takve situacije može doći, na primjer, ako proizvođač proizvoda s digitalnim elementima otkrije aktivno iskorištavanje u komponenti FOSS-a integriranoj u njegov proizvod i o tome obavijesti upravitelja te komponente; ili ako korisnik ili istraživač u području sigurnosti pronađe dokaze o iskorištavanju u komponenti FOSS-a integriranoj u proizvod s digitalnim elementima i o aktivnom iskorištavanju obavijesti upravitelja komponente.

217. Trebalo bi pojasniti i da, s obzirom na to da obveza obavješćivanja o aktivno iskorištenim ranjivostima nastaje kad proizvođač dozna za aktivno iskorištavanje, proizvođač nije dužan prijaviti ranjivosti za čije je aktivno iskorištavanje već znao prije 11. rujna 2026. (datum na koji se obveza u pogledu izvješćivanja počinje primjenjivati). Stoga Aktom o kibernetičkoj otpornosti nije propisano retroaktivno obavješćivanje o tim ranjivostima. Suprotno tomu, obveza se primjenjuje ako je proizvođač već znao za ranjivosti prije 11. rujna 2026., ali u tom trenutku nije znao za njezino aktivno iskorištavanje (zato što se ono još nije dogodilo ili zato što proizvođač za njega nije znao). Ako nakon 11. rujna 2026. dođe do aktivnog iskorištavanja ili proizvođač dozna za njega, ranjivost se smatra aktivno iskorištenom ranjivošću na koju se primjenjuje obveza u pogledu izvješćivanja.

218. Slično tomu, proizvođač je dužan obavijestiti samo o iskorištenim ranjivostima sadržanima u njegovu proizvodu s digitalnim elementima. Ako proizvod s digitalnim elementima sadržava iskorištenu ranjivost koja proizlazi iz komponente treće strane, proizvođač proizvoda s digitalnim elementima dužan je obavijestiti o toj iskorištenoj ranjivosti. Međutim, ako proizvođač zna da komponenta treće strane sadržava ranjivost, ali se ta ranjivost (i) ne može iskoristiti u njegovu proizvodu s digitalnim elementima (npr. zato što ranjivom kodu nije moguće pristupiti) ili (ii) dosad nije iskorištena u njegovu proizvodu s digitalnim elementima, ta se ranjivost ne smatra aktivno iskorištenom ranjivošću sadržanom u njegovu proizvodu s digitalnim elementima te stoga proizvođač nema obvezu obavješćivanja o njoj. Taj proizvođač i dalje može dobrovoljno izvješćivati o toj ranjivosti u skladu s člankom 15. Akta o kibernetičkoj otpornosti. Mora ispunjavati i zahtjeve u pogledu postupanja s ranjivostima iz dijela II. Priloga I. Aktu o kibernetičkoj otpornosti te obavijestiti o ranjivosti osobu ili subjekt koji proizvodi ili održava predmetnu komponentu, u skladu s člankom 13. stavkom 6. i kako je dodatno objašnjeno u odjeljku *9.2.1.* – Obavješćivanje o ranjivostima više u lancu opskrbe i dijeljenje sigurnosnih popravaka.

([30]) Ako je upravitelj uključen u razvoj proizvoda s digitalnim elementima.

219. Nakon što doznaju za aktivno iskorištenu ranjivost ili značajan incident, proizvođači su također dužni, u skladu s člankom 14. stavkom 8., obavijestiti pogođene korisnike i, prema potrebi, sve korisnike. Ako to ne učine pravodobno, CSIRT-ovi koji su primili obavijest mogu pružiti takve informacije korisnicima kad se to smatra razmjernim i potrebnim za sprečavanje ili ublažavanje učinka te ranjivosti ili incidenta.

220. U skladu s pristupom iz Akta o kibernetičkoj otpornosti koji se temelji na riziku, obveza obavješćivanja korisnika utvrđena u članku 14. stavku 8. treba se primjenjivati razmjerno i na temelju rizika. Konkretno, pružanje informacija o aktivno iskorištenoj ranjivosti ili značajnom incidentu ne podrazumijeva da se te informacije moraju objaviti ili neselektivno otkriti. Prema potrebi i s obzirom na prirodu proizvoda s digitalnim elementima, pogođene korisnike i mogući učinak ranjivosti ili incidenta, proizvođači mogu ograničiti otkrivanje detaljnih informacija na relevantne korisnike ili kupce. To se prije svega odnosi na proizvode s digitalnim elementima koji se upotrebljavaju u osjetljivim ili bitnim okruženjima jer bi u tim slučajevima sama objava tehničkih pojedinosti mogla povećati kibernetičkosigurnosne rizike ili omogućiti daljnje iskorištavanje.

221. Nakon što se ranjivost na odgovarajući način otkloni ili ublaži, može biti primjereno objavljivanje široj javnosti. To bi moglo biti poželjno, na primjer, ako objavljivanje doprinosi informiranju građana ili omogućuje korisnicima da provjere da ranjivost više ne utječe na njihove proizvode s digitalnim elementima. U tim bi slučajevima razina podrobnosti i vrijeme objave široj javnosti trebali biti razmjerni te bi se trebali uzeti u obzir preostali rizici od iskorištavanja, priroda proizvoda s digitalnim elementima i interesi predmetnih korisnika. Nadalje, u dijelu II. točki 4. Priloga I. navodi se da su proizvođači dužni javno objaviti informacije o popravljenim ranjivostima nakon izdavanja sigurnosnog ažuriranja.

9.2. **Postupanje s ranjivostima**

9.2.1. *Obavješćivanje o ranjivostima više u lancu opskrbe i dijeljenje sigurnosnih popravaka*

222. Člankom 13. stavkom 6. Akta o kibernetičkoj otpornosti propisuje se da proizvođači trebaju o ranjivosti integriranih komponenti obavijestiti osobu ili subjekt koji proizvodi ili održava tu komponentu („obavješćivanje aktera više u lancu opskrbe”).

223. Proizvođači su dužni obavješćivati aktere više u lancu opskrbe samo kad je riječ o verziji komponente koju integriraju. Ako su osoba ili subjekt koji proizvodi ili održava komponentu uspostavili sigurnosne politike, postupke koordiniranog otkrivanja ranjivosti ili namjenske kanale za obavješćivanje o ranjivostima, proizvođači bi trebali dostavljati obavijesti u skladu s njima odnosno preko njih, posebno ako bi preuranjeno otkrivanje neispravljenih ranjivosti moglo povećati kibernetičkosigurnosne rizike. Nadalje, kako bi se smanjilo opterećenje za održavatelje više u lancu opskrbe, posebno u vezi s projektima otvorenog koda, proizvođači nisu obvezni obavješćivati aktere više u lancu opskrbe ako mogu potvrditi da osoba ili subjekt koji proizvodi ili održava komponentu znaju da postoji ranjivost. Proizvođače se potiče da poduzmu razumne mjere kako bi izbjegli podnošenje dvostrukih izvješća, na primjer provjerom javno dostupnih baza podataka o ranjivostima, sigurnosnih savjeta za konkretni projekt ili uspostavljenih sustava za praćenje problema prije obavješćivanja aktera više u lancu opskrbe.

224. Proizvođači su dužni obavješćivati aktere više u lancu opskrbe samo o ranjivostima koje postoje u samoj integriranoj komponenti, a ne o ranjivostima koje proizlaze iz integracije komponente i drugog koda koji je razvio proizvođač ili integracije drugih komponenti. Međutim, mogu postojati situacije u kojima integracija komponente u određeni proizvod s digitalnim elementima otkrije određena ponašanja, interakcije ili značajke relevantne za sigurnost te komponente koje same po sebi nisu bile očite ili ih se nije moglo lako utvrditi. U tim se slučajevima proizvođače potiče da te informacije proslijede osobi ili subjektu koji proizvodi ili održava komponentu kako bi se promicala dobra praksa postupanja s ranjivostima čija je svrha olakšati učinkovito otklanjanje ranjivosti i poboljšati opću sigurnost ekosustava komponente.

225. Naposljetku, proizvođači nisu dužni obavijestiti o ranjivosti aktere više u lancu opskrbe ako komponenta više nema održavatelja ili ako se proizvođač više ne oslanja na izvornog održavatelja za nove verzije ili sigurnosne popravke. U tim se slučajevima proizvođača svejedno potiče da obavijesti korisnike o toj komponenti služeći se odgovarajućim alternativnim mjerama, kao što su postojeći mehanizmi zajednice (npr. popisi e-adresa ili sustavi za prijavu problema) ili javne evidencije ranjivosti.

226. Nadalje, na temelju članka 13. stavka 6. proizvođači koji su razvili izmjenu softvera kako bi otklonili ranjivost integrirane komponente moraju podijeliti tu izmjenu softvera („sigurnosni popravak”) s osobom ili subjektom koji proizvodi ili održava tu komponentu („dijeljenje s akterima više u lancu opskrbe”).

227. Ako su proizvođači dužni podijeliti sigurnosni popravak na temelju članka 13. stavka 6., taj bi popravak prema potrebi trebalo dostaviti u strojno čitljivom formatu i, na način koji omogućuje da ga osoba ili subjekt koji proizvodi ili održava komponentu lako provjeri i prema potrebi integrira. Ako je riječ o besplatnoj komponenti otvorenog koda, sigurnosni popravak trebalo bi dijeliti na način koji je kompatibilan s licencijom za tu komponentu, na primjer tako da se dijeli na temelju iste licencije ili licencije koja održavatelju omogućuje distribuciju popravka na temelju vlastite licencije. Ako održavatelj te komponente ima smjernice o tome kako bi se sigurnosni popravci trebali dijeliti, proizvođač bi trebao slijediti te smjernice.

228. Međutim, Aktom o kibernetičkoj otpornosti ne propisuje se da su proizvođači dužni osigurati da osoba ili subjekt koji proizvodi ili održava komponentu nužno prihvati njihove sigurnosne popravke. Isto tako, nisu dužni osigurati da se ti popravci nužno integriraju u repozitorij koda komponente, na primjer ako održavatelj preferira drugu opciju za rješavanje problema. Slično tomu, proizvođači nisu dužni prihvatiti predloženi popravak koji je razvio održavatelj komponente i mogu odlučiti riješiti problem na druge primjerene načine.

229. U nekim je slučajevima osoba ili subjekt koji proizvodi ili održava komponentu možda već dostavio sigurnosni popravak za otklanjanje ranjivosti, ali proizvođač primjenjuje drukčiju strategiju rješavanja problema (na primjer promjenom neke druge konfiguracije). U tim slučajevima u skladu s Aktom o kibernetičkoj otpornosti proizvođač nije dužan podijeliti izmjenu nekog drugog dijela sustava s akterima više u lancu opskrbe. Međutim, proizvođača se potiče da to učini ako to može pomoći osobi ili subjektu koji održava komponentu.

9.2.2. *Poznate iskoristive ranjivosti*

230. Jednim od bitnih zahtjeva iz dijela I. Priloga I. Aktu o kibernetičkoj otpornosti predviđa se da se na temelju procjene kibernetičkosigurnosnih rizika iz članka 13. stavka 2. i ako je primjenjivo, proizvodi s digitalnim elementima moraju staviti na raspolaganje na tržištu bez poznatih iskoristivih ranjivosti.

231. U članku 3. točki 41. „iskoristiva ranjivost” definirana je kao „ranjivost koju bi protivnik mogao djelotvorno iskoristiti u praktičnim operativnim uvjetima”. Ne mogu se sve ranjivosti iskoristiti u praktičnim operativnim uvjetima, a neke se ranjivosti mogu iskoristiti samo u teoretskim uvjetima (npr. u laboratoriju ili u okviru simulacije) i/ili ne u uvjetima koji bi se mogli dogoditi u operativnom okruženju proizvoda s digitalnim elementima.

232. Aktom o kibernetičkoj otpornosti propisuje se da proizvođač mora imati odgovarajuće politike i postupke za obradu i otklanjanje potencijalnih ranjivosti koje je prijavio unutarnji ili vanjski izvor (članak 13. stavak 8.). Međutim, nije izričito navedeno kad bi trebalo smatrati da proizvođač zna za iskoristivu ranjivost, čime se aktivira obveza ispunjavanja tog bitnog zahtjeva u trenutku stavljanja na tržište.

233. Ranjivost bi trebalo smatrati poznatom ako je navedena u relevantnim javno dostupnim bazama podataka o ranjivostima, kao što je europska baza podataka o ranjivostima uspostavljena člankom 12. stavkom 2. Direktive (EU) 2022/2555 ili druge istaknute baze podataka o ranjivostima.

234. Osim toga, ranjivost može biti poznata i ako je proizvođač za nju doznao iz informacija koje nisu javne, na primjer u okviru koordiniranog otkrivanja koje provodi istraživač u području sigurnosti ili vlastitog internog testiranja i analize proizvođača, među ostalim, na primjer, pri korištenju usluga koje se temelje na umjetnoj inteligenciji. Slično tomu, ranjivost može biti poznata ako je o njoj javno i široko izviješteno u pouzdanim medijima, uključujući specijalizirane publikacije o kibernetičkoj sigurnosti ili opće masovne medije.

235. Međutim, sama činjenica da je ranjivost utvrđena ili da je o njoj obaviješteno ne znači sama po sebi da se ona može iskoristiti u praksi ili da se odnosi na konkretni proizvod s digitalnim elementima. Proizvođač mora istražiti i potvrditi istinitost tih informacija i primjenjivost na vlastiti proizvod s digitalnim elementima. Stoga od prve obavijesti o ranjivosti do njezine potvrde može proteći ograničeno razdoblje. Kako je navedeno u odjeljku *9.1.* – Obveze u pogledu izvješćivanja, u prvom planu bi trebalo biti brzo djelovanje radi istrage i reagiranja.

236. Nadalje, obveza proizvođača da ispune bitne zahtjeve utvrđene u dijelu I. Priloga I. primjenjuje se u trenutku stavljanja na tržište, u skladu s člankom 13. stavkom 1. U praksi se nove potencijalno iskoristive ranjivosti mogu otkriti u završnim fazama razvojnog ciklusa proizvoda s digitalnim elementima, među ostalim neposredno prije nego što uđe u distribucijski lanac (odnosno bude stavljen na tržište).

237. Budući da je obveza stavljanja proizvoda s digitalnim elementima na tržište bez poznatih iskoristivih ranjivosti obveza koja se temelji na riziku, na proizvođaču je da utvrdi, na temelju procjene kibernetičkosigurnosnih rizika, može li se proizvod s digitalnim elementima sigurno staviti na tržište u skladu s Aktom o kibernetičkoj otpornosti. Isto tako, proizvođač može utvrditi da je prije nego što se proizvod s digitalnim elementima može staviti na tržište potrebno otkloniti novu ranjivost za koju je doznao. Pri donošenju te odluke proizvođači bi trebali uzeti u obzir ozbiljnost, iskoristivost i mogući učinak ranjivosti te rizike koji nastaju za sam proizvod s digitalnim elementima nakon njegova stavljanja u upotrebu. Mogu uzeti u obzir i rizike od odgode objavljivanja proizvoda dok se ranjivost ne otkloni, na primjer zato što se novim izdanjem otklanjaju i druge iskoristive ranjivosti ili je nužno za kontinuirani rad kritičnih sustava. U svakom slučaju, nakon što se proizvod s digitalnim elementima stavi na tržište, proizvođač i dalje ima obvezu djelotvornog postupanja s ranjivostima u skladu sa zahtjevima u pogledu postupanja s ranjivostima utvrđenima u dijelu II. Priloga I.

9.2.3. *Djelotvorna i redovita ispitivanja i preispitivanja*

238. U skladu s dijelom II. točkom 3. Priloga I. proizvođač mora u cijelom razdoblju potpore provoditi djelotvorna i redovita ispitivanja i preispitivanja proizvoda s digitalnim elementima. Za redovita ispitivanja nije nužno mehaničko ponavljanje nepromijenjenog ispitnog ciklusa u utvrđenim vremenskim razmacima. Riječ je o redovitom preispitivanju toga treba li zbog novih čimbenika, kao što su novoutvrđene prijetnje ili novootkrivene ranjivosti, ažurirati postojeća ispitivanja i provoditi ih u skladu s tim.

239. Učestalost, opseg i sadržaj preispitivanja trebali bi biti razmjerni profilu kibernetičkosigurnosne rizičnosti proizvoda s digitalnim elementima, njegovu razvoju tijekom vremena i stanju prijetnji. Ako se preispitivanjem utvrde relevantni novi čimbenici koji utječu na postavke ispitivanja, trebalo bi osmisliti nova ili izmijenjena ispitivanja i provesti ih na proizvodu kako bi se osiguralo da se sve ranjivosti otklone. To može uključivati ponovno provođenje postojećih ispitivanja ako su zbog izmjene proizvoda s digitalnim elementima te vrste ispitivanja primjerene, kao što je regresijsko ispitivanje.

240. Ako se preispitivanjem ne utvrde takvi čimbenici, nije potrebno osmisliti dodatna ispitivanja. Druge obveze postupanja s ranjivostima, uključujući one koje se odnose na razmatranje i otklanjanje ranjivosti povezanih s nastalim rizicima, i dalje se primjenjuju usporedno.

9.3. **Međudjelovanje s drugim zakonodavstvom**

9.3.1. *Uredba (EU) 2019/2144 i Uredba (EU) br. 168/2013*

241. Člankom 2. stavkom 2. točkom (c) Akta o kibernetičkoj otpornosti utvrđeno je da se Uredba ne primjenjuje na proizvode s digitalnim elementima na koje se primjenjuje Uredba (EU) 2019/2144. Uredba (EU) 2019/2144 primjenjuje se na „vozila kategorija M, N i O, utvrđenih u članku 4. Uredbe (EU) 2018/858, i na sustave, sastavne dijelove i zasebne tehničke jedinice konstruirane i izrađene za ta vozila”.

242. Slično tomu, proizvodi s digitalnim elementima koji su obuhvaćeni područjem primjene Uredbe (EU) br. 168/2013 isključeni su iz područja primjene Akta o kibernetičkoj otpornosti Delegiranom uredbom Komisije (EU) 2025/1535. Uredba (EU) br. 168/2013 primjenjuje se na vozila kategorije L i „sustave, sastavne dijelove i zasebne tehničke jedinice, kao i dijelove i opremu, konstruirane i izrađene za takva vozila” (članak 2. stavak 1.).

243. Vozila na koja se te uredbe primjenjuju nisu obuhvaćena područjem primjene Akta o kibernetičkoj otpornosti. Nadalje, potrebna su dodatna pojašnjenja područja primjene izuzeća za sustave, sastavne dijelove, zasebne tehničke jedinice, dijelove i opremu (za potrebe ovog odjeljka „sastavni dijelovi”) koji su konstruirani i izrađeni za takva vozila i koji se smatraju proizvodima s digitalnim elementima u smislu Akta o kibernetičkoj otpornosti.

244. Smatra se da se na te sastavne dijelove ne primjenjuje Akt o kibernetičkoj otpornosti, pod uvjetom da su konstruirani i izrađeni isključivo za ugradnju u vozila obuhvaćena uredbama (EU) 2019/2144 i (EU) br. 168/2013. To vrijedi neovisno o tome prodaje li ga proizvođač tog sastavnog dijela izravno proizvođaču vozila ili drugom gospodarskom subjektu u automobilskom lancu opskrbe, pod uvjetom da je taj sastavni dio očito namijenjen i prikladan isključivo za konačnu ugradnju u ta vozila.

245. S druge strane, na proizvođača koji prodaje generičke sastavne dijelove koji su proizvodi s digitalnim elementima koji se mogu ugraditi u razne vrste proizvoda, a ne isključivo u vozila obuhvaćena tim uredbama, primjenjuje se Akt o kibernetičkoj otpornosti.

246. Ocjena toga stavlja li se sastavni dio na tržište u smislu Akta o kibernetičkoj otpornosti mora se temeljiti na objektivnim uvjetima pod kojima se stavlja na raspolaganje. Ako proizvođač nudi sastavni dio koji nije prikladan isključivo za konačnu ugradnju u ta vozila distribucijskim kanalima koji su otvoreni i kupcima izvan automobilskog lanca opskrbe, kao što su opća maloprodajna mjesta ili internetski prodajni kanali koji prihvaćaju narudžbe od šire javnosti, taj je sastavni dio obuhvaćen područjem primjene Akta o kibernetičkoj otpornosti, neovisno o izjavama o njegovoj predviđenoj namjeni. U tim se okolnostima ne može smatrati da je sastavni dio konstruiran i izrađen isključivo za ugradnju u vozila obuhvaćena uredbama (EU) 2019/2144 i (EU) br. 168/2013, a proizvođač mora postupati u skladu s Aktom o kibernetičkoj otpornosti. S druge strane, upotreba ograničenih distribucijskih kanala među poduzećima dostupnih samo subjektima u automobilskom lancu opskrbe može upućivati na to da je konstruiran i izrađen isključivo za takvu ugradnju.

9.3.2. *Valjanost potvrda o EU ispitivanju tipa (članak 69. stavak 1.)*

247. U članku 69. stavku 1. Akta o kibernetičkoj otpornosti navedeno je da „[p]otvrde 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 Uredba 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”.

248. Kontinuiranu valjanost tih potvrda i odluka o odobrenju trebalo bi tumačiti kao da je ograničena na kibernetičkosigurnosne rizike i odgovarajuće zahtjeve obuhvaćene odgovarajućim zakonodavstvom Unije o usklađivanju na temelju kojeg su izdani. U kontekstu tih rizika proizvođači nisu obvezni ponovno ocijeniti ili ponovno dokazati usklađenost isključivo za potrebe Akta o kibernetičkoj otpornosti u razdoblju valjanosti iz članka 69. stavka 1. za proizvode s digitalnim elementima koje namjeravaju staviti na tržište 11. prosinca 2027. ili nakon tog datuma te do 11. lipnja 2028 ([31]). To se odnosi na izdane potvrde i odluke o odobrenju ako je u skladu s primjenjivim zakonodavstvom Unije o usklađivanju proizvođač dužan provesti postupak ocjenjivanja sukladnosti preko prijavljenog tijela te ako je proizvođač to dobrovoljno odlučio učiniti.

249. Stoga valjana potvrda ili odluka o odobrenju izdana u skladu s drugim zakonodavstvom Unije o usklađivanju ne oslobađa proizvođače od obveze provedbe sveobuhvatne procjene kibernetičkosigurnosnih rizika u skladu s Aktom o kibernetičkoj otpornosti (ili od drugih obveza na temelju tog akta). Zapravo im omogućuje da se u svojem postupku ocjenjivanja sukladnosti oslone na postojeće certifikate kao dokaz usklađenosti ako su odgovarajući kibernetičkosigurnosni rizici već obuhvaćeni. Ako je potvrda ili odluka o odobrenju na temelju drugog zakonodavstva Unije o usklađivanju valjana i nakon 11. lipnja 2028., proizvođač se na tu potvrdu ili odluku za potrebe Akta o kibernetičkoj otpornosti može osloniti samo do 11. lipnja 2028.

250. Ako se procjenom kibernetičkosigurnosnih rizika provedenom u skladu s člankom 13. stavkom 2. utvrde dodatni rizici koji nisu obuhvaćeni zahtjevima u pogledu kibernetičke sigurnosti na kojima se temelji postojeća potvrda ili odluka o odobrenju, proizvođači su i dalje odgovorni za uklanjanje tih rizika u skladu s Aktom o kibernetičkoj otpornosti. U tim slučajevima za usklađenost su potrebni procjena i uklanjanje utvrđenih nedostataka, neovisno o kontinuiranoj valjanosti postojeće potvrde ili odluke o odobrenju.

251. Kao primjer može poslužiti slučaj u kojem se na proizvod s digitalnim elementima primjenjuju zahtjevi u pogledu kibernetičke sigurnosti iz Delegirane uredbe Komisije (EU) 2022/30 o dopuni Direktive 2014/53/EU (delegirani akt o Direktivi o radijskoj opremi (RED)) i u kojem je na temelju tih zahtjeva izdana potvrda o EU ispitivanju tipa ili odluka o odobrenju. U tom slučaju potvrda ili odluka ostaju valjani, u skladu s člankom 69. stavkom 1., za kibernetičkosigurnosne rizike koji su obuhvaćeni tim certifikatom i koji su povezani s bitnim zahtjevima u pogledu kibernetičke sigurnosti iz Direktive 2014/53/EU (Direktiva o radijskoj opremi ili „RED”).

252. U tim slučajevima proizvođači za potrebe Akta o kibernetičkoj otpornosti nisu obvezni ponovno ocijeniti ili ponovno dokazati usklađenost u odnosu na rizike koji su već obuhvaćeni tim certifikatima sve dok je relevantna potvrda ili odluka o odobrenju valjana, a u svakom slučaju sve do najkasnije 11. lipnja 2028. To uključuje, na primjer, kibernetičkosigurnosne rizike koji su povezani sa zaštitom mreže, zaštitom osobnih podataka i privatnosti ili sprečavanjem prijevara (ako su ti rizici obuhvaćeni tim certifikatom) koji se odnose na zahtjeve u pogledu kibernetičke sigurnosti iz Direktive o radijskoj opremi i koji se uzimaju u obzir u ocjenjivanju sukladnosti.

253. Međutim, ako se procjenom kibernetičkosigurnosnih rizika provedenom u skladu s člankom 13. stavkom 2. Akta o kibernetičkoj otpornosti utvrde dodatni kibernetičkosigurnosni rizici koji nisu obuhvaćeni tim certifikatima, proizvođači su i dalje odgovorni za uklanjanje tih rizika u skladu s Aktom o kibernetičkoj otpornosti. To može uključivati, na primjer, rizike povezane s procesima postupanja s ranjivostima, smanjenjem količine podataka i smanjenjem površine napada ili druge kibernetičke sigurnosne aspekte specifične za proizvod koji nisu obuhvaćeni tim certifikatima ili, u svakom slučaju, koji nisu obuhvaćeni bitnim zahtjevima u pogledu kibernetičke sigurnosti iz Direktive o radijskoj opremi.

254. Stoga postojanje valjane potvrde o EU ispitivanju tipa ili odluke o odobrenju na temelju Direktive o radijskoj opremi za njezine bitne zahtjeve koji se odnose na kibernetičku sigurnost samo po sebi ne dokazuje potpunu usklađenost s Aktom o kibernetičkoj otpornosti. Zapravo se proizvođačima omogućuje da se oslone na tu potvrdu ili odluku kao dokaz usklađenosti za odgovarajuće rizike, dok se svi preostali ili novoutvrđeni rizici procjenjuju i ublažavaju u skladu s Aktom o kibernetičkoj otpornosti.

([31]) Na proizvode s digitalnim elementima stavljene na tržište prije 11. prosinca 2027. primjenjuje se zakonodavstvo Unije važeće u trenutku njihova stavljanja na tržište te se, ako su usklađeni s njim, mogu prodavati i pustiti u rad, osim ako su 11. prosinca 2027. ili nakon tog datuma znatno izmijenjeni. Za pojmove „stavljanje na tržište” i „stavljanje na raspolaganje na tržištu” vidjeti i odjeljak *2.1.* – Stavljanje na tržište ovog dokumenta te poglavlje 2. Plavog vodiča.

255. Slično tomu, ako se na proizvod s digitalnim elementima primjenjuju bitni zdravstveni i sigurnosni zahtjevi povezani s kibernetičkom sigurnošću utvrđeni u Uredbi (EU) 2023/1230 (Uredba o strojevima), koja se u potpunosti primjenjuje od 20. siječnja 2027., i ako je na temelju tih zahtjeva izdana potvrda o EU ispitivanju tipa ili odluka o odobrenju, ta potvrda ili odluka o odobrenju i dalje je valjana, u skladu s člankom 69. stavkom 1. Akta o kibernetičkoj otpornosti, za kibernetičkosigurnosne rizike obuhvaćene Uredbom o strojevima.

256. To se prije svega odnosi na aspekte kibernetičke sigurnosti povezane sa zaštitom od zlouporabe te sigurnošću i pouzdanošću kontrolnih sustava, kako je utvrđeno u odjeljcima 1.1.9. i 1.2.1. Priloga III. Uredbi o strojevima. Kad je riječ o tim rizicima, proizvođači za potrebe Akta o kibernetičkoj otpornosti nisu obvezni ponovno ocijeniti ili ponovno dokazati usklađenost sve dok je relevantna potvrda ili odluka o odobrenju valjana, a u svakom slučaju sve do najkasnije 11. lipnja 2028. To vrijedi ako su ti rizici uklonjeni u okviru ocjenjivanja sukladnosti na temelju Uredbe o strojevima.

257. Kao i u slučaju prethodno navedenih bitnih zahtjeva u pogledu kibernetičke sigurnosti iz Direktive o radijskoj opremi, ako se u okviru procjene kibernetičkosigurnosnih rizika provedene u skladu s člankom 13. stavkom 2. Akta o kibernetičkoj otpornosti utvrde dodatni kibernetičkosigurnosni rizici koji nisu obuhvaćeni relevantnim certifikatom izdanim u skladu s Uredbom o strojevima i koji su povezani sa zahtjevima u pogledu kibernetičke sigurnosti iz te uredbe, proizvođači su i dalje odgovorni za uklanjanje tih rizika u skladu s Aktom o kibernetičkoj otpornosti.