C/2026/6013

17.11.2026

SPOROČILO KOMISIJE

Smernice Komisije o uporabi Uredbe (EU) 2024/2847 (akt o kibernetski odpornosti)

(C/2026/6013)

Vsebina

Stran

1. UVOD ... 3
   - 1.1 Akt o kibernetski odpornosti ... 3
   - 1.2 Namen usmeritev ... 3
2. PODROČJE UPORABE ... 4
   - 2.1 Dajanje na trg ... 4
   - 2.2 Programska oprema kot izdelek z digitalnimi elementi ... 5
   - 2.3 Računalniška koda ... 6
   - 2.4 Kombinacija strojne in programske opreme, ki sestavlja izdelek z digitalnimi elementi ... 7
   - 2.5 Podatkovna povezava ... 8
   - 2.6 Kompleksni sistemi ... 8
   - 2.7 Izdelki z digitalnimi elementi, zasnovani pred začetkom uporabe akta o kibernetski odpornosti ... 9
3. PROSTA IN ODPRTOKODNA PROGRAMSKA OPREMA ... 11
   - 3.1 Ugotavljanje, ali je prosta in odprtokodna programska oprema pod odgovornostjo določene osebe ... 12
   - 3.2 Ugotavljanje, ali je prosta in odprtokodna programska oprema dana na trg EU ... 13
     - 3.2.1 Zaračunavanje cene ... 13
     - 3.2.2 Monetizacija drugih storitev ali zahteva po obdelavi osebnih podatkov ... 13
     - 3.2.3 Podporne storitve ... 14
     - 3.2.4 Donacije ... 15
     - 3.2.5 Financiranje proste in odprtokodne programske opreme ... 15
     - 3.2.6 Neprofitni subjekti, ustanovljeni za doseganje neprofitnih ciljev ... 16
     - 3.2.7 Vgradnja s strani drugih proizvajalcev ... 16
   - 3.3 Upravljavci odprtokodne programske opreme ... 16
     - 3.3.1 Trajna podpora in zagotavljanje sposobnosti preživetja proste in odprtokodne programske opreme ... 17
   - 3.4 Prispevajoče osebe in uporabe nižje v verigi ... 18
   - 3.5 Ponazoritveni scenariji ... 19
4. BISTVENE SPREMEMBE IN REZERVNI DELI ... 21
   - 4.1 Fizična popravila ... 22
   - 4.2 Rezervni deli ... 23
   - 4.3 Posodobitve programske opreme kot bistvene spremembe ... 24

4.4 Posledice bistvene spremembe ... 27
4.4.1 Bistvene spremembe, ki jih izvede oseba, ki ni prvotni proizvajalec ... 28
4.4.2 Bistvene spremembe, ki jih izvede prvotni proizvajalec ... 29
5. OBDOBJE PODPORE ... 29
5.1 Bistvene spremembe in obdobje podpore ... 31
6. POMEMBNI IN KRITIČNI IZDELKI Z DIGITALNIMI ELEMENTI ... 32
6.1 Osnovna funkcija ... 33
6.2 Ugotavljanje skladnosti pomembnih in kritičnih izdelkov z digitalnimi elementi ... 36
6.3 Posledice za domnevo o skladnosti ... 38
7. OCENA TVEGANJA ZA KIBERNETSKO VARNOST TER VGRADNJA IZDELKOV Z DIGITALNIMI ELEMENTI IN SESTAVNIMI DELI ... 41
7.1 O ocenjevanju in obravnavi tveganj za kibernetsko varnost ... 41
7.2 O zasnovi, razvoju in proizvodnji izdelkov z digitalnimi elementi na način, ki zagotavlja ustrezno raven kibernetske varnosti glede na tveganja ... 42
7.3 Ocena tveganja in potrebna skrbnost v zvezi z zunanjimi odvisnostmi in vgrajenimi sestavnimi deli ... 42
7.4 Ponovna uporaba ocen tveganja in dokumentacije o skladnosti za družine izdelkov z digitalnimi elementi ... 44
8. DALJINSKA OBDELAVA PODATKOV ... 44
8.1 Kaj se šteje za rešitev za daljinsko obdelavo podatkov pri izdelku z digitalnimi elementi? ... 45
8.1.1 Pojem „na daljavo“ ... 46
8.1.2 Ali brez take obdelave podatkov izdelek z digitalnimi elementi ne bi mogel opravljati ene od svojih funkcij? ... 46
8.1.3 Ali je programsko opremo zasnoval in razvil proizvajalec oziroma ali je bila zasnovana in razvita pod njegovo odgovornostjo? ... 47
8.2 Praktične in tehnične posledice rešitev za daljinsko obdelavo podatkov ter zanašanja na rešitve tretjih oseb ... 49
8.3 Primeri uporabe rešitev za daljinsko obdelavo podatkov ... 50
8.3.1 Aplikacija za mobilno bančništvo ... 51
8.3.2 Pametni termostat ... 52
8.3.3 E-bralnik ... 53
8.3.4 Industrijski robot ... 53
8.3.5 Mobilno omrežje ... 53
9. DODATNI ELEMENTI ... 54
9.1 Obveznosti poročanja ... 54
9.2 Obravnavanje ranljivosti ... 56
9.2.1 Poročanje navzgor v verigi in deljenje varnostnih popravkov ... 56
9.2.2 Znane izrabljive ranljivosti ... 57
9.2.3 Učinkovita in redna preverjanja ter pregledi ... 58
9.3 Medsebojni vpliv med to uredbo in drugo zakonodajo ... 59
9.3.1 Uredba (EU) 2019/2144 in Uredba (EU) št. 168/2013 ... 59
9.3.2 Veljavnost potrdil o EU-pregledu tipa (člen 69(1)) ... 59

1. **UVOD**

1.1 **Akt o kibernetski odpornosti**

1. Uredba (EU) 2024/2847 Evropskega parlamenta in Sveta z dne 23. oktobra 2024 o horizontalnih zahtevah glede kibernetske varnosti za izdelke z digitalnimi elementi in spremembi uredb (EU) št. 168/2013 in (EU) 2019/1020 ter Direktive (EU) 2020/1828 (Akt o kibernetski odpornosti) ([1]) je začela veljati 10. decembra 2024. Cilj uredbe je okrepiti pristop Unije h kibernetski varnosti, obravnavati kibernetsko odpornost na ravni EU ter izboljšati delovanje notranjega trga z določitvijo enotnega pravnega okvira za bistvene zahteve glede kibernetske varnosti za dajanje izdelkov z digitalnimi elementi na trg EU ter v življenjskem ciklu izdelkov z digitalnimi elementi.

2. Akt o kibernetski odpornosti temelji na novem zakonodajnem okviru EU iz Uredbe (ES) št. 765/2008 Evropskega parlamenta in Sveta z dne 9. julija 2008 o določitvi zahtev za akreditacijo in nadzor trga v zvezi s trženjem proizvodov ter razveljavitvi Uredbe (EGS) št. 339/93 in Sklepa št. 768/2008/ES Evropskega parlamenta in Sveta z dne 9. julija 2008 o skupnem okviru za trženje proizvodov in razveljavitvi Sklepa Sveta 93/465/EGS ([2]).

3. Nadzor trga in izvrševanje izvajajo nacionalni organi za nadzor trga. Za izdelke z digitalnimi elementi, ki spadajo na področje uporabe akta o kibernetski odpornosti, se uporablja Uredba (EU) 2019/1020 Evropskega parlamenta in Sveta z dne 20. junija 2019 o nadzoru trga in skladnosti proizvodov ter spremembi Direktive 2004/42/ES in uredb (ES) št. 765/2008 in (EU) št. 305/2011. Komisija in Agencija Evropske unije za kibernetsko varnost (ENISA) podpirata gospodarske subjekte in države članice pri uporabi akta o kibernetski odpornosti.

1.2 **Namen usmeritev**

4. Člen 26(1) akta o kibernetski odpornosti določa, da Komisija objavi usmeritve za pomoč gospodarskim subjektom pri uporabi Uredbe s posebnim poudarkom na lajšanju zagotavljanja skladnosti mikropodjetij ter malih in srednjih podjetij. Člen 26(2) določa minimalne vidike, ki bi jih bilo treba obravnavati v usmeritvah. Med temi so: (i) področje uporabe akta o kibernetski odpornosti (zlasti rešitve za daljinsko obdelavo podatkov ter prosta in odprtokodna programska oprema); (ii) pojem „obdobja podpore“; (iii) medsebojni vpliv med aktom o kibernetski odpornosti in drugo zakonodajo EU ter (iv) pojem „bistvena sprememba“.

5. Komisija je 3. decembra 2025 objavila vrsto pogosto zastavljenih vprašanj, ki naj bi gospodarskim subjektom pomagala pri pripravi na izvajanje akta o kibernetski odpornosti ([3]).

6. Namen teh usmeritev je gospodarskim subjektom pomagati pri zagotavljanju skladnosti z aktom o kibernetski odpornosti in podpirati dejavnosti organov za nadzor trga, priglasitvenih organov in priglašenih organov, da se zagotovi usklajeno izvrševanje akta o kibernetski odpornosti po vsej Uniji. Niso namenjene obravnavi celotnega akta o kibernetski odpornosti, temveč naj bi pojasnile utemeljitev nekaterih ključnih določb in način njihovega izvajanja v praksi. Te usmeritve se nanašajo na akt o kibernetski odpornosti in se ne uporabljajo za drugo zakonodajo EU.

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

([2]) Delovni program Komisije za leto 2026 predvideva predstavitev evropskega akta o proizvodih, s katerim bi se posodobili nov zakonodajni okvir ter pravila o nadzoru trga in standardizaciji: https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:52025DC0870.

([3]) Pogosto zastavljena vprašanja je mogoče prenesti prek Komisijinega spletišča o izvajanju akta o kibernetski odpornosti s posebne spletne strani s pogosto zastavljenimi vprašanji.

7. Pri njihovi pripravi se je izvedlo obsežno posvetovanje z deležniki, med drugim s strokovno skupino za kibernetsko varnost izdelkov z digitalnimi elementi ([4]) in v okviru javnega posvetovanja, ki je potekalo od 3. marca do 13. aprila 2026 ([5]).

8. Te usmeritve niso zavezujoče za gospodarske subjekte ali druge akterje, za katere velja akt o kibernetski odpornosti. Verodostojno razlago akta o kibernetski odpornosti lahko poda le Sodišče Evropske unije. Vendar te usmeritve vsebujejo razlago akta o kibernetski odpornosti s strani Komisije, da bi se podprlo zagotavljanje skladnosti in prispevalo k učinkovitemu izvajanju Uredbe. Poleg tega vsebujejo več primerov, ki ponazarjajo uporabo posameznih določb. Toda ti primeri niso namenjeni temu, da bi nadomestili oceno za vsak primer posebej, ki bo vedno potrebna, da se bodo upoštevale posebnosti vsakega posameznega primera.

9. Komisija lahko v skladu s členom 26 akta o kibernetski odpornosti razmisli o izdaji nadaljnjih usmeritev, vključno z usmeritvami, namenjenimi proizvajalcem, za katere veljajo akt o kibernetski odpornosti in druga harmonizacijska zakonodaja Unije ali drugi povezani pravni akti Unije. V teh usmeritvah se lahko na primer obravnavajo vprašanja medsebojnega vpliva med aktom o kibernetski odpornosti in Uredbo (EU) 2024/1689 o določitvi harmoniziranih pravil o umetni inteligenci (akt o umetni inteligenci) ter Uredbo (EU) 2022/2554 o digitalni operativni odpornosti za finančni sektor (DORA).

2. **PODROČJE UPORABE**

2.1 **Dajanje na trg**

10. Akt o kibernetski odpornosti se uporablja za izdelke z digitalnimi elementi, ki so dostopni na trgu EU. Pojem omogočanja dostopnosti na trgu v skladu s členom 3(22) akta o kibernetski odpornosti pomeni „dobavo izdelka z digitalnimi elementi za distribucijo ali uporabo na trgu Unije v okviru gospodarske dejavnosti, za plačilo ali brezplačno“. V skladu s členom 3(21) je izdelek z digitalnimi elementi dan na trg EU, ko je njegova dostopnost prvič omogočena.

11. Najnovejša izdaja „Modrega vodnika“ za izvajanje predpisov EU o proizvodih, objavljena leta 2022 (v nadaljnjem besedilu: Modri vodnik) ([6]), vsebuje usmeritve, ki olajšujejo razumevanje predpisov EU o proizvodih in njihovo enotno uporabo v različnih sektorskih pravnih okvirih, usklajenih z novim zakonodajnim okvirom, kot je akt o kibernetski odpornosti. Modri vodnik navaja, da je treba pojma „dajanje na trg“ in „zagotavljanje dostopnosti na trgu“ razumeti, kot da se nanašata „na vsak posamezen proizvod in ne na tip proizvoda, ne glede na to, ali je bil izdelan kot posamezna enota ali del serije“ (oddelek 2.3).

12. Pri bolj „tradicionalnih“ izdelkih z digitalnimi elementi, zajetih z novim zakonodajnim okvirom, kot so strojna oprema v obliki strojev ali proizvodi radijske opreme z digitalnimi elementi, je pojem „dajanja na trg“ dobro uveljavljen, Modri vodnik pa vsebuje dodatne usmeritve za pojasnitev, kdaj se šteje, da so taki izdelki dani na trg. „Povzetki primerov“ v oddelku 2.12 Modrega vodnika vsebujejo dodatne primere pojma „dajanje na trg“.

13. Toda zaradi narave nematerialnih izdelkov z digitalnimi elementi, kot je samostojna programska oprema, so potrebne dodatne usmeritve o tem, kdaj se šteje, da so taki izdelki z digitalnimi elementi dani na trg. Ko je faza proizvodnje programske opreme zaključena in se izdelek z digitalnimi elementi ponudi potencialnim uporabnikom na trgu EU, se lahko šteje, da je njegov proizvajalec izdelal več kopij istega programskega izdelka z digitalnimi elementi in jih dobavil za distribucijo ali uporabo. V nasprotju z materialnimi izdelki z digitalnimi elementi pa za samostojno programsko opremo ne veljajo omejitve fizične proizvodnje ali zalog: z vsakim

([4]) Strokovna skupina za kibernetsko varnost izdelkov z digitalnimi elementi v registru strokovnih skupin Komisije in drugih podobnih skupin.
([5]) Javno posvetovanje o osnutku usmeritev Komisije o aktu o kibernetski odpornosti.
([6]) Obvestilo Komisije „Modri vodnik“ za izvajanje predpisov EU o proizvodih 2022 2022/C 247/01 (UL C 247, 29.6.2022, str. 1).

dejanjem omogočanja dostopnosti programske opreme za prenos ali distribucijo se za uporabnika ustvari nova enaka kopija. Dokler se ta različica programske opreme ne spremeni tako, da to vpliva na skladnost z aktom o kibernetski odpornosti, se šteje, da je do dajanja na trg EU prišlo v trenutku prve ponudbe za distribucijo ali uporabo. Zato je treba možnost nadaljnjega prenosa ali distribucije te različice programskega izdelka z digitalnimi elementi šteti za primer, ko se omogoči dostopnost tega programskega izdelka z digitalnimi elementi ([7]).

14. Zato bi bilo treba šteti, da je samostojni programski izdelek z digitalnimi elementi dan na trg, ko je njegova faza proizvodnje zaključena in se ta programska oprema prvič dobavi za distribucijo ali uporabo na trgu EU v okviru gospodarske dejavnosti. Šteti bi bilo treba, da je proizvajalec hkrati dal na trg več kopij istega programskega izdelka z digitalnimi elementi. Čeprav več kopij iste programske opreme še vedno predstavlja posamezen izdelek z digitalnimi elementi, se šteje, da so dane na trg hkrati, ne glede na to, kdaj se posest ali uporaba posamezne kopije prenese na drugo fizično ali pravno osebo. Hkrati pa, kadar proizvajalec omogoči dostopnost programske opreme v različnih različicah, ki se razlikujejo po vključenih sestavnih delih, konfiguracijah ali podprtih funkcijah (na primer različice za različne operacijske sisteme ali paketi z različnimi nabori funkcij), teh različic ni mogoče šteti za več kopij istega programskega izdelka z digitalnimi elementi. Zato bi jih bilo treba za namene dajanja na trg obravnavati kot ločene izdelke z digitalnimi elementi.

Primer 1: družba A prek svojega spletišča 1. januarja 2028 prvič dobavi za distribucijo različico 1.0.0 svoje programske opreme X. Stranka 1 istega dne kupi kopijo različice 1.0.0 programske opreme X. Stranka 2 kupi kopijo različice 1.0.0 programske opreme X 15. januarja 2028. Obe kopiji različice 1.0.0 programske opreme X sta dani na trg 1. januarja 2028.

15. Glede na ponavljajočo se naravo razvoja programske opreme bi bilo treba dodatno pojasniti, da za nadaljnje različice programskega izdelka z digitalnimi elementi velja, da so na novo dane na trg, kadar se štejejo za „bistveno spremembo“ programskega izdelka z digitalnimi elementi, ki je že bil dan na trg, kot je navedeno v uvodni izjavi 41 akta o kibernetski odpornosti. Za različice, ki se ne štejejo za bistvene spremembe, proizvajalcu ni treba izvesti novega postopka ugotavljanja skladnosti, zato se datum dajanja te programske opreme na trg ne spremeni. Za več usmernitev o pojmu bistvenih sprememb glej oddelek 4 *Substantial modifications*.

Primer 2: družba A prek svojega spletišča 1. januarja 2028 prvič dobavi za distribucijo različico 1.0.0 svoje programske opreme X. Stranka 1 istega dne kupi kopijo različice 1.0.0 programske opreme X. Družba A dne 15. januarja 2028 izda posodobljeno različico 1.0.1 programske opreme X, ki ne pomeni bistvene spremembe. Stranka 2 dne 30. januarja 2028 kupi kopijo različice 1.0.1 programske opreme X. Za obe kopiji različic 1.0.0 in 1.0.1 programske opreme X se šteje, da sta dani na trg 1. januarja 2028.

16. Usmeritve iz točk 13, 14 in 15 se uporabljajo le, če je izdelek z digitalnimi elementi samostojna programska oprema. To na primer ne velja, kadar je programska oprema združena s strojno opremo, kot je obravnavano v oddelku *2.4 Combination of hardware and software forming a product*.

2.2 **Programska oprema kot izdelek z digitalnimi elementi**

17. V členu 3(1) akta o kibernetski odpornosti je izdelek z digitalnimi elementi opredeljen kot „izdelek programske ali strojne opreme ter njegove rešitve za daljinsko obdelavo podatkov, vključno s sestavnimi deli programske ali strojne opreme, ki se dajejo na trg ločeno“. Taki izdelki z digitalnimi elementi spadajo na področje uporabe akta o kibernetski odpornosti, kadar njihov predvideni namen ali razumno predvidljiva uporaba vključuje neposredno ali posredno logično ali fizično podatkovno povezavo z napravo ali omrežjem.

([7]) V skladu s členom 13(11) lahko proizvajalci vzdržujejo javne arhive programske opreme, ki izboljšujejo dostop uporabnikov do zgodovinskih različic. V teh primerih so uporabniki na lahko dostopen način jasno obveščeni o tveganjih, povezanih z uporabo nepodprte programske opreme.

18. Akt o kibernetski odpornosti lahko zato zajema vrsto izdelkov z digitalnimi elementi, med drugim: (i) samostojno programsko opremo, kot so aplikacije in računalniški programi, ki se distribuirajo digitalno ali fizično; (ii) strojno opremo z vgrajeno programsko opremo (npr. naprave interneta stvari, prenosni računalniki, tablični računalniki); (iii) samostojno strojno opremo (npr. integrirana vezja, matične plošče) ter (iv) vsako kombinacijo strojne in programske opreme, ki se dobavljata ločeno, vendar sta namenjeni skupnemu delovanju.

19. Samostojna programska oprema zato spada na področje uporabe akta o kibernetski odpornosti, kadar je dana na trg kot izdelek z digitalnimi elementi. Koristno je razlikovati med programskimi izdelki z digitalnimi elementi, za katere velja akt o kibernetski odpornosti, in opravljanjem storitev na daljavo, ki ne spadajo na področje uporabe akta o kibernetski odpornosti.

20. Da bi programska oprema spadala na področje uporabe akta o kibernetski odpornosti, se mora programski izdelek z digitalnimi elementi zagotoviti uporabniku, ta pa ga mora pridobiti in uporabljati v elektronskem informacijskem sistemu na uporabniški strani ali kot del takšnega sistema. Programska oprema, ki se prenese, namesti ali drugače dobavi uporabniku in se izvaja v uporabnikovem elektronskem informacijskem sistemu, izpolnjuje ta merila, na primer kadar je v obliki razširitve brskalnika ali aplikacije, razvite s spletnimi tehnologijami, vendar dobavljene za lokalno izvajanje.

21. Nasprotno pa programska oprema, ki se izvaja na daljavo in do katere uporabnik le dostopa, zgolj na tej podlagi ni izdelek z digitalnimi elementi. To razlikovanje je namreč pojasnjeno v uvodnih izjavah 11 in 12 akta o kibernetski odpornosti, v katerih je navedeno, da za obdelavo ali shranjevanje na daljavo akt o kibernetski odpornosti velja le v obsegu, v katerem je to potrebno, da izdelek z digitalnimi elementi opravlja svoje funkcije (tj. v okviru pojma daljinske obdelave podatkov, kot je opredeljen v členu 3(2)), sama obdelava ali shranjevanje pa ni izdelek z digitalnimi elementi. To običajno velja za spletne aplikacije, vključno s progresivnimi spletnimi aplikacijami, kadar se do njih dostopa izključno prek spletnega brskalnika. Enako velja za spletišča: čeprav se lahko spletišča v omejenem obsegu tehnično zaženejo in izvajajo na uporabnikovi napravi, iz uvodne izjave 12 akta o kibernetski odpornosti izhaja, da se spletišča sama po sebi ne štejejo za izdelke z digitalnimi elementi in spadajo na področje uporabe akta o kibernetski odpornosti le, kadar podpirajo funkcionalnost izdelka z digitalnimi elementi, tj. v obsegu, v katerem se štejejo za daljinsko obdelavo podatkov (kot je dodatno pojasnjeno v oddelku *8* in zlasti *8.1.2 Would the absence of such data processing prevent the product with digital elements from performing one of its functions?*).

Primer 3: mobilna aplikacija, ki jo uporabnik prenese iz trgovine z aplikacijami in namesti na svoj pametni telefon, je dobavljena uporabniku in se izvaja na uporabnikovi napravi, zato je izdelek z digitalnimi elementi. Kadar je dana na trg v okviru gospodarske dejavnosti, lahko spada na področje uporabe akta o kibernetski odpornosti.

Primer 4: namizna aplikacija, izdelana s spletnimi tehnologijami, vendar pakirana za lokalno namestitev, je dobavljena uporabniku in se izvaja na uporabnikovi napravi, zato je izdelek z digitalnimi elementi. Kadar je dana na trg v okviru gospodarske dejavnosti, lahko spada na področje uporabe akta o kibernetski odpornosti.

Primer 5: spletna aplikacija, do katere uporabnik dostopa izključno prek spletnega brskalnika, ni izdelek z digitalnimi elementi. Če ne podpira funkcionalnosti izdelka z digitalnimi elementi, ne spada na področje uporabe akta o kibernetski odpornosti. Nasprotno pa je aplikacija, ki se uporabniku dobavi kot odjemalec, nameščen lokalno, in se izvaja na uporabnikovi napravi, izdelek z digitalnimi elementi. Kadar je dana na trg v okviru gospodarske dejavnosti, lahko spada na področje uporabe akta o kibernetski odpornosti.

Če se ta odjemalec za opravljanje ene ali več svojih funkcij opira na obdelavo podatkov na daljavo, ki ustreza opredelitvi daljinske obdelave podatkov, je tudi ta obdelava podatkov na daljavo del izdelka z digitalnimi elementi.

Primer 6: spletišče, ki svojim obiskovalcem zgolj predstavlja informacije in ne podpira funkcionalnosti izdelka z digitalnimi elementi, samo po sebi ni izdelek z digitalnimi elementi. Zato ne spada na področje uporabe akta o kibernetski odpornosti.

2.3 **Računalniška koda**

22. Koristno je tudi pojasniti, ali lahko izvorna koda pomeni programski izdelek z digitalnimi elementi. V aktu o kibernetski odpornosti je programska oprema opredeljena kot „del elektronskega informacijskega sistema, ki ga sestavlja računalniška koda“ (člen 3(4)). Računalniška koda je lahko v obliki (i) strojne kode, tj. sklopa navodil, ki jih neposredno izvršuje procesor računalnika in so zapisana v binarni obliki, ali (ii) izvorne kode, tj. sklopa navodil in stavkov, napisanih v programskem jeziku, ki jih je treba prevesti ali razložiti, da jih lahko računalnik izvrši. Opredelitev programske opreme iz akta o kibernetski odpornosti zajema oboje.

23. Ločeno vprašanje je, ali določena dobava računalniške kode pomeni dajanje izdelka z digitalnimi elementi na trg EU, za kar mora biti dobava v okviru gospodarske dejavnosti. Pri izvorni kodi pogosto ni tako. Za fizično ali pravno osebo, ki prosto in odprto računalniško kodo deli v javno dostopnih repozitorijih, se na primer na splošno ne šteje, da za namene akta o kibernetski odpornosti daje to kodo na trg EU (kot je podrobneje obravnavano v oddelku *3 Free and open-source software*). Nedokončana koda, ki se deli v fazi zasnove in razvoja izdelka z digitalnimi elementi (npr. za preskušanje ali pregled), se za namene akta o kibernetski odpornosti prav tako ne šteje za dano na trg, saj faza izdelave te kode ni zaključena. Podobno se tudi vzorčna ali predstavitvena koda, zagotovljena kot del priročnikov ali gradiva za usposabljanje, za namene akta o kibernetski odpornosti ne šteje za dano na trg ([8]).

24. Po drugi strani pa se, kadar proizvajalec svojim strankam zagotovi računalniško kodo kot izdelek z digitalnimi elementi, ta koda šteje za dano na trg, ne glede na to, ali gre za strojno kodo ali izvorno kodo ([9]).

Primer 7: družba A družbi B podeli licenco za izvorno kodo za prilagodljivo interno platformo in to izvorno kodo zagotovi v besedilni datoteki. Tudi če mora družba B to izvorno kodo pred uporabo nadalje prilagoditi in prevesti, jo na trg daje družba A in zato zanjo velja akt o kibernetski odpornosti. Družba A ni odgovorna za skladnost nadaljnjih prilagoditev in prevajanja te kode, ki jih opravi družba B, z aktom o kibernetski odpornosti.

2.4 **Kombinacija strojne in programske opreme, ki sestavlja izdelek z digitalnimi elementi**

25. Ali je programska oprema del izdelka z digitalnimi elementi, bi bilo treba določiti na podlagi tega, ali je glede na predvideni namen in razumno predvidljivo uporabo izdelka potrebna za to, da izdelek z digitalnimi elementi opravlja svoje predvidene funkcije, in ne na podlagi tega, kako ali kdaj se ta programska oprema dobavi uporabniku. Kadar je izdelek strojne opreme z digitalnimi elementi zasnovan tako, da za opravljanje svojih funkcij deluje skupaj s posebno programsko opremo, ki jo zagotovi isti proizvajalec, strojna oprema in ta programska oprema skupaj tvorita izdelek z digitalnimi elementi. Programska oprema, ki je potrebna za upravljanje, konfiguriranje, nadzorovanje ali uporabo izdelka z digitalnimi elementi v skladu z njegovim predvidenim namenom, je zato del izdelka z digitalnimi elementi, tudi če se pridobi prek ločenega kanala (npr. trgovine z aplikacijami, povezave za prenos ali drugega digitalnega kanala po tem, ko je bil izdelek strojne opreme z digitalnimi elementi dan na trg). Šteje se, da je ta programska oprema dana na trg v istem trenutku, kot so na trg dane enote izdelkov strojne opreme z digitalnimi elementi.

Primer 8: omrežni tiskalnik je dan na trg kot izdelek strojne opreme z digitalnimi elementi, medtem ko so gonilniki programske opreme, potrebni za pošiljanje tiskalnih opravil, konfiguriranje naprave in upravljanje njenega delovanja, na voljo za prenos s spletišča proizvajalca. Čeprav se tiskalnik in gonilniki dobavijo po različnih kanalih, skupaj tvorijo en sam izdelek z digitalnimi elementi, saj tiskalnik brez gonilnikov ne more izpolniti svojega predvidenega namena.

Primer 9: nosljiva naprava za fitnes se da na trg za merjenje srčnega utripa in aktivnosti uporabnika, medtem ko je za prikaz meritev in zgodovine ter konfiguracijo naprave potrebna aplikacija za pametni telefon, ki jo zagotovi proizvajalec. Čeprav se aplikacija prenese ločeno prek trgovine z aplikacijami, nosljiva naprava in aplikacija skupaj tvorita en sam izdelek z digitalnimi elementi, ker sta zasnovani in namenjeni za skupno delovanje, da zagotavljata funkcionalnost izdelka z digitalnimi elementi.

([8]) Opozoriti je treba tudi, da člen 4(3) proizvajalcem dovoljuje, da na trgu omogočijo dostopnost nedokončane programske opreme, ki ni skladna s to uredbo, kot so alfa ali beta različice ali predizdaje, če je nedokončana programska oprema dostopna samo za obdobje, potrebno za njeno preskušanje in zbiranje povratnih informacij.

([9]) Po drugi strani pa je treba opozoriti, da za namene prava o odgovornosti za proizvode računalniška koda sama po sebi ni proizvod, zato proizvajalci, ki tako kodo dajo na trg, ne morejo biti odgovorni na podlagi Direktive (EU) 2024/2853 (direktiva o odgovornosti za proizvode z napako). V uvodni izjavi 13 navedene direktive je navedeno, da „se informacije ne štejejo za proizvod in pravila o odgovornosti za proizvode se zato ne bi smela uporabljati za vsebino digitalnih datotek, kot so medijske datoteke ali e-knjige oziroma samo izvorna koda programske opreme“. To ne izključuje možnosti, da so proizvajalci odgovorni na podlagi nacionalnega odškodninskega prava.

2.5 **Podatkovna povezava**

26. Člen 2(1) določa, da se akt o kibernetski odpornosti „uporablja za izdelke z digitalnimi elementi, dostopne na trgu, katerih predvideni namen ali razumno predvidljiva uporaba vključuje neposredno ali posredno logično ali fizično podatkovno povezavo z napravo ali omrežjem“. Področje uporabe akta o kibernetski odpornosti zato ne temelji zgolj na prisotnosti elektronike, temveč na zmožnosti izdelka z digitalnimi elementi, da izmenjuje digitalne informacije.

27. Medtem ko sta izraza „logična povezava“ in „fizična povezava“ opredeljena v členu 3, izraza „podatkovna povezava“ ali „digitalni podatki“ v aktu o kibernetski odpornosti nista opredeljena. Zato je koristno razložiti izraz podatkovna povezava, da bi se pojasnila meja področja uporabe akta o kibernetski odpornosti. Ta meja je posebej pomembna za razlikovanje izdelkov z digitalnimi elementi, ki zgolj uporabljajo električne signale, od tistih, ki sodelujejo pri digitalnem komuniciranju in so zato izpostavljeni tveganjem za kibernetsko varnost.

28. Na najosnovnejši ravni podatkovna povezava vključuje prenos informacij v binarni obliki, tj. kot zaporedje števk 0 in 1. Zgolj vklapljanje in izklapljanje izhoda (tj. 0/1) samo po sebi ne pomeni podatkovne povezave, če ti stanji nista namenjeni predstavitvi podatkov ali ju digitalni vhod ne odčitava. Da bi podatkovna povezava obstajala, mora vir binarna stanja namenoma kodirati kot informacije, na cilju pa jih mora biti mogoče dekodirati kot informacije. Z drugimi besedami, obstajati morata pošiljatelj, ki namerno ustvarja digitalne simbole v skladu z določeno shemo, in prejemnik, ki je sposoben te simbole razložiti kot podatke. Kadar se električni ali elektronski signali uporabljajo izključno za sprožitev ali izvajanje funkcije, pri tem pa ne prenašajo digitalno kodiranih informacij, za namene akta o kibernetski odpornosti podatkovna povezava ne obstaja, zato izdelek z digitalnimi elementi ne spada na področje uporabe člena 2(1).

2.6 **Kompleksni sistemi**

29. Izdelki z digitalnimi elementi, ki spadajo na področje uporabe akta o kibernetski odpornosti, so lahko sestavljeni ne le iz posameznih naprav ali sestavnih delov programske opreme, temveč tudi iz kompleksnih sistemov, vključno s sistemi iz več elementov strojne in programske opreme, ki delujejo skupaj, da se izvede določena funkcija. Kadar se tak sistem da na trg kot en sam izdelek z digitalnimi elementi, se šteje za izdelek z digitalnimi elementi v smislu akta o kibernetski odpornosti.

30. Za te kompleksne sisteme so pogosto značilni dolgi cikli zasnove in razvoja, pogodbe, ki so bile morda podpisane pred začetkom uporabe akta o kibernetski odpornosti, podaljšana obratovalna doba ter visoka stopnja tehnične in organizacijske kompleksnosti. Takšni sistemi, ki bodo dani na trg po začetku uporabe akta o kibernetski odpornosti, lahko temeljijo na sestavnih delih, danih na trg pred začetkom uporabe akta o kibernetski odpornosti, na uveljavljenih arhitekturah ali na standardih interoperabilnosti, ki se splošno uporabljajo, vključno s standardi iz druge zakonodaje EU ali sektorskih okvirov. Zato bi bilo nekatere tehnične značilnosti teh sistemov težko ali nesorazmerno zahtevno spreminjati, ne da bi to vplivalo na njihov predvideni namen, varnost, zanesljivost ali interoperabilnost z obstoječo infrastrukturo.

31. Kompleksni sistemi zaradi teh značilnosti samih po sebi niso izključeni s področja uporabe akta o kibernetski odpornosti. Značilnosti namreč ponazarjajo uporabo na tveganju temelječega pristopa akta o kibernetski odpornosti, ki omogoča, da se skladnost dokaže na različne načine glede na značilnosti in omejitve izdelka z digitalnimi elementi, v skladu s členom 13(3) akta o kibernetski odpornosti. Te značilnosti so del predvidenega namena in okolja delovanja izdelka ter so zato pomembne pri ocenjevanju skladnosti z bistvenimi zahtevami glede kibernetske varnosti (v nadaljnjem besedilu: bistvene zahteve). Zlasti v uvodni izjavi 55 se izrecno priznava, da nekatere bistvene zahteve morda niso popolnoma združljive z naravo izdelka z digitalnimi elementi. To se lahko na primer zgodi, kadar bi skladnost ogrozila obvezne zahteve glede interoperabilnosti ali pravilno delovanje sistema.

32. Zato morajo proizvajalci obravnavati tveganja za kibernetsko varnost na podlagi ocene tveganja za kibernetsko varnost iz člena 13(2). V uvodni izjavi 55 je tudi pojasnjeno, da se v nekaterih primerih posamezne bistvene zahteve ne uporabljajo ali jih ni mogoče izpolniti z izvajanjem najsodobnejših varnostnih ukrepov, na primer

zaradi predvidenega namena sistema, zaradi katerega mora izdelek z digitalnimi elementi delovati v interakciji z obstoječimi odvisnostmi ali izpolnjevati določene zahteve glede interoperabilnosti. V takih primerih bi morali proizvajalci te posebne omejitve opredeliti in dokumentirati, oceniti povezana tveganja ter izvesti ustrezne alternativne ali kompenzacijske ukrepe za zmanjšanje tveganja, da se ne bi ogrozila varnost izdelka z digitalnimi elementi. Za te namene imajo tehnična dokumentacija iz člena 31 ter informacije in navodila za uporabnika iz Priloge II ključno vlogo pri preglednem opisovanju ugotovljenih omejitev, povezanih tveganj za kibernetsko varnost in izvedenih ukrepov za zmanjšanje tveganja. Proizvajalci bi morali v skladu z obveznostjo posodabljanja ocene tveganja v obdobju podpore tudi redno ponovno ocenjevati, ali te omejitve še obstajajo. Če je te omejitve mogoče sčasoma odpraviti ali zmanjšati, bi morali proizvajalci izdelek z digitalnimi elementi ustrezno posodobiti, da bi se lahko približal ustrezni ravni kibernetske varnosti ([10]).

Primer 10: proizvajalec da na trg izdelek z digitalnimi elementi, ki pri komunikaciji z zunanjimi sistemi uporablja omrežni protokol. Proizvajalec v okviru uporabe bistvenih zahtev na podlagi ocene tveganja za kibernetsko varnost ugotovi, da je za zagotovitev zaupnosti in celovitosti podatkov, ki jih izmenjuje izdelek z digitalnimi elementi, potrebna uporaba varnega komunikacijskega protokola.

Vendar njegov predvideni namen vključuje interoperabilnost z obstoječimi sistemi, ki podpirajo le starejši ali manj varen protokol. V takih primerih lahko proizvajalec ta protokol uporabi, kadar je to potrebno za doseganje interoperabilnosti, pod pogojem, da so povezana tveganja za kibernetsko varnost opredeljena in se zmanjšajo z drugimi sredstvi.

Kadar je tehnično izvedljivo, da izdelek z digitalnimi elementi podpira tako varni protokol kot manj varni protokol, se od proizvajalca pričakuje, da bo uporabil varni protokol in privzeto omogoči njegovo uporabo. Manj varni protokol bi bil dovoljen le, kadar je potreben zaradi interoperabilnosti.

Primer 11: proizvajalec sistema za industrijsko avtomatizacijo kupi nekaj mikrokrmilnikov, preden se akt o kibernetski odpornosti začne uporabljati. Proizvajalec opravi oceno tveganja za kibernetsko varnost za svoj sistem za industrijsko avtomatizacijo, ki naj bi bil dan na trg po začetku uporabe akta o kibernetski odpornosti. Na podlagi te ocene tveganja za kibernetsko varnost proizvajalec ne ugotovi posebnih tveganj za kibernetsko varnost, povezanih z uporabo enega od teh mikrokrmilnikov. Proizvajalec ga vgradi v svoj sistem za industrijsko avtomatizacijo in zagotovi, da izdelek z digitalnimi elementi kot celota (sistem industrijske avtomatizacije) izpolnjuje bistvene zahteve.

2.7 **Izdelki z digitalnimi elementi, zasnovani pred začetkom uporabe akta o kibernetski odpornosti**

33. V nekaterih primerih bo proizvajalec enote izdelka z digitalnimi elementi, izdelane v skladu s tipom ali modelom, zasnovanim in razvitim pred datumom začetka uporabe akta o kibernetski odpornosti, dal na trg po tem, ko se akt o kibernetski odpornosti začne uporabljati 11. decembra 2027. V teh primerih za skladnost s to uredbo ni nujno potrebno, da se navedene enote izdelka z digitalnimi elementi na novo zasnujejo. Proizvajalec mora opraviti oceno tveganja za kibernetsko varnost v skladu s členom 13(2) akta o kibernetski odpornosti, da na podlagi predvidenega namena in razumno predvidljive uporabe izdelka z digitalnimi elementi določi, katere od bistvenih zahtev iz dela I Priloge I se uporabljajo za navedeni izdelek z digitalnimi elementi in kako se navedene zahteve izvajajo.

34. Kadar rezultat navedene ocene tveganja pokaže, da izdelek z digitalnimi elementi že vključuje ustrezne in učinkovite varnostne ukrepe, s katerimi se obravnavajo zadevna tveganja, se lahko proizvajalec za dokazovanje skladnosti z aktom o kibernetski odpornosti opre na te obstoječe ukrepe. Akt o kibernetski odpornosti sam po sebi ne nalaga obveznosti uvedbe novih varnostnih značilnosti ali ponovne zasnove izdelka z digitalnimi elementi, kadar to ni potrebno za obravnavanje ugotovljenih tveganj.

([10]) Opozoriti je treba, da se lahko premisleki iz tega odstavka po potrebi uporabljajo za vse izdelke z digitalnimi elementi, ki spadajo na področje uporabe akta o kibernetski odpornosti, in ne le za „kompleksne sisteme“.

35. Kljub temu za proizvajalca še naprej veljajo obveznosti, določene v aktu o kibernetski odpornosti. Te vključujejo zagotovitev, da se je pred dajanjem izdelka z digitalnimi elementi na trg izvedel veljavni postopek ugotavljanja skladnosti ter da se je pripravila izjava EU o skladnosti in namestila oznaka CE. Skladnost s temi zahtevami ni odvisna od tega, ali je bilo treba zaradi ocene tveganja spremeniti zasnovo izdelka z digitalnimi elementi. Za izdelke z digitalnimi elementi, zasnovane pred datumom začetka uporabe akta o kibernetski odpornosti, vendar dane na trg po tem datumu, je treba v primerih, ko proizvajalec ne more dokazati, kako se je ocena tveganja upoštevala v fazi zasnove in razvoja izdelka z digitalnimi elementi, obveznost iz člena 13(2) razumeti tako, da se z njo od proizvajalcev zahteva, da opravijo oceno tveganja za kibernetsko varnost in na tej podlagi dokažejo, da izdelek z digitalnimi elementi vključuje ustrezne varnostne ukrepe za zmanjšanje tveganj za kibernetsko varnost, preprečevanje incidentov in zmanjšanje njihovega učinka, tudi v zvezi z zdravjem in varnostjo uporabnikov.

36. Zato bi se lahko izdelki z digitalnimi elementi, zasnovani pred začetkom uporabe akta o kibernetski odpornosti, dali na trg v skladu z aktom o kibernetski odpornosti, ne da bi bili na novo zasnovani, če lahko proizvajalec na podlagi ocene tveganja za kibernetsko varnost in tehnične dokumentacije dokaže, da izdelek z digitalnimi elementi glede na svoj predvideni namen in razumno predvidljivo uporabo dosega ustrezno raven kibernetske varnosti in je skladen z bistvenimi zahtevami glede kibernetske varnosti.

37. Poleg tega je koristno pojasniti uporabo obveznosti glede ugotavljanja skladnosti za proizvajalce izdelkov z digitalnimi elementi, ki so dajo na trg po začetku uporabe akta o kibernetski odpornosti, vendar so izdelani v skladu s tipom ali modelom, zasnovanim in razvitim pred tem datumom. V skladu s členom 13(12) mora proizvajalec z ustreznim postopkom ugotavljanja skladnosti dokazati, da je njegov izdelek z digitalnimi elementi skladen z veljavnimi bistvenimi zahtevami, in dokaze o tem vključiti v tehnično dokumentacijo izdelka (točka 6 Priloge VII).

38. Vendar je treba uporabo takih zahtev razlagati glede na oceno tveganja za kibernetsko varnost in profil tveganja za kibernetsko varnost izdelka z digitalnimi elementi. Zlasti pri izdelkih z digitalnimi elementi, zasnovanih pred datumom začetka uporabe akta o kibernetski odpornosti (vendar danih na trg po tem datumu), za katere se uporabljajo postopki ugotavljanja skladnosti iz člena 32(1), se obveznosti predložitve dokazov v okviru postopka ugotavljanja skladnosti, kadar ocena tveganja pokaže, da izdelek z digitalnimi elementi že vključuje ustrezne in učinkovite varnostne ukrepe za obravnavanje tveganj tega izdelka, ne bi smelo razumeti tako, da se od proizvajalca zahteva predložitev rezultatov preskušanj, ki zajemajo prvotne faze zasnove in razvoja takih izdelkov z digitalnimi elementi. To ne bi bilo potrebno, saj ne bi prispevalo k večji varnosti samega izdelka z digitalnimi elementi. Kadar so preskušanja kljub temu potrebna, se od proizvajalcev ne pričakuje, da bodo predložili dokaze o preskušanjih, izvedenih na vseh različicah izdelka, temveč lahko preskušanja združijo po družinah izdelkov z digitalnimi elementi, kot je podrobneje obravnavano v oddelku *7.4 Reuse of risk assessments and conformity documentation for families of products with digital elements*.

39. Vendar bi moral proizvajalec predložiti dokaze o tem, kako zagotavlja skladnost s postopki obravnavanja ranljivosti iz dela II Priloge I, posodabljati svojo oceno tveganja v skladu s členom 13(3) ter izpolnjevati vse druge obveznosti, določene v aktu o kibernetski odpornosti, tudi z zagotavljanjem informacij in navodil uporabnikom v skladu s členom 13(18).

Primer 12: proizvajalec da na trg mikrokrmilnik, ki je bil zasnovan in razvit pred datumom začetka uporabe akta o kibernetski odpornosti. Mikrokrmilnik je namenjen vgradnji v vrsto elektronskih izdelkov z digitalnimi elementi, vključno z izdelki z digitalnimi elementi s funkcionalnostmi povezljivosti.

Preden da proizvajalec po začetku uporabe akta o kibernetski odpornosti na trg nove enote mikrokrmilnika, opravi oceno tveganja za kibernetsko varnost v skladu s členom 13(2). Proizvajalec na podlagi predvidenega namena mikrokrmilnika in njegove razumno predvidljive uporabe opredeli zadevna tveganja za kibernetsko varnost, kot so nepooblaščen dostop, manipulacija s programsko opremo ali podatki ter zloraba razpoložljivih vmesnikov.

Rezultat ocene tveganja pokaže, da mikrokrmilnik, kot je bil prvotno zasnovan, že vključuje ustrezne in učinkovite varnostne ukrepe za obravnavanje ugotovljenih tveganj. Proizvajalec torej ugotovi, da izdelek z digitalnimi elementi izpolnjuje ustrezne bistvene zahteve iz dela I Priloge I in da ponovna zasnova ali uvedba dodatnih varnostnih funkcionalnosti ni potrebna.

Kadar ni mogoče dokazati, kako se je ocena tveganja za kibernetsko varnost upoštevala v prvotni fazi zasnove in razvoja, proizvajalec dokumentira trenutno oceno tveganja za kibernetsko varnost ter pojasni, kako obstoječa zasnova in ukrepi zmanjšujejo ugotovljena tveganja. Proizvajalcu ni treba ponovno ustvariti pretekle dokumentacije o zasnovi ali preskušanju, saj to ne bi prispevalo k izboljšanju kibernetske varnosti izdelka z digitalnimi elementi. Kadar več različic mikrokrmilnika temelji na isti zasnovi in ima enak profil tveganja za kibernetsko varnost, se lahko proizvajalec opre tudi na reprezentativne dokaze, ki zajemajo zadevno družino izdelkov.

Proizvajalec zagotovi tudi skladnost z zahtevami glede obravnavanja ranljivosti, določenimi v delu II Priloge I, med drugim z vzdrževanjem postopkov za obravnavanje in odpravljanje ranljivosti ter z rednim pregledovanjem ocene tveganja za kibernetsko varnost v skladu s členom 13(3).

V teh okoliščinah se lahko mikrokrmilnik, zasnovan pred datumom začetka uporabe akta o kibernetski odpornosti, da na trg, ne da bi bil ponovno zasnovan, če lahko proizvajalec na podlagi ocene tveganja za kibernetsko varnost in tehnične dokumentacije dokaže, da glede na predvideni namen in razumno predvidljivo uporabo dosega ustrezno raven kibernetske varnosti in je skladen z veljavnimi bistvenimi zahtevami.

3. **PROSTA IN ODPRTOKODNA PROGRAMSKA OPREMA**

40. Kot je bilo opozorjeno v oddelku *2.1 Placing on the market*, se akt o kibernetski odpornosti uporablja za izdelke z digitalnimi elementi, ki so v okviru gospodarske dejavnosti prvič dostopni na trgu EU (tj. „dani na trg“), pa tudi za vsak nadaljnji primer, ki pomeni omogočanje dostopnosti istega izdelka z digitalnimi elementi na trgu. V Modrem vodniku (oddelek 2.2) je pojasnjeno, da je treba „gospodarsko dejavnost“ razumeti kot zagotavljanje blaga v okviru gospodarske dejavnosti, bodisi plačljivo bodisi brezplačno, ter da se lahko oceni le za vsak primer posebej ob upoštevanju rednosti dobav, značilnosti proizvoda, namenov dobavitelja itd.

41. Za dobavo v okviru gospodarske dejavnosti je značilna vrsta okoliščin, ki so obširno dokumentirane v Modrem vodniku in navedene v uvodni izjavi 15 akta o kibernetski odpornosti. Vključujejo lahko neposredno zaračunavanje cene in tudi „zaračunavanje cene za storitve tehnične podpore, kadar to ne služi le povrnitvi dejanskih stroškov, z namero monetizacije, na primer z zagotavljanjem platforme programske opreme, prek katere proizvajalec monetizira druge storitve, tako da kot pogoj za uporabo zahteva obdelavo osebnih podatkov za druge namene kot izključno za izboljšanje varnosti, združljivosti ali interoperabilnosti programske opreme, ali da sprejema donacije, ki presegajo stroške, povezane z zasnovo, razvojem in zagotavljanjem izdelka z digitalnimi elementi“. (uvodna izjava 15) ([11]).

42. Vendar akt o kibernetski odpornosti priznava posebnosti različnih načinov razvoja in izdajanja „proste in odprtokodne programske opreme“ ter vsebuje nekatere usmeritve za pomoč pri ugotavljanju, ali je prosta in odprtokodna programska oprema izdelek z digitalnimi elementi, dan na trg (tj. v okviru gospodarske dejavnosti), v smislu akta o kibernetski odpornosti. Kot je pojasnjeno v uvodni izjavi 18, se „pri določanju komercialne ali nekomercialne narave te dejavnosti […] ne bi smele upoštevati zgolj okoliščine, v katerih je bil izdelek z digitalnimi elementi razvit, ali način financiranja razvoja“. Natančneje, „da se zagotovi jasno razlikovanje med razvojno fazo in fazo dobave, zagotavljanje izdelkov z digitalnimi elementi, ki štejejo za prosto in odprtokodno programsko opremo, ki jih njihovi proizvajalci ne monetizirajo, ne bi smelo šteti za komercialno dejavnost“.

([11]) Opozoriti je treba tudi, da čeprav se izdelki z digitalnimi elementi pogosto monetizirajo (tudi) z obdelavo osebnih podatkov, je varstvo osebnih podatkov temeljna pravica, zato osebnih podatkov ni mogoče šteti za blago, kot je navedeno v uvodni izjavi 24 Direktive (EU) 2019/770 Evropskega parlamenta in Sveta z dne 20. maja 2019 o nekaterih vidikih pogodb o dobavi digitalne vsebine in digitalnih storitev (UL L 136, 22.5.2019, str. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Zato je koristno (i) pojasniti, kaj je prosta in odprtokodna programska oprema; (ii) kdaj se šteje, da je zanjo odgovorna fizična ali pravna oseba, in (iii) navesti primere, ki deležnikom pomagajo razumeti, kdaj distribucija proste in odprtokodne programske opreme pomeni dajanje na trg. Kadar prosta in odprtokodna programska oprema ni dana na trg, ne spada na področje uporabe akta o kibernetski odpornosti, razen če je subjekt, ki jo izdaja, pravna oseba, ki ustreza opredelitvi „upravljavca odprtokodne programske opreme“ (v nadaljnjem besedilu: upravljavec) iz člena 3(14). V tem primeru zanjo veljajo samo obveznosti iz člena 24.

44. Člen 3(48) prosto in odprtokodno programsko opremo opredeljuje kot „programsko opremo, katere izvorna koda se odprto deli in ki je na voljo na podlagi proste in odprtokodne licence, ki zagotavlja vse pravice, da postane prosto dostopna, uporabna, jo je mogoče spremeniti in prerazporediti“. Čeprav v teh usmeritvah niso navedene konkretne proste in odprtokodne licence, ki so združljive z opredelitvijo iz člena 3(48), iz besedila te določbe izhaja, da se za prosto in odprtokodno programsko opremo za namene akta o kibernetski odpornosti šteje samo programska oprema, ki kumulativno izpolnjuje dva pogoja: (i) programska oprema mora biti na voljo na podlagi proste in odprtokodne licence, ki podeljuje celoten sklop pravic iz člena 3(48), in (ii) njena izvorna koda se mora odprto deliti.

45. Zahteva, da licenca omogoča, da je programska oprema „prosto dostopna, uporabna, jo je mogoče spremeniti in prerazporediti“, odraža tradicionalno razumevanje proste in odprtokodne programske opreme, in sicer da morajo imeti uporabniki možnost dostopa do izvorne kode, njene uporabe brez neupravičenih omejitev, njenega spreminjanja in prerazporejanja izvirnih ali spremenjenih različic. Dostop do izvorne kode je zato nujen pogoj za uveljavljanje drugih pravic: brez dostopa do izvorne kode programske opreme v praksi ni mogoče spreminjati ali smiselno ponovno uporabiti.

46. Vendar člen 3(48) presega zgolj sklicevanje na licenčne pogoje, saj izrecno zahteva, da se izvorna koda „odprto deli“. Pojem „odprto deli“ pomeni, da mora biti izvorna koda javno dostopna (bodisi višje v verigi ali nižje v verigi) in ne zgolj zagotovljena na omejeni ali pogojni podlagi. Zato se programska oprema, distribuirana na podlagi proste in odprtokodne licence, katere izvorna koda pa se deli (ali jo je dovoljeno deliti) samo s plačljivimi uporabniki ali omejeno skupino uporabnikov, ne šteje za prosto in odprtokodno programsko opremo v smislu člena 3(48). Za namene akta o kibernetski odpornosti bi se zato samo za prosto in odprtokodno programsko opremo morala šteti samo programska oprema, katere izvorna koda je javno dostopna in za katero je bila izdana prosta in odprtokodna licenca, ki podeljuje celoten sklop pravic iz člena 3(48).

3.1 **Ugotavljanje, ali je prosta in odprtokodna programska oprema pod odgovornostjo določene osebe**

47. Akt o kibernetski odpornosti gospodarskim subjektom, ki dobavljajo izdelke z digitalnimi elementi na trg EU, nalaga ključne odgovornosti. Proizvajalca opredeljuje kot fizično ali pravno osebo, ki izdelek z digitalnimi elementi dobavlja pod svojim imenom ali znamko in to počne v okviru gospodarske dejavnosti (torej ga da na trg). Podobno je uvoznik fizična ali pravna oseba s sedežem v EU, ki dobavlja izdelek z digitalnimi elementi osebe s sedežem zunaj EU in to počne v okviru gospodarske dejavnosti (torej ga da na trg). Obveznosti upravljavcev veljajo za pravno osebo, ki dobavlja prosto in odprtokodno programsko opremo, namenjeno gospodarskim dejavnostim ([12]), vendar je ne daje na trg v smislu akta o kibernetski odpornosti.

48. Zato je treba za ugotovitev, ali fizična ali pravna oseba daje prosto in odprtokodno programsko opremo na trg EU, najprej pojasniti, ali ta fizična ali pravna oseba prosto in odprtokodno programsko opremo dejansko dobavlja. Da bi se pravilno določile veljavne obveznosti na podlagi akta o kibernetski odpornosti, je bistveno ugotoviti, ali fizična ali pravna oseba dejansko izvaja dejanje dobave proste in odprtokodne programske opreme. Kot je namreč opozorjeno v uvodni izjavi 18, se akt o kibernetski odpornosti ne uporablja za fizične ali pravne osebe, ki z izvorno kodo prispevajo k izdelkom z digitalnimi elementi, ki se štejejo za prosto in odprtokodno programsko opremo, za katere niso odgovorne.

([12]) To je nujen, vendar ne zadosten pogoj, da se pravna oseba šteje za upravljavca odprtokodne programske opreme, saj opredelitev iz člena 3(14) določa dodatne pogoje, da se pravna oseba šteje za upravljavca.

49. Glede na posebnosti razvoja proste in odprtokodne programske opreme, ki pogosto vključuje več prispevajočih oseb, decentralizirane modele sodelovanja in ločevanje med prispevanjem in odločanjem, je koristno pojasniti, da se šteje, da je prosta in odprtokodna programska oprema „pod odgovornostjo“ fizičnih ali pravnih oseb, ki jo izdajajo in izvajajo primarni nadzor nad njenim razvojem, izdajami in odločitvami o distribuciji (te osebe se pogosto imenujejo „vzdrževalci“). Osebe, ki prispevajo izvorno kodo, vendar nimajo nadzora nad izdajami, časovnimi načrti ali odločitvami o upravljanju, se štejejo za „prispevajoče osebe“; v takih primerih prosta in odprtokodna programska oprema ni pod njihovo odgovornostjo, čeprav so zanjo prispevale kodo. Sam obstoj tehničnih dovoljenj, kot je dostop za potrjevanje sprememb, ne zadostuje za ugotovitev, da je prosta in odprtokodna programska oprema pod odgovornostjo določene osebe; odgovornost nosijo tisti, ki prosto in odprtokodno programsko opremo izdajajo in nadzorujejo.

Primer 13: razvijalec posameznik ali zaposlena oseba v družbi v projekt proste in odprtokodne programske opreme predloži zahtevo za vlečenje („pull“) ali zahtevo za združitev („merge“), ki vsebuje varnostni popravek ali novo funkcijo. Vzdrževalci projekta kodo pregledajo, sprejmejo in dodajo v glavni repozitorij ter jo nato vključijo v novo izdajo. V tem scenariju je oseba, ki je predložila zahtevo za vlečenje, „prispevajoča oseba“ in se zanjo akt o kibernetski odpornosti ne uporablja. Čeprav je ta oseba prispevala izvorno kodo, ne izvaja primarnega nadzora nad razvojem, izdajami ali odločitvami o distribuciji.

3.2 **Ugotavljanje, ali je prosta in odprtokodna programska oprema dana na trg EU**

50. Ko se ugotovi, da je prosta in odprtokodna programska oprema pod odgovornostjo fizične ali pravne osebe, je treba ugotoviti, ali jo ta oseba dobavlja v okviru gospodarske dejavnosti, kar pomeni dajanje na trg.

3.2.1 *Zaračunavanje cene*

51. Kadar fizična ali pravna oseba, ki dobavlja prosto in odprtokodno programsko opremo, zaračuna ceno za samo programsko opremo (npr. z zaračunavanjem cene za vnaprej prevedene dvojiške datoteke), se zanjo šteje, da daje izdelek z digitalnimi elementi na trg. Oseba, ki daje prosto in odprtokodno programsko opremo na trg, je zato v skladu z aktom o kibernetski odpornosti proizvajalec.

52. Proizvajalci proste in odprtokodne programske opreme pogosto brezplačno dobavljajo različice te programske opreme (velikokrat imenovane „skupnostne“ različice), katerih kodna baza je (skoraj) enaka plačljivi različici. Vendar so ti izdelki z digitalnimi elementi različni izdelki: plačljiva različica se na nek način monetizira (npr. z zaračunavanjem cene ali na druge načine, kot je obravnavano v tem oddelku) in se zato šteje za dano na trg, s čimer nastanejo obveznosti proizvajalca. Različica, ki se zagotavlja brezplačno (ali skupnostna različica), se ne monetizira in se zato za namene akta o kibernetski odpornosti ne šteje za dano na trg. To velja tudi, kadar je plačljiva različica „izboljšana“ komercialna različica, ki razširja kodno bazo različice, ki je na voljo brezplačno, ali to različico vključuje v širši izdelek z digitalnimi elementi (npr. kot pri modelu „odprto jedro“).

53. Če je oseba, ki dobavlja skupnostno različico, pravna oseba, zanjo veljajo tudi obveznosti upravljavcev za različico, ki jo dobavlja brezplačno (skupnostno različico). Če je subjekt fizična oseba, različica, ki se zagotavlja brezplačno (skupnostna različica), ne spada na področje uporabe akta o kibernetski odpornosti.

3.2.2 *Monetizacija drugih storitev ali zahteva po obdelavi osebnih podatkov*

54. Fizična ali pravna oseba, ki izdaja prosto in odprtokodno programsko opremo, jo lahko tudi daje na trg (tj. jo dobavlja v okviru gospodarske dejavnosti), kadar zagotavlja programsko opremo, prek katere monetizira druge izdelke z digitalnimi elementi ali storitve, ali kadar kot pogoj za uporabo zahteva obdelavo osebnih podatkov za druge namene kot izključno za izboljšanje varnosti, združljivosti ali interoperabilnosti programske opreme.

Primer 14: fizična ali pravna oseba izda prosto in odprtokodno aplikacijo za spletno tržnico. Aplikacija je na voljo brezplačno in uporabnikom omogoča, da prek nje kupujejo blago ali storitve. Aplikacija osebi, ki jo je izdala, omogoča, da monetizira druge izdelke z digitalnimi elementi in storitve, ki se ponujajo prek nje (npr. z oglasi, provizijami ali naročninami). Zato se šteje, da je aplikacija dana na trg v okviru gospodarske dejavnosti.

Primer 15: fizična ali pravna oseba izda prosto in odprtokodno VPN. Aplikacija je na voljo brezplačno, vendar uporabnikom omogoča plačljivi dostop do dodatnih strežnikov ali namenskih naslovov IP. Ta aplikacija tej osebi omogoča, da monetizira druge storitve, ki se ponujajo prek nje, zato se šteje za dano na trg v okviru gospodarske dejavnosti.

Primer 16: fizična ali pravna oseba izda prosto in odprtokodno aplikacijo za spremljanje telesne pripravljenosti. Aplikacija je na voljo brezplačno, vendar je njena uporaba pogojena z obdelavo osebnih podatkov uporabnikov za namene, kot sta ciljano oglaševanje in analitika, ki niso povezani z varnostjo, združljivostjo ali interoperabilnostjo programske opreme. Ker se taka obdelava podatkov zahteva kot pogoj za uporabo, se aplikacija šteje za dano na trg v okviru gospodarske dejavnosti.

3.2.3 *Podporne storitve*

55. Zgolj dejstvo, da fizična ali pravna oseba, ki izda prosto in odprtokodno programsko opremo, ponuja tudi plačljive podporne storitve, povezane z njo, samo po sebi ne pomeni, da se izdelek z digitalnimi elementi dobavlja v okviru gospodarske dejavnosti. Podporne storitve lahko vključujejo dejavnosti, kot so svetovanje, usposabljanje ali strokovne storitve v zvezi z uporabo, dokumentacijo, konfiguracijo in uvedbo programske opreme pri stranki.

56. Odločilni dejavnik je, ali je dostop do same proste in odprtokodne programske opreme (tj. zagotavljanje izdelka z digitalnimi elementi), vključno z njenim vzdrževanjem, pogojen s plačilom, in ni zgolj ponujanje strokovnih storitev v zvezi s prosto dostopnim izdelkom z digitalnimi elementi, kot je navedeno v uvodni izjavi 18 akta o kibernetski odpornosti („zagotavljanje izdelkov z digitalnimi elementi, ki štejejo za prosto in odprtokodno programsko opremo, ki jih njihovi proizvajalci ne monetizirajo, [se] ne bi smelo šteti za komercialno dejavnost“). Kadar je prosto in odprtokodno programsko opremo mogoče prosto prenesti in namestiti, uporabniki pa se lahko neobvezno odločijo za ločen nakup strokovnih storitev, se ta prosta in odprtokodna programska oprema ne šteje za dano na trg.

57. Nasprotno pa je v nekaterih primerih dostop do določene različice izdelka z digitalnimi elementi, vključno z nekaterimi ugodnostmi, kot sta tehnična pomoč ali optimizacija delovanja, pogojen s plačilom. V teh primerih to zagotavljanje pomeni monetizirano zagotavljanje izdelka z digitalnimi elementi, ki se dobavlja v okviru gospodarske dejavnosti, in se zato šteje za dajanje na trg. To vključuje primere, kadar je plačljiva izdaja ali različica za podjetja na voljo na podlagi poslovnega sporazuma, ne glede na to, ali je funkcionalno enakovredna programska oprema na voljo tudi brezplačno na podlagi proste in odprtokodne licence.

Primer 17: fizična ali pravna oseba izda prost in odprtokoden operacijski sistem ter ponuja njegovo plačljivo različico, ki vključuje podporne storitve, kot sta tehnična pomoč ali optimizacija delovanja. Plačljiva različica operacijskega sistema se šteje za dano na trg v okviru gospodarske dejavnosti.

Primer 18: fizična ali pravna oseba izda prosto in odprtokodno ukaznovrstično orodje. Orodje je prosto dostopno, prenese in namesti ga lahko vsakdo. Ta fizična ali pravna oseba ločeno ponuja strokovne storitve, kot so neobvezne storitve svetovanja, v okviru katerih usposablja uporabnike in jim pomaga pri nameščanju in uporabi orodja. Ta prosta in odprtokodna programska oprema se ne šteje za dano na trg v smislu akta o kibernetski odpornosti.

58. Zlasti v primeru fizičnih oseb, ki izdajajo prosto in odprtokodno programsko opremo, se neposredno zagotavljanje tehnične pomoči skupaj z dostopom do izdelka z digitalnimi elementi še vedno ne bi štelo za gospodarsko dejavnost, če zaračunavanje cene, kot je navedeno v uvodni izjavi 15 akta o kibernetski odpornosti, služi le povrnitvi dejanskih stroškov. Taki dejanski stroški vključujejo različne stroške, povezane z zasnovo, razvojem in vzdrževanjem zadevne programske opreme, vključno z razumnimi življenjskimi stroški osebe. Zato se za fizično osebo, ki izdaja prosto in odprtokodno programsko opremo ter ponuja tehnično pomoč, da pokrije svoje stroške in pridobi pravično plačilo, zgolj na tej podlagi ne šteje, da daje to programsko opremo na trg EU.

59. Za fizično ali pravno osebo, ki zagotavlja tehnično pomoč v zvezi s prosto in odprtokodno programsko opremo, ki ni pod njeno odgovornostjo, se ne šteje, da daje to programsko opremo na trg, razen če ta oseba v skladu s členom 22 v okviru zagotavljanja take pomoči bistveno spremeni prosto in odprtokodno programsko opremo.

Primer 19: ponudnik storitev ne izda proste in odprtokodne programske opreme, temveč stranki pomaga pri njeni namestitvi na strežnik na lokaciji stranke. To stori, ne da bi bistveno spremenil to prosto in odprtokodno programsko opremo. Zato se za ponudnika storitev ne šteje, da daje prosto in odprtokodno programsko opremo na trg.

3.2.4 *Donacije*

60. Fizične ali pravne osebe, ki objavljajo projekte proste in odprtokodne programske opreme, vanje običajno vključijo načine, na katere lahko uporabniki te programske opreme prostovoljno donirajo denar, da se zahvalijo izdajatelju oziroma izdajateljem projekta in tudi zagotovijo, da se projekt še naprej aktivno vzdržuje.

61. Kot je navedeno v uvodni izjavi 15 akta o kibernetski odpornosti, se „sprejemanje donacij brez namena ustvarjanja dobička […] ne bi smelo šteti za gospodarsko dejavnost“. Zgolj vključitev povezave do platforme za donacije ali podobnih orodij za zbiranje donacij se ne bi smela šteti za namen ustvarjanja dobička, tudi kadar znesek, zbran z donacijami, presega zgolj stroške, povezane z zasnovo, razvojem in zagotavljanjem izdelka z digitalnimi elementi. To vključuje razumno nadomestilo za prispevajoče osebe, ki jih zaposli pravna oseba, in/ali razumne življenjske stroške fizične osebe. Donacije se po svoji naravi s časom spreminjajo, zato je treba pri ocenjevanju, ali se prosta in odprtokodna programska oprema, ki se monetizira izključno z donacijami, šteje za dano na trg, dopustiti določeno mero prožnosti. Za prosto in odprtokodno programsko opremo, ki se podpira samo z donacijami, zato ni verjetno, da bi se štela za dano na trg v smislu akta o kibernetski odpornosti.

Primer 20: fizična ali pravna oseba izda orodje proste in odprtokodne programske opreme v javnem spletnem repozitoriju, s čimer vsakomur omogoči, da ga prenese, uporablja, spreminja in ponovno distribuira na podlagi proste in odprtokodne licence. Izdajatelj pozove uporabnike, naj prek platforme za donacije namenijo prostovoljne donacije za podporo nadaljnjemu razvoju in vzdrževanju projekta. Dostop do programske opreme, njene izvorne kode in njenih posodobitev ni pogojen z donacijo. Ta prosta in odprtokodna programska oprema se ne šteje za dobavljeno v okviru gospodarske dejavnosti in se ne šteje za dano na trg v smislu akta o kibernetski odpornosti.

62. Kljub temu obstajajo primeri, ko se lahko prosta in odprtokodna programska oprema, podprta z donacijami, šteje za dano na trg. To velja, kadar so na podlagi celovite ocene okoliščin donacije dejansko enakovredne zaračunavanju cene za dostop do izdelka z digitalnimi elementi ali nekaterih njegovih funkcij. To lahko velja zlasti, kadar je dostop do proste in odprtokodne programske opreme, ključnih funkcij ali posodobitev v praksi pogojen z donacijo ali kadar so donacije povezane s pogodbenimi koristmi ali ekskluzivnimi ugodnostmi, ki presegajo ugodnosti skupnosti.

Primer 21: fizična ali pravna oseba izda programski izdelek z digitalnimi elementi na podlagi proste in odprtokodne licence, vendar prenos izdaj in varnostne posodobitve zagotavlja samo uporabnikom, ki donirajo. Uporabniki, ki ne donirajo, nimajo dostopa do trenutne različice programske opreme.

V tem primeru so donacije dejansko pogoj za dostop do izdelka z digitalnimi elementi in zato pomenijo zaračunavanje cene. Ta prosta in odprtokodna programska oprema se zato šteje za dano na trg v smislu akta o kibernetski odpornosti.

Primer 22: fizična ali pravna oseba javno objavi izvorno kodo proste in odprtokodne programske opreme, vendar vnaprej prevedene dvojniške datoteke, redne posodobitve in zajamčene varnostne popravke zagotavlja samo donatorjem. V tem primeru so donacije povezane z dostopom do bistvenih vidikov izdelka z digitalnimi elementi in pomenijo plačilo za dobavo tega izdelka. Ta prosta in odprtokodna programska oprema se zato šteje za dano na trg v okviru gospodarske dejavnosti.

3.2.5 *Financiranje proste in odprtokodne programske opreme*

63. Samo dejstvo, da je tretja oseba plačala, sponzorirala ali drugače financirala razvoj proste in odprtokodne programske opreme, ne določa, ali je ta programska oprema dana na trg. V ekosistemu proste in odprtokodne programske opreme je običajna praksa, da posamezni razvijalci, fundacije ali skupnosti prejemajo finančna sredstva od družb, javnih organov ali drugih sponzorjev, da razvijajo posebne funkcije, odpravljajo napake ali vzdržujejo kritične sestavne dele. To financiranje je lahko številnih oblik, vključno z nepovratnimi sredstvi, nagradami za prijavljanje ranljivosti, sponzorstvi, pogodbami o storitvah ali plačanim razvojnim delom.

64. Kot je bilo že opozorjeno, je v uvodni izjavi 18 akta o kibernetski odpornosti pojasnjeno, da se pri določanju komercialne ali nekomercialne narave te dejavnosti ne bi smele upoštevati zgolj okoliščine, v katerih je bil izdelek z digitalnimi elementi razvit, ali način financiranja razvoja.

65. Kadar se torej prosta in odprtokodna programska oprema odprto deli in je vsem prosto na voljo za dostop, uporabo, spreminjanje in ponovno distribucijo, se dejstva, da je gospodarski subjekt morda plačal za navedeni projekt, ne bi smelo upoštevati pri ugotavljanju, ali je programska oprema dana na trg. Če se ta prosta in odprtokodna programska oprema namreč ne monetizira drugače, se ne šteje za dano na trg. Kadar družba, ki je financirala razvoj proste in odprtokodne programske opreme (pa tudi katera koli druga družba), to programsko opremo vgradi v svoj izdelek z digitalnimi elementi, mora biti pri tem primerno skrbna v skladu s členom 13(5) akta o kibernetski odpornosti.

Primer 23: razvijalec posameznik objavi projekt proste in odprtokodne programske opreme in ga aktivno vzdržuje. Proizvajalec A od razvijalca posameznika zahteva, da tej prosti in odprtokodni programski opremi doda posebno funkcijo, in financira razvoj te funkcije. Razvijalec funkcijo doda kodni bazi proste in odprtokodne programske opreme, jo odprto deli in vsem prosto omogoči dostop do nje, njeno uporabo, spreminjanje in ponovno distribucijo. Ne šteje se, da je razvijalec posameznik to prosto in odprtokodno programsko opremo dal na trg. Če proizvajalec prosto in odprtokodno programsko opremo vgradi v svoj izdelek z digitalnimi elementi, mora biti v skladu s členom 13(5) pri tem primerno skrben.

3.2.6 *Neprofitni subjekti, ustanovljeni za doseganje neprofitnih ciljev*

66. Kadar je pravna oseba, ki izda prosto in odprtokodno programsko opremo, neprofitna organizacija, „ustanovljena na način, ki zagotavlja, da se vsi prihodki po stroških uporabijo za doseganje neprofitnih ciljev“ (uvodna izjava 18 akta o kibernetski odpornosti), se prosta in odprtokodna programska oprema, ki jo je izdala, ne šteje za dano na trg. Kadar ta pravna oseba ustreza opredelitvi pojma „upravljavec“, zanjo veljajo ustrezne obveznosti (člen 24 akta o kibernetski odpornosti).

Primer 24: pravna oseba izda prosti in odprtokodni brskalnik, ki se neposredno monetizira prek partnerstev z iskalniki, vendar se vsi njegovi prihodki po stroških uporabijo za neprofitne cilje. Brskalnik se ne šteje za dan na trg v smislu akta o kibernetski odpornosti. Za pravno osebo, ki ga izda, veljajo obveznosti, ki se uporabljajo za upravljavce.

3.2.7 *Vgradnja s strani drugih proizvajalcev*

67. V nekaterih primerih prosto in odprtokodno programsko opremo izda jasno določljiva fizična ali pravna oseba, vendar je ta programska oprema „namenjen[a] temu, da [jo] drugi proizvajalci vključijo v svoje izdelke z digitalnimi elementi“. V takih primerih se ta prosta in odprtokodna programska oprema ne šteje za dano na trg EU, razen če jo oseba, ki jo je izdala (tj. prvotni proizvajalec), tudi monetizira v skladu s prejšnjimi oddelki teh usmeritev.

68. Kadar ta prosta in odprtokodna programska oprema ni dana na trg, bi za pravno osebo, ki jo izda, veljale obveznosti upravljavcev, če ta oseba trajno zagotavlja podporo v skladu z opredelitvijo pojma „upravljavec“.

Primer 25: pravna oseba izda knjižnico proste in odprtokodne programske opreme za izdelavo uporabniških vmesnikov. Dobave te knjižnice ne monetizira, temveč knjižnico vgradi v enega od svojih izdelkov z digitalnimi elementi (ki se da na trg). Knjižnica se ne šteje za dano na trg v smislu akta o kibernetski odpornosti, vendar je namenjena vgradnji v izdelke z digitalnimi elementi. Pravna oseba, ki jo izda, je njen upravljavec.

Primer 26: pravna oseba da na trg operacijski sistem in izda tudi knjižnice proste in odprtokodne programske opreme, ki uporabnikom tega operacijskega sistema služijo kot referenčne izvedbe. Pravna oseba ne monetizira knjižnic proste in odprtokodne programske opreme, ki so namenjene vgradnji v druge izdelke z digitalnimi elementi. Pravna oseba, ki jih izda, je upravljavec teh knjižnic proste in odprtokodne programske opreme.

3.3 **Upravljavci odprtokodne programske opreme**

69. Akt o kibernetski odpornosti zaradi „pomena, ki ga imajo za kibernetsko varnost številni izdelki z digitalnimi elementi, ki štejejo za prosto in odprtokodno programsko opremo in ki se izdajo, vendar niso dostopni na trgu v smislu [akta o kibernetski odpornosti]“ (uvodna izjava 19 akta o kibernetski odpornosti) uvaja novo pravno kategorijo „upravljavca odprtokodne programske opreme“.

70. V nekaterih primerih prosto in odprtokodno programsko opremo izda, vendar ne omogoči njene dostopnosti na trgu v smislu akta o kibernetski odpornosti, pravna oseba, katere „namen ali cilj je sistematično in trajno zagotavljati podporo za razvoj [proste in odprtokodne programske opreme] […], [namenjen[e] komercialnim dejavnostim, in ki zagotavlja sposobnost preživetja teh izdelkov“ (člen 3(14) akta o kibernetski odpornosti). V teh primerih za navedeno pravno osebo veljajo obveznosti upravljavcev.

71. Upravljavec je opredeljen kot „pravna oseba, ki ni proizvajalec“, saj je proizvajalec po opredelitvi fizična ali pravna oseba, ki daje izdelke z digitalnimi elementi na trg („jih trži“) pod svojim imenom ali znamko. Pravna oseba je lahko upravljavec samo tistih izdelkov z digitalnimi elementi, ki se štejejo za prosto in odprtokodno programsko opremo ter so izdani, vendar niso dostopni na trgu v smislu akta o kibernetski odpornosti. Pojem upravljavca se zato uporablja za konkretne primerke proste in odprtokodne programske opreme, ki so „na koncu namenjeni komercialnim dejavnostim, kot je vključevanje v komercialne storitve ali v monetizirane izdelke z digitalnimi elementi“ (uvodna izjava 19 akta o kibernetski odpornosti ([13])), vendar niso dostopni na trgu v smislu akta o kibernetski odpornosti in za katere pravna oseba, ki izda zadevno prosto in odprtokodno programsko opremo, zagotavlja sistematično podporo.

72. To, da je pravna oseba upravljavec določene proste in odprtokodne programske opreme, ne pomeni nujno, da je tudi upravljavec druge proste in odprtokodne programske opreme, ki jo izda. Podobno to, da je pravna oseba proizvajalec določene proste in odprtokodne programske opreme, ne pomeni, da ne more biti upravljavec druge proste in odprtokodne programske opreme. To vključuje zagotavljanje „skupnostnih“ različic iste proste in odprtokodne programske opreme, kot je opisano v oddelku *3.2.1 Charging a price*.

73. Pravna oseba je zato lahko hkrati upravljavec določene proste in odprtokodne programske opreme (kadar upravljavec sistematično in trajno zagotavlja podporo ter sposobnost preživetja programske opreme) in proizvajalec druge določene proste in odprtokodne programske opreme (kadar jo daje na trg). Povedano drugače, od istega pravnega subjekta se lahko zahteva, da ima različne vloge za različne projekte proste in odprtokodne programske opreme.

74. Pravna oseba bo morala za vsako določeno prosto in odprtokodno programsko opremo, ki jo izda, ugotoviti, ali se šteje, da je ta prosta in odprtokodna programska oprema dana na trg v smislu akta o kibernetski odpornosti. Če je tako, je pravna oseba proizvajalec programske opreme. Če se ne šteje, da je prosta in odprtokodna programska oprema dana na trg, je lahko pravna oseba njen upravljavec, če je programska oprema namenjena komercialnim dejavnostim in če pravna oseba zanjo zagotavlja podporo v skladu z opredelitvijo upravljavca ([14]).

3.3.1 *Trajna podpora in zagotavljanje sposobnosti preživetja proste in odprtokodne programske opreme*

75. V uvodni izjavi 19 je pojasnjeno, da lahko zagotavljanje trajne podpore razvoju izdelka z digitalnimi elementi med drugim vključuje: (i) gostovanje in upravljanje platform za sodelovanje pri razvoju programske opreme; (ii) gostovanje izvorne kode ali programske opreme; (iii) urejanje ali upravljanje izdelkov z digitalnimi elementi, ki štejejo za prosto in odprtokodno programsko opremo, ter (iv) usmerjanje razvoja takih izdelkov z digitalnimi elementi.

76. To lahko na primer velja za pravni subjekt, ki razvija prosto in odprtokodno programsko opremo za vključitev v svoje izdelke z digitalnimi elementi in jo nato izda, ne da bi jo dal na trg. To je obravnavano tudi v oddelku *3.2.7 Integration by other manufacturers*. V tem primeru pravni subjekt ni proizvajalec programske opreme, lahko pa je njen upravljavec. Kot je pojasnjeno tudi v prejšnjih oddelkih, se lahko pravni subjekt, ki izda brezplačno (ali skupnostno) različico in monetizirano različico iste proste in odprtokodne programske opreme, šteje tudi za upravljavca brezplačne (ali skupnostne) različice in proizvajalca monetizirane različice.

77. Podobno je pravni subjekt, ki monetizira prosto in odprtokodno programsko opremo, vendar je neprofitni subjekt, čigar prihodki po stroških se uporabijo za doseganje neprofitnih ciljev (in se zato njegova prosta in odprtokodna programska oprema ne šteje za dano na trg v smislu akta o kibernetski odpornosti, kot je obravnavano v oddelku *3.2.6 Not-for-profit entities*), upravljavec proste in odprtokodne programske opreme, ki jo izda.

78. Poleg tega nekatere fundacije ponujajo platforme za sodelovanje z različnimi oblikami upravljanja, ki proizvajalcem omogočajo, da redno prispevajo k razvoju proste in odprtokodne programske opreme, in/ali ki jih redno financirajo proizvajalci. Take fundacije je treba šteti za upravljavce v zvezi z določeno prosto in odprtokodno programsko opremo, ki je namenjena komercialnim dejavnostim in za katero fundacija zagotavlja trajno podporo. Toda, kot je pojasnjeno v oddelku *3.3 Open-source software stewards*, za tako fundacijo morda ne veljajo nobene obveznosti iz akta o kibernetski odpornosti za drugo določeno prosto in odprtokodno programsko opremo, ki jo gosti, če ne zagotavlja sistematične podpore za določeno prosto in odprtokodno programsko opremo, ne zagotavlja njene sposobnosti preživetja in/ali če ta določena programska oprema ni namenjena komercialnim dejavnostim.

([13]) Ta pojem je zajet tudi v besedni zvezi „namenjeni komercialnim dejavnostim“, vključeni v opredelitev pojma „upravljavec odprtokodne programske opreme“ iz člena 3(14) akta o kibernetski odpornosti.

([14]) Za pravno osebo morda tudi ne veljajo nobene obveznosti iz akta o kibernetski odpornosti v primerih, kadar: (i) določena prosta in odprtokodna programska oprema ni dana na trg v smislu akta o kibernetski odpornosti in (ii) pravni subjekt ne ustreza opredelitvi upravljavca v zvezi s to določeno prosto in odprtokodno programsko opremo.

79. Vrsta „trajne podpore“, ki jo fundacije in podobne organizacije zagotavljajo določenim projektom proste in odprtokodne programske opreme, se lahko zelo razlikuje. Nekatere pravne osebe na primer zagotavljajo le netehnično podporo, kot so upravljanje znamčenja projektov, določitev pravil upravljanja, organiziranje skupnostnih dogodkov ali zbiranje donacij. Drugi subjekti zagotavljajo tudi osnovno infrastrukturo IT, potrebno za izvajanje projekta, kot so gostovanje repozitorijev izvorne kode, zagotavljanje sistemov za nadzor različic ali generiranje podpisnih ključev. Drugi gredo pri vrsti podpore, ki jo zagotavljajo, še dlje, tako da projektu aktivno prispevajo inženirske vire, na primer z zaposlovanjem razvijalcev, usklajevanjem razvojnega dela, pregledovanjem ali združevanjem kode, upravljanjem izdaj ali obravnavanjem poročil o ranljivostih in varnostnih popravkov. Čeprav morajo vse pravne osebe, ki se štejejo za upravljavce na podlagi akta o kibernetski odpornosti, izpolnjevati obveznosti iz člena 24(1) in (2), se obseg, v katerem se obveznosti iz člena 14(1), (3) in (8) uporabljajo za te pravne osebe, razlikuje glede na vrsto podpore, ki jo zagotavljajo, v skladu s členom 24(3).

80. Upravljavec, ki zagotavlja le netehnično podporo, na primer po opredelitvi ni vključen v razvoj izdelka z digitalnimi elementi in mu zato ni treba sporočiti aktivno izrabljenih ranljivosti. Ta upravljavec tudi ne zagotavlja nobenih omrežij in informacijskih sistemov za razvoj takih izdelkov z digitalnimi elementi, zato mu ni treba poročati o resnih incidentih agenciji ENISA in skupinam CSIRT ali prizadetim uporabnikom. Kljub temu bi moral upravljavec, kadar ugotovi aktivno izrabljeno ranljivost (npr. prek poročila iz zunanjih virov, kot so raziskovalci varnosti), informacije deliti z vzdrževalci izdelka z digitalnimi elementi v skladu s svojo politiko kibernetske varnosti. Vzdrževalci izdelkov z digitalnimi elementi in/ali upravljavci bi morali razmisliti tudi o prostovoljnem sporočanju ranljivosti v skladu s členom 15.

81. Po drugi strani pa mora upravljavec, kadar zagotavlja osnovno infrastrukturo IT za določene izdelke z digitalnimi elementi, v skladu s členom 14(3) o vsakem resnem incidentu, povezanem s to infrastrukturo, ki vpliva na varnost izdelkov z digitalnimi elementi obvestiti agencijo ENISA in skupine CSIRT. Po potrebi mora obvestiti tudi vse uporabnike (npr. s splošno objavo). Kot je navedeno v prejšnji točki, upravljavcu ni treba sporočiti aktivno izrabljanih ranljivosti, ki jih ugotovi, moral pa bi spodbujati pravilno obravnavanje ranljivosti in razmisliti o prostovoljnem obveščanju v skladu s členom 15.

82. Nazadnje, kadar upravljavec zagotavlja tudi inženirske vire za določene izdelke z digitalnimi elementi, mora: (i) v skladu s členom 14(1) sporočiti aktivno izrabljene ranljivosti, ki jih ugotovi, in (ii) po potrebi obvestiti vse uporabnike. Kadar ima upravljavec tudi neposredno razmerje s prizadetimi uporabniki, jih mora v skladu s členom 14(8) obvestiti tudi neposredno.

83. Kadar subjekt preneha sistematično in trajno zagotavljati podporo za določeno prosto in odprtokodno programsko opremo, morda ne ustreza več opredelitvi upravljavca in zato zanj morda ne veljajo več ustrezne obveznosti. V takih primerih se ta subjekt spodbuja, naj jasno sporoči spremembo svojega statusa v zvezi s to določeno prosto in odprtokodno programsko opremo.

84. V nekaterih primerih se lahko subjekt, ki je bil upravljavec določenega projekta, odloči ta projekt neposredno monetizirati, tako, da izdelek z digitalnimi elementi da na trg, pri čemer mu nastanejo obveznosti proizvajalca iz akta o kibernetski odpornosti. V takih okoliščinah se ta subjekt šteje za proizvajalca izdelka z digitalnimi elementi od datuma, ko ga da na trg (ne pa v zvezi s prejšnjimi različicami, katerih upravljavec je bil).

3.4 **Prispevajoče osebe in uporabe nižje v verigi**

85. Kot je že navedeno v oddelku *3.1 Determining if free and open-source software is* under one's responsibility, je v aktu o kibernetski odpornosti pojasnjeno, da se ne uporablja „za fizične ali pravne osebe, ki z izvorno kodo prispevajo k izdelkom z digitalnimi elementi, ki se štejejo za prosto in odprtokodno programsko opremo, za katere niso odgovorne“ (uvodna izjava 18).

86. Proizvajalci izdelkov z digitalnimi elementi, ki v svoje izdelke z digitalnimi elementi vključujejo sestavne dele proste in odprtokodne programske opreme, prav tako ne postanejo odgovorni za posamično skladnost takih sestavnih delov z aktom o kibernetski odpornosti, tudi če prispevajo izvorno kodo za njihovo vzdrževanje.

87. Podobno zgolj to, da proizvajalci sestavne dele proste in odprtokodne programske opreme vključujejo v svoje (monetizirane) izdelke z digitalnimi elementi, ne vpliva na status tega sestavnega dela proste in odprtokodne programske opreme na podlagi akta o kibernetski odpornosti. Vzdrževalci sestavnih delov proste in odprtokodne programske opreme, ki niso dani na trg, nimajo obveznosti v zvezi z drugimi subjekti, ki lahko take sestavne dele vgradijo v svoje izdelke z digitalnimi elementi. Ali se akt o kibernetski odpornosti uporablja za določen sestavni del proste in odprtokodne programske opreme, je odvisno izključno od tega, ali ga fizična ali pravna oseba, ki ga je izdala, da na trg.

88. Kljub temu morajo proizvajalci izdelkov z digitalnimi elementi, ki vključujejo sestavne dele proste in odprtokodne programske opreme, izpolnjevati zahteve akta o kibernetski odpornosti za svoje izdelke z digitalnimi elementi. V skladu s členom 13(5) imajo tudi obveznost, da so primerno skrbni pri vgradnji sestavnih delov proste in odprtokodne programske opreme. Poleg tega morajo v skladu s členom 13(6) sporočiti ranljivosti v vgrajenih sestavnih delih in deliti varnostne popravke. Za dodatne usmeritve o tej temi glej oddelek *9.2.1 Reporting upstream and sharing security fixes*.

3.5 **Ponazoritveni scenariji**

89. Spodaj navedeni primeri so popolnoma hipotetični in namenjeni zgolj ponazoritvi različnih primerov, kot so pojasnjeni v zgornjih oddelkih.

Primer 27: razvijalec posameznik A je razvil prosto in odprtokodno programsko opremo. Razvijalec A to prosto in odprtokodno programsko opremo izda pod svojim imenom ali znamko, vendar za njeno uporabo ne zaračunava cene. Programska oprema se odprto deli in je vsem prosto na voljo za dostop, uporabo, spreminjanje in ponovno distribucijo. Razvijalec A vključi tudi povezavo do platforme za zbiranje prostovoljnih donacij.

Družbe B, C in D to prosto in odprtokodno programsko opremo vključijo v svoje izdelke z digitalnimi elementi. Naveden družbe za podporo tekočemu vzdrževanju razvijalcu A dajejo prostovoljne donacije, ki mu omogočajo, da projekt še naprej aktivno vzdržuje.

Ta prosta in odprtokodna programska oprema ni dana na trg v smislu akta o kibernetski odpornosti. Razvijalec A nima obveznosti na podlagi akta o kibernetski odpornosti. Družbe B, C in D morajo biti pri vgradnji te proste in odprtokodne programske opreme v svoje izdelke z digitalnimi elementi v skladu s členom 13(5) primerno skrbne.

Primer 28: neprofitna fundacija F izda sestavni del proste in odprtokodne programske opreme za vgradnjo v druge komercialne izdelke z digitalnimi elementi. Fundacija F se zaveže, da bo zagotavljala trajno podporo za to prosto in odprtokodno programsko opremo, da bi zagotovila njeno sposobnost preživetja in uvedbo. Družbe A, B in C to prosto in odprtokodno programsko opremo vgradijo v svoje izdelke z digitalnimi elementi. Družbi A in B prostovoljno prispevata del časa svojih razvijalcev k razvoju in vzdrževanju projektov proste in odprtokodne programske opreme v okviru fundacije F, tudi za to prosto in odprtokodno programsko opremo.

Ker je fundacija F neprofitni subjekt, ustanovljen tako, da se vsi prihodki po stroških uporabijo za doseganje neprofitnih ciljev, se prosta in odprtokodna programska oprema ne šteje za dano na trg v smislu akta o kibernetski odpornosti. Fundacija F je upravljavec te proste in odprtokodne programske opreme, zanjo pa veljajo ustrezne obveznosti iz člena 24. Družbe A, B in C morajo biti pri vgradnji te proste in odprtokodne programske opreme v svoje izdelke z digitalnimi elementi v skladu s členom 13(5) primerno skrbne.

Primer 29: družba A je razvila sestavni del proste in odprtokodne programske opreme za vgradnjo v svoje izdelke z digitalnimi elementi. To prosto in odprtokodno programsko opremo tudi ločeno izda pod svojim imenom ali znamko in jo aktivno vzdržuje. Vendar ne zaračunava njene uporabe niti je ne monetizira na druge načine. Družbe B, C in D to prosto in odprtokodno programsko opremo vgradijo v svoje izdelke z digitalnimi elementi in prostovoljno prispevajo del časa svojih razvijalcev k njenemu vzdrževanju.

Ta prosta in odprtokodna programska oprema se ne šteje za dano na trg v smislu akta o kibernetski odpornosti. Družba A ni njen proizvajalec, temveč njen upravljavec. Družbe B, C in D morajo biti pri vgradnji te proste in odprtokodne programske opreme v svoje izdelke z digitalnimi elementi v skladu s členom 13(5) primerno skrbne.

Primer 30: Družba A izda prosto in odprtokodno programsko opremo pod svojim imenom ali znamko in jo ponudi kot plačljivo različico, ki vključuje nekatere ugodnosti, kot sta tehnična pomoč ali optimizacija delovanja. Razvijalci iz družb B, C in D prispevajo k vzdrževanju proste in odprtokodne programske opreme, vendar ta ostaja pod nadzorom družbe A.

Družba A se šteje za proizvajalca te proste in odprtokodne programske opreme ([15]). Za družbe B, C in D ne veljajo obveznosti iz akta o kibernetski odpornosti za to prosto in odprtokodno programsko opremo. Če jo vgradijo v svoje izdelke z digitalnimi elementi, morajo biti v skladu s členom 13(5) pri tem primerno skrbne.

Primer 31: družba A izda prosto in odprtokodno programsko opremo pod svojim imenom ali znamko in zagotavlja stalno vzdrževanje, da zagotovi njeno dolgoročno sposobnost preživetja, kar omogoča vgradnjo te programske opreme v izdelke z digitalnimi elementi drugih družb. Družba A ne zaračunava njene uporabe, ne obdeluje osebnih podatkov, ki jih zbira prek izdelka z digitalnimi elementi, niti ne prodaja podpornih storitev, povezanih z izdajo proste in odprtokodne programske opreme.

Družba B prispeva kodo in čas razvijalcev k vzdrževanju proste in odprtokodne programske opreme, vendar je komercialno ne distribuira. Družba B ponuja storitve tehnične podpore neodvisno od distribucije proste in odprtokodne programske opreme. Družba A se šteje za upravljavca te proste in odprtokodne programske opreme, družba B pa nima obveznosti iz akta o kibernetski odpornosti za to prosto in odprtokodno programsko opremo.

Primer 32: sestavni del proste in odprtokodne programske opreme izda neprofitni subjekt, ustanovljen na način, ki zagotavlja, da se vsi prihodki po stroških uporabijo za doseganje neprofitnih ciljev. Subjekt zagotavlja trajno podporo, da zagotovi dolgoročno sposobnost preživetja projekta. Vzdrževanje se financira iz javnih sredstev, kot so nepovratna sredstva za raziskave. Dodatne razvojne dejavnosti, vključno z novimi funkcijami, se financirajo z donacijami in posebnimi projekti, ki se izvajajo v partnerstvu s proizvajalci, ki to prosto in odprtokodno programsko opremo vgrajujejo v svoje izdelke z digitalnimi elementi. Te funkcije so vključene v kodno bazo proste in odprtokodne programske opreme.

Neprofitni subjekt, ki izda prosto in odprtokodno programsko opremo, se šteje za upravljavca tega sestavnega dela proste in odprtokodne programske opreme. Proizvajalec, ki je prispeval k razvoju nekaterih funkcij, ne postane proizvajalec tega sestavnega dela proste in odprtokodne programske opreme. Kadar proizvajalec ta sestavni del proste in odprtokodne programske opreme vgradi v svoj izdelek z digitalnimi elementi, mora biti v skladu s členom 13(5) pri tem primerno skrben.

Primer 33: neprofitni subjekt, ustanovljen na način, ki zagotavlja, da se vsi prihodki po stroških uporabijo za doseganje neprofitnih ciljev, izda paket za razvoj proste in odprtokodne programske opreme in zagotavlja njegovo stalno vzdrževanje. Paket za razvoj programske opreme se odprto deli in je vsem prosto na voljo za dostop, uporabo, spreminjanje in ponovno distribucijo. Financiranje se zagotavlja s članarinami, ki se plačujejo neprofitnemu subjektu, razvijalci, zaposleni v organizacijah članicah, pa prispevajo kodo in druge vire k razvoju paketa za razvoj programske opreme. Proizvajalci uporabljajo paket za razvoj programske opreme kot sestavni del za izdelavo drugih izdelkov z digitalnimi elementi.

Neprofitni subjekt, ki izda ta paket za razvoj programske opreme, je njegov upravljavec. Člani fundacije niso odgovorni za skladnost paketa za razvoj programske opreme z aktom o kibernetski odpornosti. Kadar proizvajalci paket za razvoj programske opreme uporabijo za izdelavo lastnega izdelka z digitalnimi elementi, morajo biti v skladu s členom 13(5) primerno skrbni.

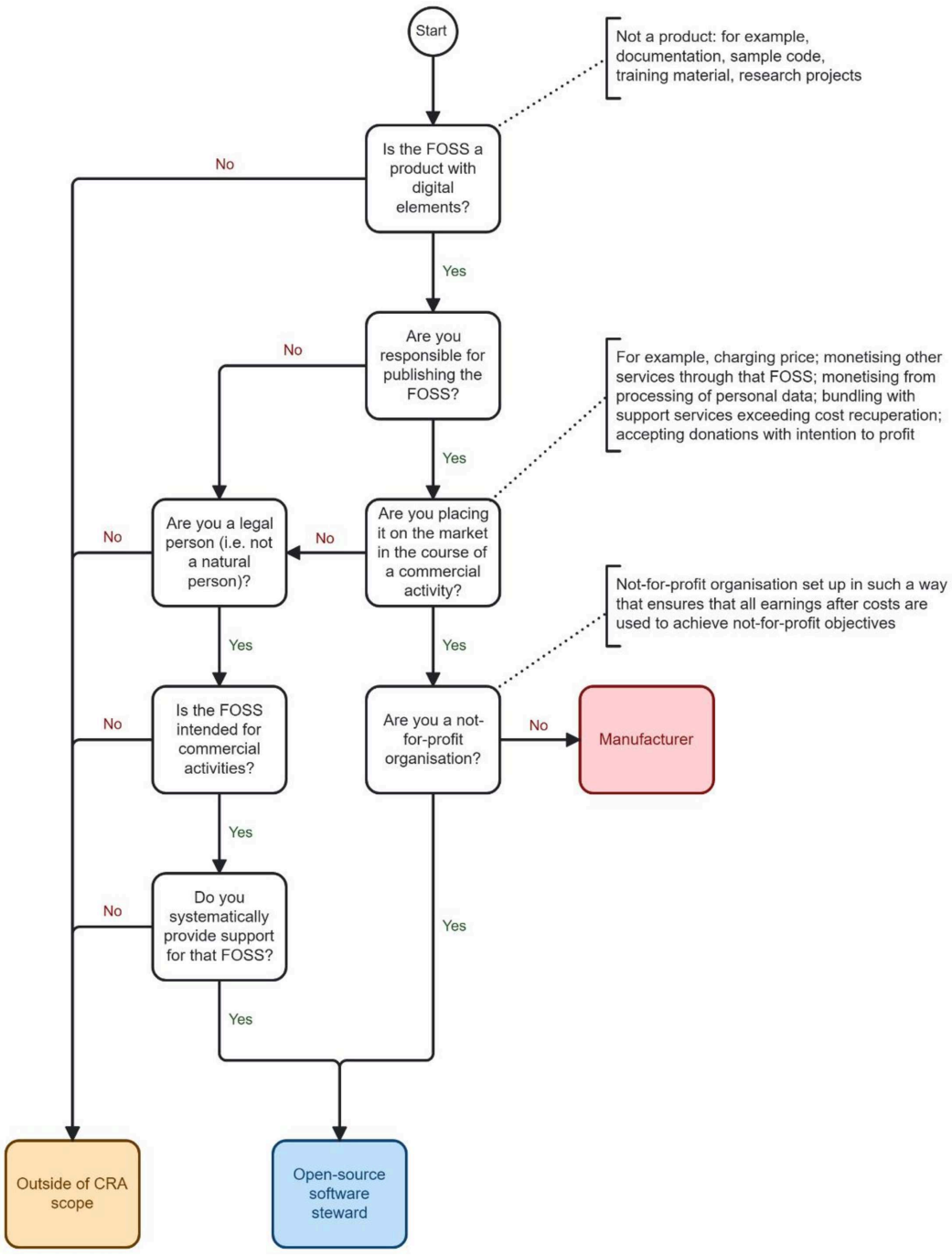
Primer 34: razvijalec posameznik izda knjižnico proste in odprtokodne programske opreme v javnem repozitoriju paketov za določen programski jezik in jo aktivno vzdržuje. Razvijalec v dokumentacijo paketa doda povezavo za zbiranje donacij. Proizvajalec to knjižnico brezplačno prenese iz repozitorija in jo vključi v svoj izdelek z digitalnimi elementi.

Razvijalec posameznik in repozitorij paketov nimata nobenih obveznosti iz akta o kibernetski odpornosti. Proizvajalec, ki vključi knjižnico, mora biti v skladu s členom 13(5) primerno skrben.

([15]) Razen če je družba A neprofitni subjekt, ustanovljena na način, ki zagotavlja, da se vsi prihodki po stroških uporabijo za doseganje neprofitnih ciljev; v tem primeru bi bila upravljavec te proste in odprtokodne programske opreme.

Slika 1

Stiliziran diagram poteka vključitve proste in odprtokodne programske opreme v področje uporabe akta o kibernetski odpornosti



4 BISTVENE SPREMEMBE IN REZERVNI DELI

90. V členu 3(30) akta o kibernetski odpornosti je „bistvena sprememba“ opredeljena kot sprememba izdelka z digitalnimi elementi po tem, ko je bil dan na trg, ki (i) vpliva na skladnost izdelka z digitalnimi elementi z bistvenimi zahtevami glede kibernetske varnosti iz dela I Priloge I ali (ii) povzroči spremembo predvidenega namena, za katerega je bil izdelek z digitalnimi elementi ocenjen.

91. Pojem bistvene spremembe je pomemben za ugotavljanje obveznosti na podlagi akta o kibernetski odpornosti v več primerih, vključno z naslednjimi:

(a) v skladu s členom 21 se uvoznik ali distributer, ki bistveno spremeni izdelek z digitalnimi elementi, ki je že bil dan na trg, šteje za njegovega proizvajalca;

(b) v skladu s členom 22 se vsaka fizična ali pravna oseba, ki bistveno spremeni izdelek z digitalnimi elementi ter omogoči dostopnost tega izdelka na trgu, šteje za njegovega proizvajalca;

(c) v skladu s členom 69(2) se vsaka fizična ali pravna oseba, ki po 11. decembru 2027 bistveno spremeni izdelek z digitalnimi elementi, dan na trg pred 11. decembrom 2027, in ga da na trg, šteje za njegovega proizvajalca;

(d) za proizvajalce izdelkov z digitalnimi elementi, danih na trg po 11. decembru 2027, da se ugotovi, ali je treba za izdelek z digitalnimi elementi zaradi sprememb, izvedenih po navedenem datumu, izvesti nov postopek ugotavljanja skladnosti, zlasti glede na ponavljajočo se naravo razvoja programske opreme.

92. Zato je pomembno zagotoviti usmeritve, ki gospodarskim subjektom pomagajo razumeti, kdaj spremembe strojne ali programske opreme pomenijo bistvene spremembe.

4.1 **Fizična popravila**

93. Kot je navedeno v uvodni izjavi 42 akta o kibernetski odpornosti, „kadar za izdelek z digitalnimi elementi veljajo ‚prenovitev', ‚vzdrževanje' in ‚popravilo', kakor so opredeljeni v členu 2, točke 18, 19 in 20 Uredbe (EU) 2024/1781 Evropskega parlamenta in Sveta, to ne povzroči nujno bistvene spremembe izdelka, če se na primer predviden namen in funkcije ter raven tveganja ne spremenijo. Nadgradnja izdelka z digitalnimi elementi, ki jo izvede proizvajalec, pa lahko povzroči spremembe zasnove in razvoja izdelka ter tako vpliva na njegov predviden namen in skladnost z zahtevami iz te uredbe." To je v skladu z oddelkom 2.1 Modrega vodnika, v katerem je opozorjeno, da je treba „proizvod, ki je bil po dajanju v uporabo bistveno spremenjen ali predelan, […] šteti za nov proizvod, če: (i) se spremenijo njegovo prvotno delovanje, namen ali tip, ne da bi bilo to predvideno v prvotni oceni tveganja; (ii) se je spremenila narava nevarnosti ali povečala stopnja tveganja glede na ustrezno harmonizacijsko zakonodajo Unije in (iii) je proizvod dostopen (ali dan v uporabo, če veljavna zakonodaja na svojem področju uporabe zajema tudi dajanje v uporabo). To je treba oceniti za vsak primer posebej in zlasti glede na cilj zakonodaje in tip proizvodov, zajetih z zadevno zakonodajo."

94. Prenovitev, vzdrževanje ali popravilo, ki povzročijo fizičnih sprememb izdelkov z digitalnimi elementi, ki so že bili dani na trg, ne pomenijo nujno bistvenih sprememb. Zato bi bila potrebna ocena za vsak primer posebej, da se ugotovi, ali taka fizična sprememba vpliva na skladnost izdelka z digitalnimi elementi z bistvenimi zahtevami iz dela I Priloge I ali povzroči spremembo predvidenega namena izdelka, zajetega z oceno tveganja za kibernetsko varnost.

95. Zamenjava delov z napako ali iztrošenih delov z deli, ki delujejo bolje (npr. zaradi tehničnega napredka ali ker se stari del ne proizvaja več), sama po sebi ne povzroči bistvene spremembe popravljenega izdelka z digitalnimi elementi. To se zgodi le, če sprememba delovanja ali način delovanja popravljenega izdelka z digitalnimi elementi (i) vpliva na njegovo skladnost z bistvenimi zahtevami ali (ii) povzroči spremembo predvidenega namena, ki ni bila zajeta z oceno tveganja.

Primer 35: proizvajalec računalniškega strežnika opravi popravilo, pri čemer okvarjeni pomnilnik RAM zamenja z novim, zmogljivejšim. To ne vpliva na skladnost strežnika z bistvenimi zahtevami. Strežnik deluje bolje, vendar njegovo novo delovanje ostaja v okviru njegove predvidene uporabe, kot se je upoštevala v oceni tveganja za kibernetsko varnost. Za računalniški strežnik se ne šteje, da je bil bistveno spremenjen.

4.2 **Rezervni deli**

96. Člen 2(6) akta o kibernetski odpornosti določa, da se akt o kibernetski odpornosti ne uporablja za rezervne dele, namenjene nadomestitvi enakih sestavnih delov in proizvedenih v skladu z istimi specifikacijami kot sestavni deli, ki naj bi jih nadomestili. V uvodni izjavi 29 je nadalje navedeno, da izjema velja za rezervne dele, ki so bili dani na voljo pred datumom začetka uporabe te akta o kibernetski odpornosti, kot tudi za rezervne dele, za katere je bil že opravljen postopek ugotavljanja skladnosti na podlagi Uredbe.

97. Izjemo iz člena 2(6) akta o kibernetski odpornosti bi bilo treba razumeti tako, da se uporablja le, kadar se rezervni del posebej dobavi za popravilo ali podaljšanje trajnosti izdelka z digitalnimi elementi, ki je že bil dan na trg (pred 11. decembrom 2027 ali po njem). Kadar se izdelek z digitalnimi elementi dobavi kot samostojen izdelek brez kakršne koli povezave z vzdrževanjem ali popravilom predhodno obstoječega izdelka z digitalnimi elementi, je dan na trg v smislu akta o kibernetski odpornosti in se ne bi smel šteti za rezervni del, ki spada na področje uporabe člena 2(6). Namen vzdrževanja ali popravila bi moral biti razviden iz okoliščin dobave, na primer z identifikacijo izdelka z digitalnimi elementi ali družine izdelkov v naročilu ali komercialni ponudbi ali z dobavo prek poprodajnih ali servisnih kanalov. Dokazila za to bi morala biti na voljo tudi organom za nadzor trga. Dejstvo, da bi se izdelek z digitalnimi elementi tehnično lahko uporabil za nadomestitev sestavnega dela, samo po sebi ne zadostuje, da bi spadal na področje uporabe izjeme, če ti elementi ne obstajajo.

98. Kadar je nadomestni del enak sestavnemu delu, ki je že vključen v izdelek z digitalnimi elementi, ki je bil dan na trg pred datumom začetka uporabe akta o kibernetski odpornosti ali v skladu z njim, se torej akt o kibernetski odpornosti za ta rezervni del ne uporablja.

99. Pri oceni, ali bi bilo treba rezervni del šteti za enakega sestavnemu delu, bi se bilo treba osredotočiti na njegovo funkcionalno vlogo v izdelku z digitalnimi elementi in lastnosti, ki so lahko pomembne za kibernetsko varnost. Čeprav je vedno potrebna ocena za vsak primer posebej, razlike, ki ne vplivajo na varnostne lastnosti ali profil tveganja za kibernetsko varnost sestavnega dela, same po sebi ne preprečujejo, da bi ta rezervni del spadal na področje uporabe člena 2(6) akta o kibernetski odpornosti.

100. Nasprotno pa lahko razlike v lastnostih, pomembnih za kibernetsko varnost sestavnega dela, kot so algoritmi, protokoli, kriptografski mehanizmi, elementi za nadzor dostopa ali druge lastnosti, pomembne za varnost, pomenijo, da se novi del ne more šteti za enakega sestavnemu delu, ki naj bi ga nadomestil.

101. Kadar rezervni del ni enak prvotnemu sestavnemu delu, se šteje za samostojen izdelek z digitalnimi elementi in se zato zanj uporablja akt o kibernetski odpornosti. V takih primerih je treba skladnost z bistvenimi zahtevami oceniti glede na predvideni namen nadomestnega sestavnega dela. Posebej pomembna je funkcija nadomestnega sestavnega dela, da zagotavlja združljivost ali interoperabilnost z obstoječim izdelkom z digitalnimi elementi, tudi kadar je ta izdelek izdelek z digitalnimi elementi, dan na trg pred začetkom uporabe akta o kibernetski odpornosti. Kadar nekaterih bistvenih zahtev zaradi predvidenega namena ali tehničnih omejitev ni mogoče razumno izpolniti, mora proizvajalec to upoštevati v oceni tveganja za kibernetsko varnost ter izvesti ustrezne alternativne ali kompenzacijske ukrepe za zmanjšanje tveganja, da se ne ogrozi varnost izdelka z digitalnimi elementi. Kot je obravnavano tudi v oddelku *2.6 Complex systems*, imajo tehnična dokumentacija ter informacije in navodila za uporabnika ključno vlogo pri preglednem opisovanju ugotovljenih omejitev, povezanih tveganj za kibernetsko varnost in izvedenih ukrepov za zmanjšanje tveganja. Kot je pojasnjeno v oddelku *4.1 Physical repairs*, zamenjava delov z napako ali iztrošenih delov z deli, ki delujejo bolje, sama po sebi ne pomeni bistvene spremembe popravljenega izdelka z digitalnimi elementi.

Primer 36: proizvajalec je dal na trg EU povezane krmilnike. V enem primeru je bil krmilnik dan na trg leta 2026, pred datumom začetka uporabe akta o kibernetski odpornosti. V drugem primeru je bil krmilnik dan na trg leta 2028 v skladu z aktom o kibernetski odpornosti. Leta 2028 se okvari digitalni komunikacijski modul v obeh vrstah krmilnikov. Proizvajalec kot rezervni del dobavi nadomestni modul, ki je enak in izdelan po enakih specifikacijah kot prvotni modul.

V obeh primerih nadomestni modul spada na področje uporabe izjeme iz člena 2(6). Za sam rezervni del se akt o kibernetski odpornosti ne uporablja, čeprav je izdelek z digitalnimi elementi, saj nadomešča enak sestavni del v izdelku z digitalnimi elementi. Popravilo ne pomeni bistvene spremembe izdelka z digitalnimi elementi.

Primer 37: proizvajalec je dal leta 2026, pred datumom začetka uporabe akta o kibernetski odpornosti, na trg EU povezani industrijski krmilnik. Leta 2028 se v navedenem krmilniku okvari komunikacijski čip. Ker proizvajalec navedenega čipa ne proizvaja več, kot rezervni del dobavi novejši čip z enakovredno funkcijo, vendar z drugačno kriptografsko izvedbo in posodobljenim mehanizmom varnega zagona, da bi ohranil združljivost in nadaljnje delovanje.

V tem primeru nadomestnega čipa ni mogoče šteti za enakega, saj razlike v kriptografski izvedbi in mehanizmu varnega zagona vplivajo na lastnosti čipa z vidika kibernetske varnosti. Zato zanj ne velja izjema iz člena 2(6) in pomeni izdelek z digitalnimi elementi, za katerega se uporablja akt o kibernetski odpornosti. Skladnost nadomestnega dela je treba oceniti glede na njegov predvideni namen, vključno z njegovo vlogo pri zagotavljanju interoperabilnosti z izdelkom z digitalnimi elementi, danim na trg pred začetkom uporabe akta o kibernetski odpornosti.

Primer 38: proizvajalec da leta 2028 na trg krmilnik za pametno stavbo v skladu z aktom o kibernetski odpornosti. Leta 2029 se v tem krmilniku okvari brezžični modul. Ker proizvajalec navedenega modula ne proizvaja več, kot rezervni del dobavi nov modul, ki opravlja enako funkcijo z uporabo enakih komunikacijskih protokolov in varnostnih mehanizmov, vendar temelji na drugem čipnem naboru in ima posodobljeno vdelano strojno programsko opremo, ki ne spreminja lastnosti, ki bi lahko bile pomembne za kibernetsko varnost.

V tem primeru se lahko nadomestni modul šteje za enakega. Zato za modul velja izjema iz člena 2(6) in se akt o kibernetski odpornosti zanj ne uporablja.

102. Za rezervne dele se izjema uporablja ne glede na to, ali rezervni del nadomešča sestavni del v izdelku z digitalnimi elementi ali celoten izdelek z digitalnimi elementi, ki je sam del večjega izdelka, tudi kadar je ta večji izdelek z digitalnimi elementi sestavljen iz več vgrajenih sestavnih delov, pod pogojem, da se nadomestni del posebej dobavi kot rezervni del, kot je pojasnjeno v prejšnjih odstavkih.

Primer 39: proizvajalec da leta 2027 na trg sistem za industrijsko avtomatizacijo, ki vključuje programirljivi logični krmilnik kot enega od sestavnih delov. Leta 2031 se okvari centralna procesna enota programirljivega logičnega krmilnika. Proizvajalec ponuja dve možnosti popravila: (i) dobavo nadomestne centralne procesne enote, ki se lahko šteje za enako prvotno nameščeni centralni procesni enoti, ali (ii) dobavo celotnega nadomestnega programirljivega logičnega krmilnika, ki se lahko šteje za enakega prvotno nameščenemu programirljivemu logičnemu krmilniku. V vsakem primeru se nadomestni del dobavi prek poprodajnega servisnega kanala proizvajalca kot rezervni del, sistem za industrijsko avtomatizacijo, kateremu je nadomestni del namenjen, pa je jasno opredeljen. V obeh primerih nadomestni del spada na področje uporabe izjeme iz člena 2(6), ne glede na to, ali se zamenjava nanaša na sestavni del v programirljivem logičnem krmilniku ali na programirljivi logični krmilnik kot celoto.

4.3 **Posodobitve programske opreme kot bistvene spremembe**

103. Razvoj programske opreme je po svoji naravi ponavljajoč se, programski izdelki z digitalnimi elementi, ki so že dani na trg, pa se pogosto in stalno posodabljajo. V tem okviru je koristno zagotoviti dodatne usmeritve za ugotavljanje, kdaj se programska oprema šteje za bistveno spremenjeno. Takšne usmeritve naj bi proizvajalcem programskih izdelkov z digitalnimi elementi, ki spreminjajo lastne izdelke, zlasti pomagale ugotoviti, ali te spremembe pomenijo bistveno spremembo.

104. V uvodni izjavi 39 je navedeno, da je izdelek z digitalnimi elementi bistveno spremenjen, kadar se s spremembo spremeni stopnja tveganja za kibernetsko varnost in tega spremenjenega ali dodatnega tveganja proizvajalec ni upošteval v oceni tveganja in posledično pri izpolnjevanju bistvenih zahtev. Zato bi moral proizvajalec za vsak primer posebej oceniti, ali posodobitev programske opreme povzroči nova ali povečana tveganja za kibernetsko varnost in ali je taka tveganja že obravnaval v oceni tveganja.

105. Kadar proizvajalec v izdelek z digitalnimi elementi uvede nove funkcije, zaradi katerih se spremeni predvideni namen izdelka kot celote, takih sprememb verjetno ni upošteval v oceni tveganja. V takih okoliščinah bi sprememba na splošno pomenila bistveno spremembo.

Primer 40: proizvajalec da na trg pregledno ploščo, ki zbira podatke iz strojev ter prikazuje trende in opozorila, ne more pa teh strojev upravljati. Proizvajalec nato razvije novo različico te pregledne plošče, s katero uvede funkcije, ki ji omogočajo upravljanje strojev, med drugim s prilagajanjem obratovalnih parametrov in ponovnim zagonom strojev po nastopu stanj z okvaro. Zaradi teh sprememb se je predvideni namen pregledne plošče razvil prek tega, kar je bilo predvideno v oceni tveganja, in sicer se je iz orodja za situacijsko zavedanje spremenila v izdelek z digitalnimi elementi, namenjen izvajanju operativnega nadzora nad drugimi napravami. Pregledna plošča je bila torej bistveno spremenjena.

Primer 41: proizvajalec da na trg potrošniško aplikacijo, namenjeno organiziranju in prikazovanju osebnih podatkov, kot so elektronska pošta, sporočila ali dokumenti, ter podpiranju osnovnih funkcij iskanja in filtriranja. Proizvajalec nato uvede posodobitev, ki omogoča, da aplikacija samodejno analizira uporabniške vsebine, da bi se ustvarili vedenjski profili in sprejemale avtomatizirane odločitve, ki vplivajo na prednostno razvrščanje, omejevanje ali priporočanje vsebin brez posredovanja uporabnika. Zaradi te spremembe se predvideni namen programske opreme spremeni iz uporabniško nadzorovanega orodja za upravljanje informacij v sistem za avtomatizirano sprejemanje odločitev, kar ni bilo predvideno v oceni tveganja. Aplikacija je bila torej bistveno spremenjena.

106. Hkrati pa je mogoče, da proizvajalec postopoma uvaja nove funkcije, ki so že vključene v njegovo oceno tveganja ali ki same po sebi ne spreminjajo profila tveganja za kibernetsko varnost izdelka z digitalnimi elementi. To se lahko zgodi na primer, kadar je proizvajalec predvidel razvoj teh funkcij, že opisal in ocenil povezana tveganja ter izvedel ustrezne blažilne ukrepe za zagotovitev stalne skladnosti z bistvenimi zahtevami. To se lahko zgodi tudi, kadar nove funkcije ne uvajajo sprememb, ki bi povzročile nova ali povečana tveganja. Posodobitve take narave se zato ne bi smele šteti za bistvene spremembe, saj ne povečujejo tveganja za kibernetsko varnost in posledično ne spreminjajo izpolnjevanja bistvenih zahtev.

Primer 42: aplikacija za pošiljanje sporočil se prvotno izda s funkcijo, omejeno na pošiljanje sporočil eden z enim. Proizvajalec v oceni tveganja zajame pozneje uvedeno skupinsko pošiljanje sporočil, vključno na primer z bolj kompleksnim usmerjanjem sporočil. Z nadaljnjo posodobitvijo proizvajalec doda funkcijo skupinskega klepeta skupaj s skrbniškimi kontrolami in orodji za moderiranje, ki so bili že predvideni in ocenjeni v prvotni zasnovi. S posodobitvijo se uvedejo funkcije, ki spadajo v okvir prvotnega predvidenega namena in ocene tveganja. Aplikacija za pošiljanje sporočil zato ni bila bistveno spremenjena.

Primer 43: sistem za spremljanje proizvodnje je dan na trg z omogočenimi preglednimi ploščami samo za branje, funkcije avtomatiziranega krmiljenja pa so v arhitekturi sistema, vendar ostanejo onemogočene. Proizvajalec v oceni tveganja izrecno zajame prihodnjo aktivacijo avtomatiziranih krmilnih zank, vključno s tveganji za kibernetsko varnost, povezanimi s krmiljenjem v zaprti zanki, in zaščitnimi ukrepi, kot so mehanizmi za prevzem nadzora s strani operaterja in stanja varne zaustavitve. Z naknadno posodobitvijo proizvajalec omogoči funkcije avtomatiziranega krmiljenja in aktivira zaščitne ukrepe, kot so bili prvotno ocenjeni. Sistem za spremljanje proizvodnje zato ni bil bistveno spremenjen.

107. Nasprotno pa lahko tudi omejene ali navidezno manjše nove funkcije povzročijo znatna tveganja za kibernetsko varnost, ki vplivajo na skladnost z bistvenimi zahtevami. Ocena bistvene spremembe zato ne bi smela temeljiti na obsegu ali kompleksnosti spremembe, temveč na njenem morebitnem škodljivem vplivu na profil tveganja za kibernetsko varnost izdelka z digitalnimi elementi in posledično na izpolnjevanje bistvenih zahtev.

Primer 44: Proizvajalec uvede posodobitev aplikacije, s katero doda funkcijo „zapomni si me“ ali funkcijo trajne prijave, ki lokalno shranjuje avtentikacijske žetone za večjo priročnost za uporabnike. Čeprav je obseg funkcije omejen, z njo nastanejo nova tveganja, povezana s krajo žetonov, nepooblaščenim dostopom in ugrabitvijo seje, ki se v oceni tveganja niso upoštevala. Posodobitev torej vpliva na skladnost z bistvenimi zahtevami. Aplikacija je bila bistveno spremenjena.

Primer 45: proizvajalec obstoječemu programskemu izdelku z digitalnimi elementi doda novo funkcijo beleženja in diagnostike, ki omogoča izvoz podrobnih sistemskih dnevnikov za namene odpravljanja težav. Čeprav se zdi funkcija manj pomembna, povzroči zbiranje in shranjevanje občutljivih operativnih podatkov v nešifrirani obliki, s čimer nastanejo tveganja razkritja podatkov, ki se prej niso ocenila ali zmanjšala. Sprememba ima zato lahko znaten vpliv na profil tveganja za kibernetsko varnost izdelka z digitalnimi elementi. Programski izdelek z digitalnimi elementi je bil bistveno spremenjen.

108. V skladu z uvodno izjavo 39 akta o kibernetski odpornosti se varnostne posodobitve na splošno ne bi smele šteti za bistvene spremembe, saj je njihov glavni namen zmanjšati raven tveganja za kibernetsko varnost, povezanega z izdelkom z digitalnimi elementi. Varnostna posodobitev, ki ne povzroči spremembe predvidenega namena izdelka z digitalnimi elementi in ne uvaja novih tveganj za kibernetsko varnost, se zato ne bi smela šteti za bistveno spremembo, tudi kadar se lahko z njo uvedejo znatne tehnične spremembe. To vključuje primere, ko se določene funkcije spremenijo ali omejijo izključno z namenom ublažitve ugotovljenih ranljivosti in zagotavljanja nadaljnje skladnosti z bistvenimi zahtevami.

Primer 46: proizvajalec uvede varnostno posodobitev za odpravo ranljivosti v kodni bazi izdelka z digitalnimi elementi, in sicer tako, da popravi napako pri potrjevanju vhoda, ki bi lahko povzročila prekoračitev medpomnilnika, ali odpravi logično napako, ki omogoča, da se avtentikacija zaobide z neustreznim preverjanjem žetona seje. S posodobitvijo se spremeni notranja izvedba programske opreme, ne da bi to vplivalo na predvideni namen tega izdelka ali povzročilo nastanek nove izpostavljenosti. Taka posodobitev je namenjena izključno zmanjšanju tveganja za kibernetsko varnost. Varnostna posodobitev se ne bi smela šteti za bistveno spremembo.

Primer 47: proizvajalec uvede varnostno posodobitev, s katero okrepi obstoječe varnostne konfiguracije, kot so poostritev pravil požarnega zidu, onemogočanje neuporabljenih omrežnih vrat, sprememba privzetih politik skrbniških gesel ali uvedba obvezne večfaktorske avtentikacije, kadar je bila taka funkcija že na voljo ali predvidena. Čeprav lahko posodobitev vpliva na to, kako uporabniki konfigurirajo izdelek z digitalnimi elementi ali dostopajo do njega, se z njo ne spremeni predvideni namen izdelka in je namenjena izključno izboljšanju stanja varnosti izdelka. Varnostna posodobitev se ne bi smela šteti za bistveno spremembo.

Primer 48: proizvajalec da na trg programski izdelek z digitalnimi elementi, ki varuje komunikacije z nastavljivim šifrirnim ogrodjem, ki podpira več kriptografskih algoritmov in velikosti ključev, kot je opisano v tehnični dokumentaciji izdelka in oceni tveganja. Ocena tveganja zajema vse kriptografske možnosti, zagotovljene v izdelku z digitalnimi elementi, in predvideva opuščanje nekaterih algoritmov v prihodnosti. Ocena tveganja vključuje tudi blažilne ukrepe, kot so kriptografska prožnost, notranje upravljanje ključev in testiranje združljivosti. Proizvajalec v odziv na nastajajoče kriptografske usmeritve uvede varnostno posodobitev, ki onemogoči opuščeni algoritem in aktivira močnejšo, že podprto alternativo, pri čemer se ne uvede nova zunanja odvisnost niti ne spremenijo podatkovni tokovi. Ker se s posodobitvijo izvede varnostni ukrep, ki je bil predviden in ocenjen kot del prvotne zasnove, in ker posodobitev ne povzroči novih tveganj za kibernetsko varnost, se ne bi smela šteti za bistveno spremembo.

109. Nasprotno pa se lahko varnostna posodobitev šteje za bistveno spremembo, kadar kljub svojemu varnostnemu cilju povzroči, da se predvideni namen izdelka z digitalnimi elementi spremeni onkraj prvotno predvidenega ali da nastanejo nova ali povečana tveganja za kibernetsko varnost. To se lahko zgodi na primer, kadar posodobitev znatno spremeni meje tega izdelka ali strukturo odvisnosti na način, ki ni bil predviden v oceni tveganja, na primer z znatno spremembo podatkovnih tokov ali dodajanjem novih vmesnikov, dostopnih od zunaj.

Primer 49: proizvajalec da na trg programski izdelek z digitalnimi elementi, namenjen zagotavljanju lokalnega šifriranja datotek za podatke, shranjene na napravi uporabnika, ki uporabnikom omogoča šifriranje in dešifriranje datotek na zahtevo. Po odkritju ranljivosti v delovnem toku šifriranja proizvajalec uvede varnostno posodobitev, s katero odstrani funkcijo lokalnega šifriranja in namesto tega zahteva, da se vse datoteke naložijo v oddaljeno storitev šifriranja, ki jo upravlja proizvajalec, se v njej shranijo in obdelujejo. Zaradi te spremembe izdelek z digitalnimi elementi ne izvaja več lokalnega šifriranja, kot je bilo prvotno predvideno, temveč deluje kot oddaljena storitev šifriranja in obdelave podatkov. Čeprav se posodobitev uvede iz varnostnih razlogov, temeljno spreminja predvideni namen tega izdelka na način, ki ni bil predviden v oceni tveganja, zato pomeni bistveno spremembo.

Primer 50: proizvajalec da na trg programski izdelek z digitalnimi elementi, ki za varovanje komunikacij med sestavnimi deli izdelka z digitalnimi elementi uporablja uveljavljen šifrirni protokol in notranje upravljani življenjski cikel ključev. V odziv na novo ugotovljene kriptografske pomanjkljivosti proizvajalec uvede varnostno posodobitev, s katero obstoječi šifrirni mehanizem nadomesti z drugim protokolom, ki zahteva uporabo zunanje storitve upravljanja ključev, ki jo upravlja tretja oseba. S tem se povzroči bistvena sprememba odvisnosti in podatkovnih tokov izdelka z digitalnimi elementi, pri čemer se uvedejo novi zunanji vmesniki in uporaba storitev tretjih oseb, ki se niso upoštevali v oceni tveganja. Čeprav je posodobitev usmerjena v varnost, uvaja nova tveganja za kibernetsko varnost in zato pomeni bistveno spremembo.

110. Kot je navedeno v točki 104 zgoraj, bi bilo treba vprašanje, ali posodobitev programske opreme pomeni bistveno spremembo, oceniti za vsak primer posebej. Pri izvajanju te ocene lahko proizvajalci med drugim upoštevajo, ali se s posodobitvijo programske opreme:

(a) uvajajo novi vektorji groženj, kot so dodatni vmesniki, komunikacijski kanali, izvajalska okolja ali zunanje odvisnosti, prek katerih bi se lahko grožnje uresničile;

(b) omogočajo novi scenariji napadov, na primer tudi na nove načine, na katere bi lahko verjetno prišlo do nepooblaščenega dostopa, manipulacije, motenj ali zlorabe izdelka z digitalnimi elementi ali podatkov, ki jih obdeluje;

(c) spremeni verjetnost predhodno opredeljenih scenarijev napadov, na primer tako, da je za njihovo izkoriščanje potrebnega manj napora ali strokovnega znanja, da se poveča izpostavljenost akterjem, ki niso vredni zaupanja, ali oslabijo obstoječi zaščitni ukrepi;

(d) spremeni morebitni vpliv predhodno opredeljenih scenarijev napadov, vključno na primer z obsegom prizadetih podatkov ali funkcij, resnostjo operativnih, varnostnih ali gospodarskih posledic ali zmožnostjo odkrivanja in zajezitve incidenta ali okrevanja po njem.

111. V nekaterih primerih se s posodobitvijo programske opreme ne uvedejo novi vektorji groženj, ne omogočijo novi scenariji napadov in ne spremeni bistveno verjetnost ali vpliv predhodno opredeljenih scenarijev napadov. To lahko kaže, da posodobitev ne povzroča novih ali povečanih tveganj za kibernetsko varnost, pod pogojem, da predpostavke in blažilni ukrepi, na katerih temelji ocena tveganja, ostanejo veljavni in učinkoviti. Zato taka posodobitev verjetno ne pomeni bistvene spremembe.

112. Nasprotno pa se lahko s posodobitvijo programske opreme uvedejo novi vektorji groženj, omogočijo novi scenariji napadov ali bistveno spremeni verjetnost ali vpliv obstoječih scenarijev napadov. V takih primerih bi moral proizvajalec ponovno oceniti tveganja za kibernetsko varnost izdelka z digitalnimi elementi in ugotoviti, ali so bistvene zahteve še vedno izpolnjene, vključno s tem, ali posodobitev povzroči nova ali povečana tveganja, ki niso bila predvidena v oceni tveganja.

113. Vprašanje, ali posodobitev programske opreme pomeni bistveno spremembo, je pomembno pri ugotavljanju, ali veljajo nekatere obveznosti iz akta o kibernetski odpornosti, kot je določeno v točki 91. Vendar proizvajalci ne glede na to opredelitev ostanejo odgovorni za zagotavljanje varnosti posodobitev programske opreme in svojega izdelka z digitalnimi elementi v njegovem obdobju podpore v skladu z zahtevami glede obravnavanja ranljivosti iz dela II Priloge I k aktu o kibernetski odpornosti. Poleg tega morajo proizvajalci ne glede na to, ali posodobitve programske opreme štejejo za bistvene spremembe ali ne, v skladu s členoma 13(7) in 31(2) zagotavljati, da sta ocena tveganja in tehnična dokumentacija točni, popolni ter se stalno posodabljata.

4.4 **Posledice bistvene spremembe**

114. Posledice bistvene spremembe, ki jo izvede akter, ki ni prvotni proizvajalec izdelka z digitalnimi elementi, ki je že bil dan na trg, so obravnavane v členih 21 in 22 akta o kibernetski odpornosti. Člen 21 se nanaša na uvoznike in distributerje, člen 22 pa vsako fizično ali pravno osebo, ki ni proizvajalec, uvoznik ali distributer.

115. Kadar bistveno spremembo izvede prvotni proizvajalec izdelka z digitalnimi elementi, posledice izhajajo iz splošno uveljavljenega pojma bistvene spremembe iz uvodne izjave 41 akta o kibernetski odpornosti in so podrobneje pojasnjene v oddelku 2.1 Modrega vodnika. V navedenem oddelku je navedeno, da je treba izdelek, ki je bil po dajanju na trg bistveno spremenjen ali predelan, šteti za nov izdelek, če se spremenijo njegovo prvotno delovanje, namen ali tip, če se je spremenila narava nevarnosti ali povečala stopnja tveganja in če je izdelek z digitalnimi elementi dostopen na trgu.

116. Splošno priznana posledica je torej, da je treba, kadar se sprememba izdelka z digitalnimi elementi šteje za bistveno spremembo in je spremenjeni izdelek z digitalnimi elementi dostopen na trgu, ta izdelek za namene akta o kibernetski odpornosti obravnavati kot nov izdelek z digitalnimi elementi. Posledično dejanje dajanja bistveno spremenjenega izdelka na trg pomeni novo dajanje na trg. To velja ne glede na to, ali bistveno spremembo izvede prvotni proizvajalec ali druga oseba. Da bi se zagotovila enotna in sorazmerna uporaba akta o kibernetski odpornosti pri različnih kategorijah akterjev, ki lahko izvedejo bistveno spremembo, so v naslednjih pododdelkih obravnavane posledične obveznosti osebe, ki izvede bistveno spremembo, kadar se bistveno spremenjeni izdelek z digitalnimi elementi da na trg. Posledice za obdobje podpore za izdelek z digitalnimi elementi so obravnavane v oddelku *5 Support period*.

4.4.1 *Bistvene spremembe, ki jih izvede oseba, ki ni prvotni proizvajalec*

117. V skladu s členoma 21 in 22 se v primeru, ko izdelek z digitalnimi elementi, ki je že bil dan na trg, bistveno spremeni fizična ali pravna oseba, ki ni proizvajalec izdelka z digitalnimi elementi, oseba, ki izdelek z digitalnimi elementi bistveno spremeni in omogoči njegovo dostopnost na trgu, šteje za proizvajalca spremenjenega izdelka z digitalnimi elementi, ne glede na to, ali je ta oseba sodelovala pri prvotni zasnovi ali dajanju tega izdelka na trg.

118. Člen 22 nadalje pojasnjuje, da za osebo, ki izvede spremembo, obveznosti iz členov 13 in 14 veljajo le za del izdelka z digitalnimi elementi, na katerega vpliva bistvena sprememba, ali za celotni izdelek, če bistvena sprememba vpliva na kibernetsko varnost izdelka z digitalnimi elementi kot celoto.

119. Kadar bistvena sprememba vpliva na skladnost z bistvenimi zahtevami, vendar ne vpliva negativno na kibernetsko varnost izdelka z digitalnimi elementi kot celoto, se za osebo, ki izvede spremembo, člena 13 (vključno z obveznostjo zagotavljanja skladnosti z bistvenimi zahtevami in izvedbe postopka ugotavljanja skladnosti) in 14 (obveznosti poročanja) uporabljata le v zvezi z delom izdelka z digitalnimi elementi, ki je bil bistveno spremenjen ([16]). Poleg tega se obveznosti prvotnega proizvajalca na podlagi akta o kibernetski odpornosti še naprej uporabljajo za prvotni izdelek z digitalnimi elementi, ki je bil dan na trg, s čimer se zagotovi neprekinjenost obravnavanja ranljivosti in nadaljnja skladnost nespremenjenih delov.

120. Primera bistvene spremembe ne bi smeli zamenjevati s primeri vgradnje, v katerih oseba sestavi sestavne dele (po potrebi tudi tako, da jih spremeni) v nov izdelek z digitalnimi elementi, ki ga sama da na trg. V takih primerih integrator ne spremeni izdelka z digitalnimi elementi, ki ga je na trg že dal drug proizvajalec, temveč daje na trg svoj nov izdelek z digitalnimi elementi. Integrator je za namene akta o kibernetski odpornosti proizvajalec takega novega izdelka z digitalnimi elementi in mora v zvezi z izdelkom z digitalnimi elementi kot celoto ravnati v celoti v skladu z Uredbo. Kadar proizvajalec vgradi sestavne dele, za katere se uporablja akt o kibernetski odpornosti, si lahko zagotavljanje skladnosti z aktom o kibernetski odpornosti olajša tako, da se opre na dejavnosti zagotavljanja skladnosti proizvajalcev sestavnih delov.

Primer 51: družba od tretjih dobaviteljev kupi standardne mikrokrmilniške module in sestavne dele za povezljivost, razvije lastno strojno programsko opremo in paket senzorjev ter jih sestavi v povezani izdelek z digitalnimi elementi za spremljanje v kmetijstvu, ki ga da na trg pod svojim imenom. Čeprav je družba spremenila osnovne mikrokrmilniške module in jih povezala z drugimi sestavnimi deli, ni bistveno spremenila izdelka z digitalnimi elementi, ki je že bil dan na trg, temveč daje na trg nov izdelek z digitalnimi elementi. Družba je za namene akta o kibernetski odpornosti proizvajalec izdelka za spremljanje v kmetijstvu in mora v zvezi s tem izdelkom kot celoto ravnati v skladu z Uredbo.

([16]) V skladu z oddelkom 2.1 Modrega vodnika „[z]a vidike, na katere sprememba ne vpliva, ni treba ponoviti preskusov in pripraviti nove dokumentacije. Fizična ali pravna oseba, ki izvede ali naroči spremembe proizvoda, mora dokazati, da ni treba posodobiti vseh elementov tehnične dokumentacije. Fizična ali pravna oseba, ki izvede ali naroči spremembe proizvoda, je odgovorna za skladnost spremenjenega proizvoda in pripravi izjavo o skladnosti, tudi če uporabi obstoječe preskuse in tehnično dokumentacijo.“

121. Kadar izdelek z digitalnimi elementi bistveno spremeni oseba, ki ni prvotni proizvajalec, in ta sprememba negativno vpliva na kibernetsko varnost takega izdelka kot celote, na primer ker sprememba ni več ciljno usmerjena ali omejena na določen sestavni del ali podsistem, je treba spremenjeni izdelek z digitalnimi elementi, ki je dostopen na trgu, obravnavati kot nov izdelek z digitalnimi elementi, za katerega se v celoti uporablja akt o kibernetski odpornosti. V takih primerih se je splošni profil tveganja za kibernetsko varnost navedenega izdelka spremenil, spremembe pa ni mogoče oceniti brez upoštevanja izdelka z digitalnimi elementi kot celote. Za osebo, ki izvede spremembo, veljajo obveznosti proizvajalca iz členov 13 in 14 v zvezi s spremenjenim izdelkom z digitalnimi elementi kot celoto.

4.4.2 *Bistvene spremembe, ki jih izvede prvotni proizvajalec*

122. Kadar bistveno spremembo izvede prvotni proizvajalec, tudi v okviru ponavljajočega se razvoja programskih izdelkov z digitalnimi elementi, ta proizvajalec ostane proizvajalec za namene akta o kibernetski odpornosti. Vendar se za bistveno spremenjeni izdelek z digitalnimi elementi šteje, da je na novo dan na trg.

123. V skladu z oddelkom 2.1 Modrega vodnika lahko prvotni proizvajalec, ki bistveno spremenjeni izdelek z digitalnimi elementi da na trg, ponovno uporabi obstoječo dokumentacijo in preskuse za vidike izdelka z digitalnimi elementi, na katere bistvena sprememba ne vpliva. Zlasti kadar proizvajalec daje na trg bistveno spremenjene različice istega izdelka z digitalnimi elementi, bi moral biti postopek ugotavljanja skladnosti osredotočen na bistveno spremenjene dele izdelka z digitalnimi elementi. Podobno bi se moral organ za ugotavljanje skladnosti, kadar ugotavljanje skladnosti izvede tretja oseba, v svoji oceni osredotočiti na bistveno spremenjene dele. Za nespremenjene dele izdelka z digitalnimi elementi lahko ponovno uporabi obstoječo dokumentacijo in rezultate preskusov.

124. Premisleki glede sorazmernosti iz prejšnjega pododdelka se enako uporabljajo za bistvene spremembe, ki jih izvede prvotni proizvajalec izdelka z digitalnimi elementi, danega na trg pred 11. decembrom 2027. Taka bistvena sprememba, ki jo izvede prvotni proizvajalec, sama po sebi ne zahteva, da proizvajalec celoten izdelek z digitalnimi elementi, dan na trg pred navedenim datumom, popolnoma uskladi z aktom o kibernetski odpornosti, razen če sprememba negativno vpliva na kibernetsko varnost izdelka z digitalnimi elementi kot celoto. Kadar sprememba ne vpliva na kibernetsko varnost izdelka z digitalnimi elementi kot celoto, bi morale biti obveznosti prvotnega proizvajalca v zvezi s spremembo omejene na bistveno spremenjene dele.

5. **OBDOBJE PODPORE**

125. Na podlagi člena 13(8) akta o kibernetski odpornosti se od proizvajalcev zahteva, da določijo obdobje podpore, v katerem se ranljivosti izdelka z digitalnimi elementi, vključno z njegovimi sestavnimi deli, obravnavajo učinkovito in v skladu z bistvenimi zahtevami iz dela II Priloge I. Obdobje podpore odraža obdobje, v katerem se pričakuje, da se bo izdelek z digitalnimi elementi uporabljal (pričakovani čas uporabe), in bi ga bilo treba določiti glede na merila iz člena 13(8), zlasti razumna pričakovanja uporabnikov, naravo izdelka z digitalnimi elementi, vključno z njegovim predvidenim namenom, ter ustrezno pravo Unije, ki določa življenjsko dobo izdelkov z digitalnimi elementi ([17]). Na splošno je treba takšna merila pri določitvi obdobja podpore upoštevati na način, ki zagotavlja sorazmernost.

([17]) Dodatna merila, ki se lahko v skladu s členom 13(8) upoštevajo, vključujejo obdobja podpore za izdelke z digitalnimi elementi, ki ponujajo podobno funkcionalnost in jih dajo na trg drugi proizvajalci, razpoložljivost delovnega okolja, obdobja podpore za integrirane sestavne dele, ki zagotavljajo osnovne funkcije in so pridobljeni od tretjih oseb, ter ustrezne usmeritve, ki jih zagotovita skupina za upravno sodelovanje na področju akta o kibernetski odpornosti in Komisija.

126. S členom 13(8) se tudi zahteva, da obdobje podpore traja vsaj pet let, razen če se pričakuje, da se bo izdelek z digitalnimi elementi uporabljal manj kot pet let; v tem primeru obdobje podpore ustreza pričakovanemu času uporabe. Minimalno obdobje podpore zato deluje le kot zaščitni ukrep, ki zagotavlja, da se ranljivosti obravnavajo dovolj dolgo, proizvajalcem pa hkrati omogoča, da upoštevajo izdelke z digitalnimi elementi z dejansko krajšim pričakovanim časom uporabe. Uvodna izjava 60 vsebuje dodatne usmeritve v zvezi s tem, in sicer je pojasnjeno, da bi morali imeti izdelki z digitalnimi elementi, za katere se upravičeno pričakuje, da se bodo uporabljali dlje kot pet let, ustrezno daljša obdobja podpore. Petletno obdobje podpore se zato ne sme šteti za privzeto obdobje za vse izdelke z digitalnimi elementi. Proizvajalec bi moral ustrezno obdobje podpore določiti glede na merila iz člena 13(8).

127. Člen 13(19) od proizvajalcev zahteva, da ob nakupu na jasen in razumljiv način navedejo končni datum obdobja podpore (vsaj mesec in leto). Od proizvajalcev zahteva tudi, da uporabnikom prikažejo obvestilo, ko se obdobje podpore izteče, kadar je to tehnično izvedljivo glede na naravo izdelka z digitalnimi elementi. Namen te obveznosti je uporabnikom zagotoviti preglednost glede trajanja obdobja, v katerem lahko pričakujejo varnostno podporo.

128. Pri programskih izdelkih z digitalnimi elementi, ki se pogosto razvijajo in izdajajo ponavljajoče ter katerih bistveno spremenjene različice se lahko skozi čas pogosto dajejo na trg, je treba obdobje podpore razumeti glede na ta razvojni model. Vsaka bistveno spremenjena različica programskega izdelka z digitalnimi elementi, ki je dana na trg, mora imeti navedeno obdobje podpore, ki je v skladu s členom 13(8). To vključuje minimalno petletno obdobje podpore, razen če je pričakovani čas uporabe zadevne različice dokazljivo krajši, kot je pojasnjeno tudi v uvodni izjavi 60. V oddelku *5.1 Substantial modifications and the support period* je nadalje pojasnjeno, da kadar bistvena sprememba ne povzroči sprememb dejavnikov, na podlagi katerih se je prvotno določil pričakovani čas uporabe izdelka z digitalnimi elementi, ostane prvotno obdobje podpore nespremenjeno (tj. tudi v primerih, ko je preostalo obdobje podpore krajše od petih let).

129. Člen 13(10) zagotavlja prožnost za programske izdelke z digitalnimi elementi, saj proizvajalcem pod določenimi pogoji omogoča, da skladnost z zahtevo glede obravnavanja ranljivosti iz točke 2 dela II Priloge I (obravnavanje in odpravljanje ranljivosti) zagotovijo samo za različico programskega izdelka z digitalnimi elementi, ki je bila nazadnje dana na trg. To je dovoljeno, kadar imajo uporabniki različic, ki so bile predhodno dane na trg, brezplačen dostop do različice, ki je bila nazadnje dana na trg, in nimajo dodatnih stroškov zaradi prilagoditve okolja strojne in programske opreme, v katerem uporabljajo prvotno različico tega izdelka.

130. Za namene člena 13(10) bi bilo treba pojem „dodatni stroški“ razlagati praktično in sorazmerno, ob upoštevanju običajnih in pričakovanih praks pri vzdrževanju in delovanju programske opreme. Pojem ne zajema razumnega operativnega napora, ki je neločljivo povezan z uporabo posodobitev programske opreme ali vzdrževanjem varnega okolja delovanja, kot so čas osebja, rutinsko preskušanje, prilagoditve konfiguracije ali nadgradnje osnovnih odvisnosti programske opreme, ki so potrebne za obravnavanje sestavnih delov ob koncu življenjske dobe ali znanih varnostnih ranljivosti. Nasprotno pa se „dodatni stroški“ nanašajo na bremena, ki presegajo to, kar je mogoče običajno pričakovati v okviru posodobitev programske opreme, kot so obvezni nakupi nove strojne opreme, zamenjava infrastrukture ali temeljne spremembe okolja delovanja.

131. Pri stalno razvijajočih se programskih izdelkih z digitalnimi elementi lahko proizvajalci v razmeroma kratkih časovnih presledkih na trg dajejo zaporedne bistveno spremenjene različice in pričakujejo, da jih bodo uporabniki redno nadgrajevali. V takih primerih mora biti v skladu s členom 13(8) obdobje podpore za vsako bistveno spremenjeno različico navedeno ob dajanju na trg. Povedano drugače, proizvajalec mora za tako bistveno spremenjeno različico navesti novo obdobje podpore. Vendar lahko proizvajalci na podlagi člena 13(10) prenehajo obravnavati in odpravljati ranljivosti prejšnjih različic, ko lahko uporabniki izdelek brezplačno nadgradijo na

poznejšo različico in brez dodatnih stroškov, kot je navedeno zgoraj, tudi če je zaradi tega dejansko obdobje podpore za prejšnje različice krajše ([18]). Za proizvajalca še naprej veljajo druge zahteve glede obravnavanja ranljivosti iz dela II Priloge I in obveznosti poročanja iz člena 14. Kot je pojasnjeno tudi v uvodni izjavi 40, te zahteve za vse nadaljnje bistveno spremenjene različice programskega izdelka z digitalnimi elementi, dane na trg, med drugim vključujejo naslednje: (i) vzdrževanje politike usklajenega razkrivanja ranljivosti in (ii) ukrepe za lažjo izmenjavo informacij o morebitnih ranljivostih ([19]).

Primer 52: proizvajalec da na trg EU model pametnega telefona in navede obdobje podpore X let od datuma dajanja na trg, v katerem bo zagotavljal varnostne posodobitve za obravnavanje ranljivosti. V tem obdobju proizvajalec izdaja redne posodobitve programske opreme in bistveno spremenjene različice operacijskega sistema, ki jih lahko uporabniki namestijo brezplačno, ne da bi bila potrebna nova strojna oprema.

Proizvajalec lahko v skladu s členom 13(10) obravnava in odpravlja ranljivosti najnovejše različice operacijskega sistema, ki je na voljo za ta model pametnega telefona, pod pogojem, da se prejšnje različice lahko nadgradijo brezplačno in brez dodatnih stroškov. Med obdobjem podpore za proizvajalca še naprej veljajo druge zahteve glede obravnavanja ranljivosti, kot so usklajeno razkrivanje ranljivosti in ukrepi za izmenjavo informacij.

Primer 53: proizvajalec da na trg programski izdelek z digitalnimi elementi za podjetja in vsakih nekaj mesecev izda bistveno spremenjene različice, ki odražajo varnostne izboljšave, nove funkcije in združljivost s posodobljenimi operacijskimi sistemi in platformami. Vsaka različica se da na trg z navedenim obdobjem podpore v skladu s členom 13(8). Proizvajalec pričakuje, da bodo uporabniki izdelek redno nadgrajevali v okviru običajnega delovanja, in jim brezplačno zagotavlja dostop do najnovejše različice. Uporaba nadgradenj lahko zahteva razumen operativni napor, kot so preskušanje ali prilagoditve konfiguracije, niso pa potrebni dodatni stroški, na primer nakup nove strojne opreme ali temeljne spremembe infrastrukture. V tem okviru lahko proizvajalec na podlagi člena 13(10) preneha obravnavati in odpravljati ranljivosti prejšnjih različic, ko lahko uporabniki izdelek nadgradijo na najnovejšo različico, hkrati pa še naprej izpolnjuje druge zahteve glede obravnavanja ranljivosti vseh nadaljnjih bistveno spremenjenih različic.

5.1 **Bistvene spremembe in obdobje podpore**

132. Kot je navedeno v oddelku 4.4 *Consequences of a substantial modification,* se v primeru, kadar se sprememba izdelka z digitalnimi elementi šteje za bistveno spremembo in je spremenjeni izdelek z digitalnimi elementi dostopen na trgu, ta izdelek za namene akta o kibernetski odpornosti obravnava kot nov izdelek, dejanje dajanja bistveno spremenjenega izdelka z digitalnimi elementi na trg pa pomeni novo dajanje na trg. Zato je koristno pojasniti učinek, ki ga ima to novo dajanje na trg na obdobje podpore bistveno spremenjenega izdelka z digitalnimi elementi.

133. Obdobje podpore bistveno spremenjenega izdelka z digitalnimi elementi bi bilo treba določiti glede na pričakovani čas uporabe tega izdelka, ob upoštevanju meril iz člena 13(8) akta o kibernetski odpornosti. Zaradi bistvene spremembe bi bilo torej treba opraviti ponovno oceno glede na navedena merila, vendar ta sprememba ne povzroči, da se obdobje podpore samodejno ponovno določi ali celo podaljša. Ustrezno vprašanje je, ali bistvena sprememba vpliva na dejavnike, na podlagi katerih je bil prvotno določen pričakovani čas uporabe izdelka in s tem prvotno obdobje podpore.

([18]) Opozoriti je treba, da člen 13(19) od proizvajalcev zahteva, da, kadar je to tehnično izvedljivo glede na naravo izdelka z digitalnimi elementi, uporabnikom prikažejo obvestilo, v katerem jih obvestijo, da je njihov izdelek z digitalnimi elementi dosegel konec obdobja podpore. Kadar se torej obravnavanje in odpravljanje ranljivosti za prejšnje različice preneha, se pričakuje, da so uporabniki, ki izdelka niso nadgradili na najnovejšo različico, obveščeni, če je to tehnično izvedljivo.

([19]) Opozoriti je treba, da se lahko proizvajalci, kadar uporabniki izdelek lahko nadgradijo na najnovejšo različico programske opreme brez dodatnih stroškov, kljub temu odločijo, da bodo še naprej obravnavali in odpravljali ranljivosti prejšnjih različic te programske opreme, tudi proti plačilu ali v okviru drugih poslovnih dogovorov. Akt o kibernetski odpornosti ne določa, da morajo proizvajalci za take prejšnje različice brezplačno zagotavljati varnostne posodobitve.

134. Kadar bistvena sprememba ne vpliva na navedene dejavnike, je glede na merila iz člena 13(8) pričakovani čas uporabe enak, kot je bil prvotno določen, obdobje podpore spremenjenega izdelka z digitalnimi elementi pa bi moralo biti usklajeno s preostalim pričakovanim časom uporabe izdelka, kot je bil določen, ko je bil izdelek prvotno dan na trg. To običajno velja, kadar je bil pričakovani čas uporabe določen predvsem na podlagi dejavnikov, ki se zaradi spremembe ne spremenijo, kot je fizična trajnost sestavnih delov strojne opreme, in kadar se bistvena sprememba nanaša samo na programsko funkcionalnost ali zaledne storitve.

Primer 54: *proizvajalec da na trg robotski sesalnik s pričakovanim časom uporabe X let, določenim na podlagi narave izdelka z digitalnimi elementi, vključno s fizično trajnostjo in značilnostmi obrabe sestavnih delov strojne opreme, ter ob upoštevanju razumnih pričakovanj uporabnikov glede življenjske dobe tega izdelka. Proizvajalec določi obdobje podpore X let. Po Y letih izda posodobitev programske opreme, ki se šteje za bistveno spremembo, saj doda nove načine čiščenja in navigacijske funkcije. Posodobitev programske opreme ne vpliva na fizično trajnost strojne opreme in ne povzroči spremembe razumnih pričakovanj uporabnikov glede življenjske dobe navedenega izdelka. Zato je glede na merila iz člena 13(8) pričakovani čas uporabe še naprej enak. Obdobje podpore spremenjenega izdelka z digitalnimi elementi je usklajeno s preostalim pričakovanim časom uporabe, kot je bil prvotno določen.*

Primer 55: proizvajalec da na trg kompleksen izdelek z digitalnimi elementi v obliki industrijskega stroja z oblačnim zaledjem kot rešitvijo za daljinsko obdelavo podatkov. Pričakovani čas uporabe je X let in je določen ob upoštevanju razumnih pričakovanj uporabnikov in narave izdelka z digitalnimi elementi, kot sta fizična trajnost strojne opreme stroja in pričakovana obraba. Obdobje podpore je določeno tako, da je usklajeno s pričakovanim časom uporabe X let. Proizvajalec po Y letih preoblikuje arhitekturo oblačnega zaledja (rešitve za daljinsko obdelavo podatkov) z uvedbo novih vmesnikov za aplikacijsko programiranje in podatkovnih tokov, in sicer tako, da se to šteje za bistveno spremembo izdelka z digitalnimi elementi, ne spremeni pa narave tega izdelka niti ne vpliva na pričakovanja uporabnikov. Zato je glede na merila iz člena 13(8) pričakovani čas uporabe še naprej enak. Obdobje podpore spremenjenega izdelka z digitalnimi elementi je usklajeno s preostalim pričakovanim časom uporabe, kot je bil prvotno določen.

135. Kadar bistvena sprememba vpliva na dejavnike, na podlagi katerih je bil prvotno določen pričakovani čas uporabe izdelka z digitalnimi elementi, bi moral proizvajalec ponovno izračunati obdobje podpore, da bi odražalo novi pričakovani čas uporabe, pri čemer ustrezno uporabi merila iz člena 13(8). To lahko na primer velja za spremembe za obnovo strojne opreme, s katerimi se podaljša obratovalna življenjska doba zadevnega izdelka, ali za bistveno reprogramiranje ali prepis jedrne programske opreme izdelka, ki bistveno spremeni njegov pričakovani čas uporabe ([20]).

Primer 56: proizvajalec da na trg programirljivi logični krmilnik s pričakovanim časom uporabe X let, določenim predvsem na podlagi narave izdelka z digitalnimi elementi in trajnosti osnovne strojne opreme. Obdobje podpore se določi temu ustrezno. Proizvajalec več let po prvotnem dajanju na trg izdelek bistveno spremeni, in sicer vgrajeno računalniško platformo programirljivega logičnega krmilnika, vključno s procesorjem, pomnilnikom in izvajalnim okoljem, zamenja z novo generacijo sestavnih delov, zasnovanih za bistveno daljšo obratovalno dobo. Zaradi spremembe se razumna pričakovanja uporabnikov in narava izdelka z digitalnimi elementi spremenijo: uporabnik programirljivega logičnega krmilnika lahko zdaj upravičeno pričakuje, da bo programirljivi logični krmilnik ob podpori nove računalniške platforme ostal v produktivni uporabi tudi po prvotno navedenem pričakovanem času uporabe. Na podlagi meril iz člena 13(8) je zato pričakovani čas uporabe daljši, proizvajalec pa obdobje podpore za ta konkretni krmilnik ustrezno ponovno izračuna.

6. **POMEMBNI IN KRITIČNI IZDELKI Z DIGITALNIMI ELEMENTI**

136. Člen 7(1) akta o kibernetski odpornosti določa, da se izdelki z digitalnimi elementi, ki imajo osnovno funkcijo kategorije izdelkov iz Priloge III k Uredbi, štejejo za „pomembne izdelke z digitalnimi elementi“. V Prilogi III so pomembni izdelki z digitalnimi elementi nadalje razdeljeni na razred I in razred II. Podobno člen 8(1) določa, da se izdelki z digitalnimi elementi, ki imajo osnovno funkcijo kategorije izdelkov iz Priloge IV k aktu o kibernetski odpornosti, štejejo za „pomembne izdelke z digitalnimi elementi“ ([21]).

([20]) Opozoriti je treba, da se, kot je navedeno v oddelku *4.1 Physical repairs,* prenova, vzdrževanje ali popravila na splošno ne štejejo za bistvene spremembe.

([21]) Izvedbena uredba Komisije (EU) 2025/2392 določa tehnični opis kategorij pomembnih in kritičnih izdelkov.

137. Razvrstitev izdelka z digitalnimi elementi kot pomembnega ali kritičnega ali, nasprotno, kot izdelka, ki spada v „privzeto“ kategorijo ([22]), je pomembna pri določanju postopka ugotavljanja skladnosti, ki ga mora proizvajalec upoštevati v skladu s členom 32, preden lahko navedeni izdelek z digitalnimi elementi da na trg. Za izdelke z digitalnimi elementi iz privzete kategorije se lahko vedno uporabi postopek notranje kontrole na podlagi modula A („samoocenjevanje“) ([23]). Za pomembne izdelke z digitalnimi elementi razreda I ali II in kritične izdelke z digitalnimi elementi veljajo strožji postopki ugotavljanja skladnosti. To ne velja za pomembne izdelke z digitalnimi elementi razreda I ali II, ki se štejejo za prosto in odprtokodno programsko opremo ter so dani na trg, pri katerih lahko proizvajalci v skladu s členom 32(5) uporabijo postopke privzete kategorije.

138. Pojem osnovne funkcije je zato bistven, da proizvajalec določi veljavni režim ugotavljanja skladnosti. Vendar ta pojem v aktu o kibernetski odpornosti ni izrecno opredeljen. Izdelki z digitalnimi elementi lahko opravljajo različne funkcije, od katerih so nekatere lahko pomožne glede na osnovno funkcijo takega izdelka in ne bi smele vplivati na razvrstitev izdelka med izdelke iz privzete kategorije/pomembne izdelke razreda I/pomembne izdelke razreda II/kritične izdelke. Zato je koristno zagotoviti dodatne usmeritve za pomoč proizvajalcem pri pravilnem izvajanju ustreznih postopkov ugotavljanja skladnosti, organom za nadzor trga pa pri zagotavljanju usklajenega izvrševanja akta o kibernetski odpornosti po vsej EU.

6.1 **Osnovna funkcija**

139. Osnovna funkcija izdelka z digitalnimi elementi pomeni glavne značilnosti in tehnične zmogljivosti takega izdelka, brez katerih ta ne bi mogel izpolniti svojega predvidenega namena. Oceni se lahko ob upoštevanju posebnih okoliščin in pogojev uporabe izdelka, pri čemer se med drugim upoštevajo informacije, ki jih proizvajalec navede v navodilih za uporabo, promocijskem ali prodajnem gradivu in izjavah ter v tehnični dokumentaciji.

Primer 57: programski izdelek z digitalnimi elementi zagotavlja abstrakcijsko raven nad osnovno strojno opremo in upravlja izvajanje sestavnih delov programske opreme. Njegove glavne značilnosti vključujejo inicializacijo strojne opreme in zunanjih naprav, upravljanje procesov in pomnilnika, upravljanje vhoda in izhoda, časovno načrtovanje, dodeljevanje virov ter izpostavljanje sistemskih storitev in vmesnikov za aplikacijsko programiranje, prek katerih aplikacije komunicirajo z viri strojne in programske opreme naprave. V tehnični dokumentaciji je navedeno, da izdelek z digitalnimi elementi usklajuje računalniške vire, uveljavlja sistemske konfiguracije in zagotavlja standardizirane vmesnike za programske module in povezane zunanje naprave. Proizvajalec poudarja, da te zmogljivosti platformi omogočajo, da deluje kot osrednje programsko okolje, v katerem se lahko aplikacije zanesljivo izvajajo. Izdelek z digitalnimi elementi ima osnovno funkcijo operacijskega sistema, kot je opisana v točki 11 Priloge I k Izvedbeni uredbi (EU) 2025/2392.

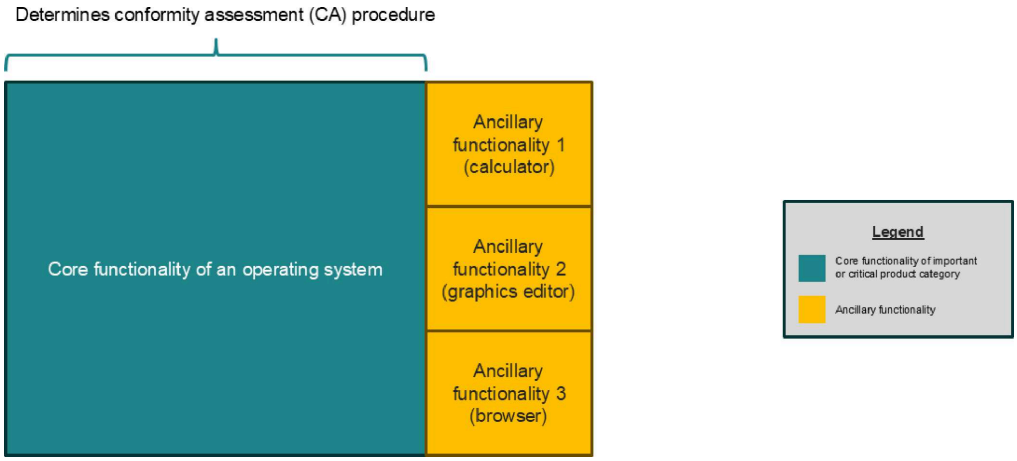
140. Funkcija izdelka z digitalnimi elementi je redko omejena izključno na njegovo osnovno funkcijo, saj izdelki z digitalnimi elementi pogosto – če ne vedno – opravljajo dodatne funkcije, ki ne prispevajo k osnovni funkciji izdelka. To lahko vključuje tudi vgradnjo sestavnih delov, ki imajo sami funkcijo drugega pomembnega ali kritičnega izdelka z digitalnimi elementi. Vendar dejstvo, da izdelek z digitalnimi elementi opravlja funkcije, ki niso navedene v tehničnih opisih pomembnih ali kritičnih izdelkov z digitalnimi elementi ali jih opravlja poleg navedenih funkcij, samo po sebi ne preprečuje, da bi imel izdelek eno tako osnovno funkcijo.

([22]) Izraz „privzeta“ kategorija v aktu o kibernetski odpornosti ni opredeljen. Uporaba izraza v tem dokumentu se nanaša na izdelke z digitalnimi elementi, ki nimajo osnovne funkcije kategorije izdelkov iz Priloge III ali IV k aktu o kibernetski odpornosti in za katere posledično velja režim ugotavljanja skladnosti iz člena 32(1).

([23]) Proizvajalec se lahko kljub temu vedno odloči, da bo uporabil strožji postopek ugotavljanja skladnosti, kot je določeno v členu 32(1).

Slika 2

Prikaz, kako se veljavni postopek ugotavljanja skladnosti določi glede na osnovno funkcijo in ne glede na pomožne funkcije



141. Izdelek z digitalnimi elementi je lahko zmožen opravljati funkcije kategorije pomembnih ali kritičnih izdelkov, vendar ima kljub temu osnovno funkcijo, ki se razlikuje od osnovne funkcije take kategorije izdelkov. V teh primerih se navedeni izdelek z digitalnimi elementi ne bi štel za pomemben ali kritičen izdelek z digitalnimi elementi. Kot je izrecno navedeno v členu 7(1) akta o kibernetski odpornosti v zvezi s pomembnimi izdelki z digitalnimi elementi (pri čemer se enaka logika uporablja za kritične izdelke z digitalnimi elementi), zgolj vgradnja pomembnega ali kritičnega izdelka z digitalnimi elementi sama po sebi ne pomeni, da je izdelek z digitalnimi elementi pomemben ali kritičen izdelek z digitalnimi elementi.

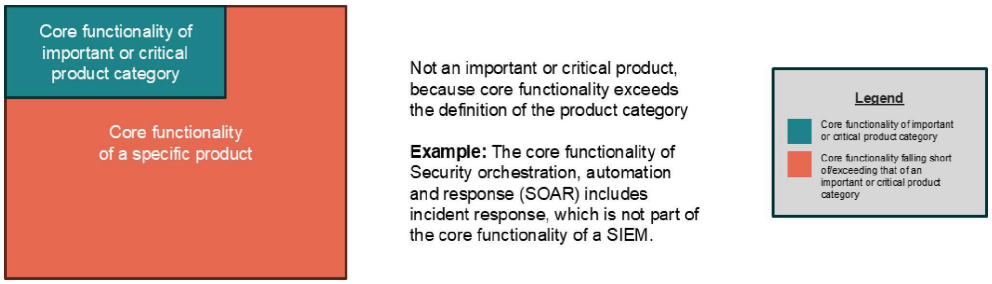
Primer 58: pametni telefon vključuje operacijski sistem, ki zagotavlja funkcije, opisane v točki 11 Priloge I k Izvedbeni uredbi (EU) 2025/2392. Čeprav operacijski sistem omogoča upravljanje virov strojne opreme in izvajanje aplikacij, ima pametni telefon kot celota drugačno osnovno funkcijo (npr. uporabnikom omogoča, da komunicirajo ter dostopajo do informacij in storitev). Sama vgradnja operacijskega sistema ne pomeni, da ima pametni telefon osnovno funkcijo operacijskega sistema.

142. Nekateri izdelki z digitalnimi elementi so lahko podobni kategoriji pomembnih ali kritičnih izdelkov ali spadajo v isto splošno družino izdelkov, vendar lahko njihova osnovna funkcija znatno presega osnovno funkcijo take kategorije ali je še zdaleč ne dosega. To ne velja, kadar izdelek z digitalnimi elementi vključuje dodatne funkcije, ki zgolj dopolnjujejo ali izboljšujejo osnovno funkcijo, ta pa ustreza osnovni funkciji kategorije pomembnih ali kritičnih izdelkov; v takih primerih izdelek z digitalnimi elementi ohrani osnovno funkcijo zadevne kategorije in se ustrezno razvrsti. Ta ocena bi morala temeljiti na glavnih značilnostih in tehničnih zmogljivostih zadevnega izdelka, ki se objektivno obravnavajo glede na njegov predvideni namen, in ne na tem, kako je izdelek z digitalnimi elementi opisan ali se trži, kadar ta opis ne odraža njegovih dejanskih tehničnih značilnosti.

Primer 59: programska oprema za varnostno organizacijo, avtomatizacijo in odzivanje lahko na primer pogosto opravlja funkcije izdelkov z digitalnimi elementi v kategoriji „varnostni sistem za upravljanje informacij in dogodkov“, tj. zbira podatke iz več virov, jih analizira in povezuje ter predstavlja kot uporabne informacije za varnostne namene. Vendar osnovna funkcija te programske opreme znatno presega funkcijo varnostnega sistema za upravljanje informacij in dogodkov, saj kot osrednje elemente svojih tehničnih zmogljivosti vključuje storitve, kot je odzivanje na incidente. Zato se za programsko opremo za varnostno organizacijo, avtomatizacijo in odzivanje na splošno ne šteje, da ima osnovno funkcijo varnostnih sistemov za upravljanje informacij in dogodkov.

Slika 3

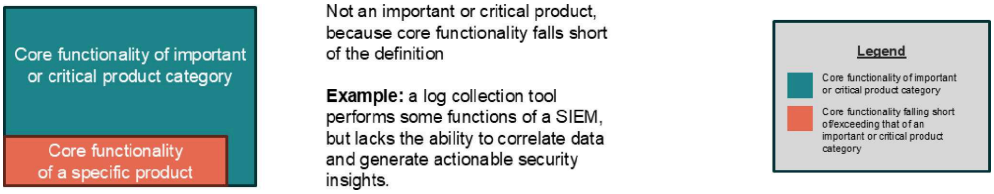
Prikaz osnovne funkcije izdelka z digitalnimi elementi, ki znatno presega opredelitev kategorije pomembnih ali kritičnih izdelkov



Primer 60: nekatera orodja za zbiranje in vizualizacijo dnevnikov lahko črpajo dnevniške podatke in prikazujejo osnovne nadzorne plošče, ki prikazujejo sistemske dogodke. Čeprav lahko ta orodja podpirajo dejavnosti spremljanja varnosti, njihova osnovna funkcija ne dosega osnovne funkcije varnostnih sistemov za upravljanje informacij in dogodkov, saj ne izvajajo korelacije podatkov niti ne zagotavljajo uporabnih varnostnih vpogledov. Zato se za taka orodja na splošno ne šteje, da imajo osnovno funkcijo varnostnih sistemov za upravljanje informacij in dogodkov.

Slika 4

Prikaz osnovne funkcije izdelka z digitalnimi elementi, ki še zdaleč ne dosega opredelitve kategorije pomembnih ali kritičnih izdelkov

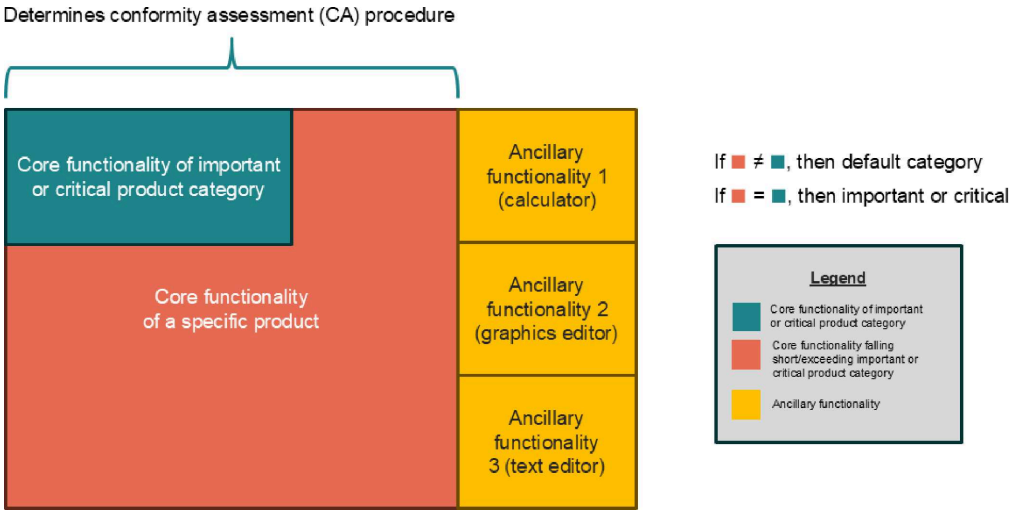


143. Proizvajalec ne sme napačno predstavljati osnovne funkcije svojega izdelka z digitalnimi elementi tako, da bi se izognil režimu ugotavljanja skladnosti, ki se uporablja za pomembne ali kritične izdelke z digitalnimi elementi, npr. s pretiranim poudarjanjem ali zmanjševanjem pomena vloge določenih funkcij, zaradi česar bi izdelek bistveno presegal določeno osnovno funkcijo ali je še zdaleč ne dosegal. To bi na primer veljalo, kadar obstajajo očitne nedoslednosti med promocijskim gradivom, navodili za uporabo in tehnično dokumentacijo.

144. Izdelek z digitalnimi elementi za namene določanja veljavnega režima ugotavljanja skladnosti ne sme imeti več kot ene osnovne funkcije. V skladu s Prilogo VII k aktu o kibernetski odpornosti morajo proizvajalci v okviru tehnične dokumentacije izdelka opisati predvideni namen svojega izdelka z digitalnimi elementi in postopek ugotavljanja skladnosti, ki so ga opravili. Osnovna funkcija izdelka bi morala biti zato jasno opredeljena. To omogoča pravilno identifikacijo veljavnega režima ugotavljanja skladnosti ter organom za nadzor trga omogoča, da nadzorujejo in preverijo, ali se Uredba pravilno uporablja.

Slika 5

Prikaz, kako se glede na osnovno funkcijo določenega izdelka z digitalnimi elementi določi razred izdelka in s tem veljavni postopek ugotavljanja skladnosti



145. Nekateri izdelki z digitalnimi elementi se dajo na trg kot enotni izdelki z digitalnimi elementi, vendar so sestavljeni iz ločenih modulov z ločenimi funkcijami. Kadar proizvajalec omogoči dostopnost teh modulov na trgu tudi ločeno, na primer so na voljo ločeno za nakup, pridobitev licence ali naročnino, ti moduli sami po sebi pomenijo samostojne izdelke z digitalnimi elementi. Kot take jih je treba razvrstiti na podlagi njihovih osnovnih funkcij (zato zanje velja ustrezen režim ugotavljanja skladnosti na podlagi osnovne funkcije posameznega modula). To ne posega v primere, ko se moduli dobavljajo izključno kot sestavni deli integriranega izdelka z digitalnimi elementi in niso na voljo ločeno; v takih primerih se osnovna funkcija določi na ravni integriranega izdelka z digitalnimi elementi.

Primer 61: proizvajalec da na trg poenoten varnostni paket, ki združuje več modulov, vključno z varnostnim sistemom za upravljanje informacij in dogodkov, sistemom za zaznavanje vdorov in analitičnim modulom. Proizvajalec navedene module ponuja tudi za ločeno naročnino. V tem scenariju je vsak modul ločen izdelek z digitalnimi elementi in se razvrsti na podlagi osnovne funkcije. Za modul varnostnega sistema za upravljanje informacij in dogodkov se uporablja režim ugotavljanja skladnosti za pomembne izdelke z digitalnimi elementi razreda I, saj je njegova osnovna funkcija funkcija „varnostnih sistemov za upravljanje informacij in dogodkov“. Za sistem za zaznavanje vdorov se uporablja režim ugotavljanja skladnosti za pomembne izdelke z digitalnimi elementi razreda II, saj je njegova osnovna funkcija funkcija kategorije „požarni zidovi, sistemi za zaznavanje in preprečevanje vdorov“. Za analitični modul se uporablja režim ugotavljanja skladnosti za „privzete“ izdelke z digitalnimi elementi, saj njegova osnovna funkcija ni funkcija kategorije pomembnih ali kritičnih izdelkov.

146. Neizpolnjevanje obveznosti iz člena 32 akta o kibernetski odpornosti lahko povzroči upravne globe v skladu s členom 64(3).

6.2 Ugotavljanje skladnosti pomembnih in kritičnih izdelkov z digitalnimi elementi

147. Ko proizvajalec določi osnovno funkcijo svojega izdelka z digitalnimi elementi, mora izvesti enega od veljavnih postopkov ugotavljanja skladnosti. Zagotoviti mora, da izdelek z digitalnimi elementi kot celota izpolnjuje bistvene zahteve, pri čemer po potrebi upošteva varnost vgrajenih sestavnih delov ali funkcij.

148. Strožji postopek ugotavljanja skladnosti, pri katerem sodeluje tretja oseba (na podlagi modulov B + C, modula H ali certifikacijskih shem za kibernetsko varnost), je obvezen za pomembne izdelke z digitalnimi elementi razreda II (razen tistih, ki se štejejo za prosto in odprtokodno programsko opremo v skladu s členom 32(5)) in za kritične izdelke z digitalnimi elementi ([24]). Nasprotno pa morajo pomembni izdelki z digitalnimi elementi razreda I (razen tistih, ki se štejejo za prosto in odprtokodno programsko opremo v skladu s členom 32(5)) prestati postopek ugotavljanja skladnosti, ki ga opravi tretja oseba, samo, če proizvajalec ni uporabil ali ni v celoti uporabil ustreznih harmoniziranih standardov, sklici na katere so bili objavljeni v *Uradnem listu Evropske unije* (v nadaljnjem besedilu: harmonizirani standardi), skupnih specifikacij ali evropskih certifikacijskih shem za kibernetsko varnost na ravni zanesljivosti vsaj „znatno“ ([25]).

149. Da bi bil torej pomemben izdelek z digitalnimi elementi razreda I upravičen do postopka notranje kontrole, (i) je treba uporabiti vse veljavne zahteve ustreznega harmoniziranega standarda in (ii) področje uporabe standarda mora zajemati vsaj vsa tveganja za kibernetsko varnost, povezana z osnovno funkcijo tega izdelka.

150. Področje uporabe izdelka z digitalnimi elementi je lahko širše od področja uporabe, predvidenega z ustreznim harmoniziranim standardom, take dodatne funkcije pa lahko pomenijo drugačna ali dodatna tveganja za kibernetsko varnost. Proizvajalec mora vedno opraviti oceno tveganja na podlagi člena 13(2) in bi moral zato preveriti, ali izvajanje harmoniziranega standarda zajema vsa tveganja, povezana z izdelkom z digitalnimi elementi. Kadar izvajanje standarda ne zajema vseh tveganj, bi moral proizvajalec na drug način zagotoviti, da je njegov izdelek z digitalnimi elementi skladen z bistvenimi zahtevami.

151. Če je torej proizvajalec pomembnega izdelka z digitalnimi elementi razreda I uporabil ustrezen harmonizirani standard, ki zajema tveganja, povezana z osnovno funkcijo tega izdelka, se lahko odloči za uporabo postopka notranje kontrole za dokazovanje skladnosti svojega izdelka. Proizvajalec bo moral v okviru svojih dejavnosti ugotavljanja skladnosti še vedno dokazati, da so obravnavana vsa tveganja, povezana z njegovim izdelkom z digitalnimi elementi. Zato mora proizvajalec, kadar obstaja vrzel med tem, kar je zajeto s harmoniziranim standardom, in področjem uporabe izdelka z digitalnimi elementi kot celote, še vedno dokumentirati, katere dodatne ukrepe je uvedel za obravnavanje teh tveganj.

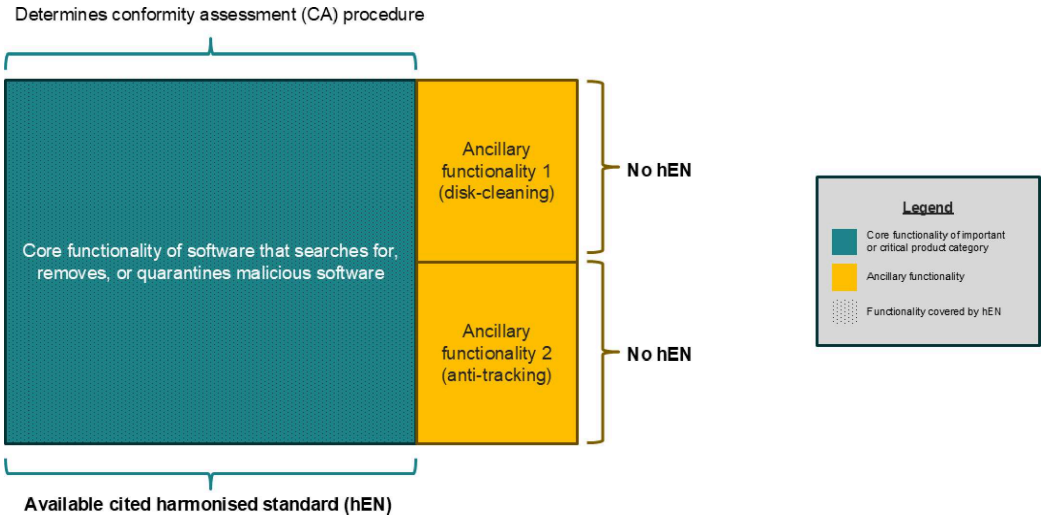
Primer 62: protivirusna programska oprema ima osnovno funkcijo programske opreme, ki išče, odstranjuje ali daje v karanteno zlonamerno programsko opremo, kot je opisano v točki 4 Priloge I k Izvedbeni uredbi (EU) 2025/2392. Ta izdelek z digitalnimi elementi vključuje tudi dodatne funkcije, in sicer funkcijo čiščenja diska in funkcijo za preprečevanje sledenja pri potovanju po spletu. Proizvajalec izvede oceno tveganja, ki v celoti zajema izdelek z digitalnimi elementi, vključno z osnovno funkcijo protivirusne programske opreme, funkcijo čiščenja diska in funkcijo za preprečevanje sledenja. Pri tem uporabi harmonizirani standard, ki zajema tveganja, povezana z osnovno funkcijo protivirusne programske opreme, in dodatne ukrepe za obravnavanje tveganj, ki izhajajo iz dodatnih funkcij. Proizvajalcu je dovoljeno uporabiti postopek notranje kontrole pri ugotavljanju skladnosti izdelka z digitalnimi elementi kot celote, vključno s funkcijo čiščenja diska in funkcijo za preprečevanje sledenja.

([24]) To velja tudi pri uporabi evropske certifikacijske sheme za kibernetsko varnost na ravni zanesljivosti, ki je vsaj „znatna“, saj je potrebno sodelovanje certifikacijskega organa tretje osebe.

([25]) Zaradi jedrnatosti se preostanek tega oddelka nanaša le na harmonizirane standarde, sklici na katere so bili objavljeni v *Uradnem listu Evropske unije*. Vendar se iste usmeritve uporabljajo tudi za skupne specifikacije, sprejete v skladu s členom 27(2), in za evropske certifikacijske sheme za kibernetsko varnost, kadar Komisija to določi z delegiranimi akti v skladu s členom 27(9).

Slika 6

Ponazoritev, kako se na podlagi uporabe navedenega harmoniziranega standarda, ki zajema le osnovno funkcijo, določi veljavni postopek ugotavljanja skladnosti



152. To velja tudi, kadar izdelek z digitalnimi elementi vključuje dodatno funkcijo, ki je tudi sama funkcija drugega pomembnega ali kritičnega izdelka z digitalnimi elementi. Dejansko je osnovna funkcija izdelka z digitalnimi elementi kot celote, in ne funkcija vgrajenih sestavnih delov, obravnavanih ločeno, tista, ki določa, ali izdelek z digitalnimi elementi spada v kategorijo pomembnih ali kritičnih izdelkov (in s tem veljavni režim ugotavljanja skladnosti). Če ima izdelek z digitalnimi elementi na primer osnovno funkcijo pomembnega izdelka z digitalnimi elementi razreda I, za navedeni izdelek kot celoto velja režim ugotavljanja skladnosti, ki se uporablja za pomembne izdelke z digitalnimi elementi razreda I, čeprav vključuje sestavni del, ki je sam kritični izdelek z digitalnimi elementi. Kadar proizvajalec v teh primerih uporabi harmonizirani standard, ki zajema tveganja, povezana z osnovno funkcijo takega izdelka, lahko uporabi postopek notranje kontrole.

Primer 63: izdelek strojne opreme z digitalnimi elementi ima osnovno funkcijo usmerjevalnika, kot je opisano v točki 12 Priloge I k Izvedbeni uredbi (EU) 2025/2392. Ta izdelek z digitalnimi elementi vključuje tudi dodatne funkcije, med drugim zmogljivosti požarnega zidu, saj vključuje sestavni del požarnega zidu. Proizvajalec izvede oceno tveganja, ki v celoti zajema izdelek z digitalnimi elementi, vključno z osnovno funkcijo usmerjevalnika in funkcijo požarnega zidu. Pri tem uporabi harmonizirani standard, ki zajema tveganja, povezana z osnovno funkcijo usmerjevalnika, in dodatne ukrepe za obravnavanje tveganj, ki izhajajo iz dodatnih funkcij. Proizvajalec lahko na primer uporabi harmonizirani standard za požarne zidove, da zajame tveganja, povezana s funkcijo požarnega zidu. Proizvajalcu je dovoljeno uporabiti postopek notranje kontrole pri ugotavljanju skladnosti izdelka z digitalnimi elementi kot celote, vključno s funkcijo požarnega zidu.

6.3 Posledice za domnevo o skladnosti

153. V členu 27(1) akta o kibernetski odpornosti je določeno, da se za izdelke z digitalnimi elementi in postopke, ki jih je vzpostavil proizvajalec in ki so v skladu s harmoniziranimi standardi ali njihovimi deli, katerih sklici so bili objavljeni v *Uradnem listu Evropske unije*, domneva, da so skladni z bistvenimi zahtevami akta o kibernetski

odpornosti, določenimi v Prilogi I, iz teh standardov ali njihovih delov ([26]). Člen 27(5) isto domnevo o skladnosti razširja na izdelke z digitalnimi elementi in postopke, ki jih je vzpostavil proizvajalec in ki so v skladu s skupnimi specifikacijami, ki jih je Komisija sprejela z izvedbenimi akti, člen 27(8) pa določa domnevo o skladnosti za izdelke z digitalnimi elementi in postopke, ki jih je vzpostavil proizvajalec, za katere sta bila EU izjava o skladnosti ali certifikat izdana na podlagi evropske certifikacijske sheme za kibernetsko varnost, sprejete v skladu z Uredbo (EU) 2019/881, če je bilo to določeno z delegiranimi akti v skladu s členom 27(9) ([27]).

154. Kadar je torej proizvajalec uporabil harmonizirani standard, sklici na katerega so bili objavljeni v *Uradnem listu Evropske unije*, lahko izkoristi domnevo o skladnosti za tveganja, zajeta s tem standardom. To bi se lahko zgodilo, kadar navedeni harmonizirani standard obravnava vsa tveganja, povezana z osnovno funkcijo izdelka z digitalnimi elementi, in kadar ni dodatnih funkcij, ki bi pomenile tveganja za kibernetsko varnost. Pričakuje se na primer, da bo harmonizirani standard za usmerjevalnike obravnaval vsaj tveganja, povezana z osnovno funkcijo teh izdelkov z digitalnimi elementi. Če tak izdelek ne vsebuje nobenih dodatnih funkcij ali če te dodatne funkcije ne pomenijo tveganj, ki jih standard ne obravnava, lahko za izdelek z digitalnimi elementi velja domneva o skladnosti.

155. V primerih iz točk 151 in 152 je proizvajalcu dovoljeno uporabiti postopek notranje kontrole, ker harmonizirani standard zajema tveganja, povezana z osnovno funkcijo izdelka z digitalnimi elementi. Vendar lahko izdelki z digitalnimi elementi, opisani v navedenih primerih, presegajo področje uporabe harmoniziranih standardov, dodatne funkcije pa lahko pomenijo tveganja za kibernetsko varnost, ki jih tak harmonizirani standard ne obravnava. Za navedene izdelke z digitalnimi elementi zato morda ne velja domneva o skladnosti teh dodatnih funkcij.

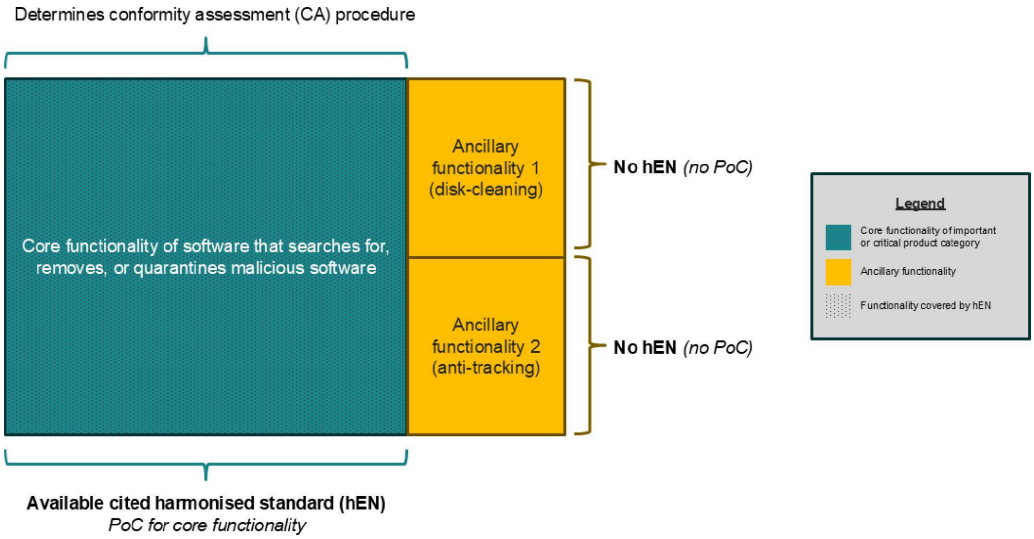
Primer 64: protivirusna programska oprema ima osnovno funkcijo programske opreme, ki išče, odstranjuje ali daje v karanteno zlonamerno programsko opremo, tveganja, povezana z navedeno osnovno funkcijo, pa so zajeta s harmoniziranim standardom. Ta izdelek z digitalnimi elementi vključuje tudi dodatne funkcije, in sicer funkcijo čiščenja diska in funkcijo za preprečevanje sledenja pri potovanju po spletu, katerih tveganja niso zajeta s harmoniziranim standardom. Če se harmonizirani standard uporabi, lahko proizvajalec pri ugotavljanju skladnosti uporabi postopek notranje kontrole. Domnevo o skladnosti bo lahko izkoristil za tveganja, povezana z osnovno funkcijo tega izdelka, ne pa tudi za tveganja, povezana z dodatnimi funkcijami.

([26]) Kot je jasno navedeno v oddelku 4.1.2.2 Modrega vodnika, „[p]ri harmonizacijski zakonodaji v zvezi s tveganji […] proizvajalci vedno, tudi kadar uporabljajo harmonizirane standarde, sklici na katere so objavljeni v *Uradnem listu Evropske unije*, ostanejo v celoti odgovorni za ocenjevanje vseh tveganj v zvezi z njihovim proizvodom, da ugotovijo, katere bistvene (ali druge) zahteve so ustrezne. Po tej oceni se lahko proizvajalec nato odloči, da bo uporabil tehnične specifikacije iz harmoniziranih standardov, sklici na katere so objavljeni v *Uradnem listu Evropske unije*, za izvajanje ‚ukrepov za zmanjševanje tveganja', ki so določeni v teh standardih."

([27]) Kot zgoraj se zaradi jedrnatosti preostanek tega oddelka nanaša le na harmonizirane standarde, sklici na katere so objavljeni v *Uradnem listu Evropske unije*. Vendar se iste usmeritve uporabljajo tudi za skupne specifikacije in evropske certifikacijske sheme za kibernetsko varnost.

Slika 7

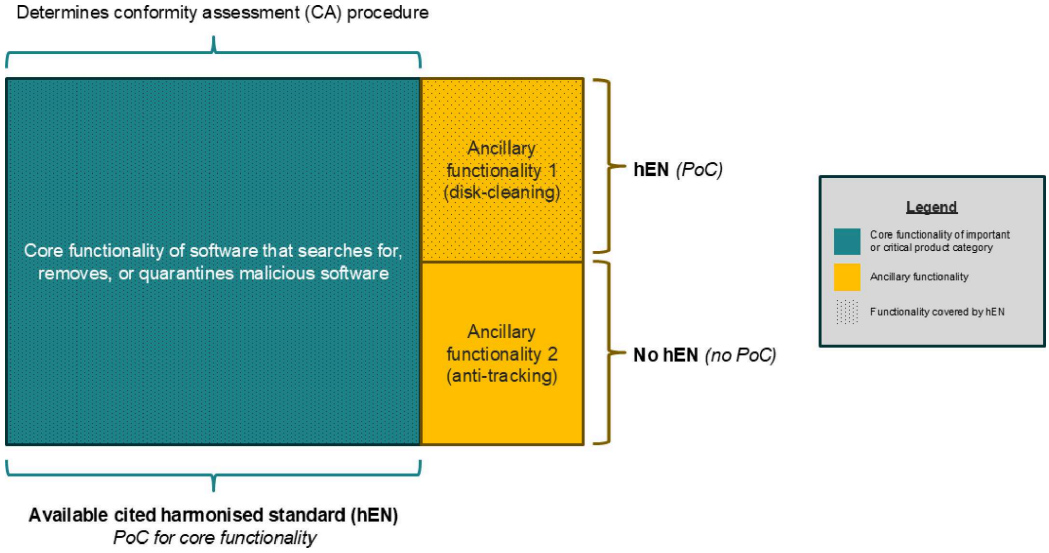
S harmoniziranim standardom se zagotavlja domneva o skladnosti za osnovno funkcijo, saj standard obravnava vsa tveganja, povezana s to osnovno funkcijo, ne pa tudi za pomožni funkciji



Primer 65: v istem scenariju kot v prejšnjem primeru je bil harmonizirani standard zdaj posodobljen tako, da zajema tudi tveganja, povezana z eno od dodatnih funkcij, in sicer funkcijo čiščenja diska, ne pa z drugo (tj. funkcijo za preprečevanje sledenja). Če se harmonizirani standard uporabi, lahko proizvajalec pri ugotavljanju skladnosti uporabi postopek notranje kontrole. Domnevo o skladnosti bo lahko izkoristil za tveganja, povezana z osnovno funkcijo tega izdelka in funkcijo čiščenja diska, ne pa tudi za tveganja, povezana s funkcijo za preprečevanje sledenja.

Slika 8

S harmoniziranim standardom se zagotavlja domneva o skladnosti za osnovno funkcijo in pomožno funkcijo 1, saj standard obravnava vsa tveganja, povezana z navedenima funkcijama, ne pa tudi za pomožno funkcijo 2



7. **OCENA TVEGANJA ZA KIBERNETSKO VARNOST TER VGRADNJA IZDELKOV Z DIGITALNIMI ELEMENTI IN SESTAVNIMI DELI**

7.1 **O ocenjevanju in obravnavi tveganj za kibernetsko varnost**

156. Ocena tveganja za kibernetsko varnost iz člena 13(2) akta o kibernetski odpornosti od proizvajalcev zahteva, da opredelijo ustrezna tveganja in ocenijo njihov morebitni vpliv na izdelek z digitalnimi elementi. Proizvajalci morajo uvesti tudi ustrezne ukrepe za obravnavo teh tveganj v skladu z bistvenimi zahtevami iz Priloge I.

157. Pri obvladovanju tveganj v organizacijah se tveganja običajno ocenjujejo glede na merila za sprejemanje tveganj, ki izhajajo iz notranjih ciljev organizacije ali njene pripravljenosti prevzeti tveganje. Nasprotno pa bi bilo treba v okviru akta o kibernetski odpornosti preostalo tveganje za kibernetsko varnost oceniti ob upoštevanju zahteve, da izdelek z digitalnimi elementi, dan na trg, zagotavlja ustrezno raven kibernetske varnosti glede na tveganja, pri čemer se upoštevata njegov predvideni namen in razumno predvidljiva uporaba.

158. Zato notranje dopustno tveganje, poslovna strategija ali zgolj stroškovni vidiki proizvajalca niso pomembni pri ugotavljanju, ali so bila tveganja obravnavana. Za namene člena 13(2) in (3) morajo biti proizvajalci sposobni ugotoviti, ali so bila ugotovljena tveganja za kibernetsko varnost zadostno obravnavana z izpolnjevanjem bistvenih zahtev iz dela I Priloge I, ob upoštevanju predvidenega namena, razumno predvidljive uporabe in pogojev uporabe, vključno z operativnim okoljem (kot so predvideni uporabniki izdelka z digitalnimi elementi) in sredstvi, ki jih je treba zaščititi, ter ob upoštevanju trajanja pričakovane uporabe izdelka, kot je ustrezno.

159. Preostalo tveganje za kibernetsko varnost je neločljiv rezultat ocene tveganja in obravnave tveganja. Priznava se, da tveganj za kibernetsko varnost v praksi ni mogoče v celoti odpraviti. Vendar obstoj preostalega tveganja ne pomeni, da lahko proizvajalec po lastni presoji sprejme katero koli tveganje. Izdelek z digitalnimi elementi se lahko da na trg le, kadar so bila preostala tveganja po sprejetju ustreznih ukrepov zadostno obravnavana z izpolnjevanjem bistvenih zahtev, ob upoštevanju predvidenega namena in razumno predvidljive uporabe izdelka z digitalnimi elementi.

160. V skladu s členom 13(3) morajo proizvajalci, kadar se ugotovijo tveganja za kibernetsko varnost, ta tveganja obravnavati z ustreznimi ukrepi, tudi na ravni izdelka. Glede na okoliščine lahko to na primer vključuje zmanjšanje napadalne površine, izvajanje tehničnih zaščitnih ukrepov, omejitev ali prilagoditev funkcije ali natančnejšo opredelitev predvidenega namena izdelka z digitalnimi elementi. Proizvajalci lahko sprejmejo tudi ukrepe za izoblikovanje razumno predvidljive uporabe izdelka z digitalnimi elementi, na primer z obveščanjem o tveganjih, usmeritvami za uporabnike ali zasnovo uporabniškega vmesnika, da bi usmerjali vedenje uporabnikov k varnim vzorcem uporabe.

161. V aktu o kibernetski odpornosti ni določeno, da se proizvajalec pomanjkljivostim pri zasnovi proizvoda izogne tako, da tveganje za kibernetsko varnost ali odgovornost prenese na uporabnike ali tretje osebe, niti s tem upraviči neobravnavanja kibernetskih tveganj. Obveznost dati na trg varen izdelek z digitalnimi elementi in dokazati skladnost z bistvenimi zahtevami je še vedno odgovornost proizvajalca.

162. Informacije in navodila, ki se zagotovijo uporabnikom, se lahko uporabijo v podporo varni uvedbi in delovanju izdelka z digitalnimi elementi, tudi kadar se je proizvajalec odločil omejiti predvideni namen tega izdelka na zaupanja vredna okolja, ter za obveščanje uporabnikov o preostalih tveganjih na način, ki je ustrezen glede na naravo izdelka z digitalnimi elementi in njegove predvidene uporabnike.

Primer 66: proizvajalec razvije industrijski senzor za uporabo v zaupanja vrednih okoljih. Da bi senzor pravilno izvajal svojo funkcijo, proizvajalec ne izvede ukrepov za zaščito pred fizičnimi napadi na sam senzor. Da bi zmanjšal povezana tveganja, ugotovljena v oceni tveganja, proizvajalec predvideni namen senzorja omeji na uporabo zgolj v zaupanja vrednih okoljih, kjer je preprečen nepooblaščen fizični dostop do izdelka z digitalnimi elementi. Informacije in navodila za uporabnike vsebujejo jasne informacije o teh omejitvah uporabe senzorja na način, ki je ustrezen glede na naravo izdelka z digitalnimi elementi in njegove predvidene uporabnike.

Primer 67: proizvajalec razvije aplikacijo za poklicno uporabo na upravljanih namiznih in mobilnih napravah. Aplikacija obdeluje lokalno shranjene občutljive podatke in vsebino, ki jo ustvarijo uporabniki. Proizvajalec pri oceni tveganja ugotovi tveganje nepooblaščenega dostopa do takih podatkov, če se ti v napravi shranjujejo v nešifrirani obliki. Namesto da bi v sami aplikaciji zasnoval in izvedel lastniški mehanizem šifriranja, se proizvajalec odloči, da se bo zanesel na funkcije šifriranja in upravljanja ključev, ki jih izvorno zagotavlja operacijski sistem, na katerem naj bi aplikacija delovala, saj so vgrajene kriptografske storitve operacijskega sistema dobro uveljavljene in se redno vzdržujejo.

163. Kadar se pri oceni tveganja za kibernetsko varnost ugotovijo tveganja, ki jih ni mogoče zadovoljivo obravnavati z ustreznimi ukrepi, so lahko za doseganje skladnosti z aktom o kibernetski odpornosti potrebne spremembe zasnove, funkcije ali predvidenega namena izdelka z digitalnimi elementi. Vidiki, ki se nanašajo izključno na stroške ali komercialno izvedljivost, niso zadostna podlaga za to, da taka tveganja ostanejo neobravnavana, kadar bi to preprečilo, da bi izdelek z digitalnimi elementi izpolnjeval bistvene zahteve.

7.2 O zasnovi, razvoju in proizvodnji izdelkov z digitalnimi elementi na način, ki zagotavlja ustrezno raven kibernetske varnosti glede na tveganja

164. Bistvena zahteva glede kibernetske varnosti iz točke 1 dela I Priloge I k aktu o kibernetski odpornosti je, da so izdelki z digitalnimi elementi zasnovani, razviti in proizvedeni tako, da zagotavljajo ustrezno raven kibernetske varnosti glede na tveganja.

165. Namen te bistvene zahteve je obravnavati vsa tveganja za kibernetsko varnost, ugotovljena v oceni tveganja za kibernetsko varnost. To zlasti vključuje tveganja za kibernetsko varnost, ki sicer niso ustrezno obravnavana v okviru izpolnjevanja bistvenih zahtev iz dela I Priloge I, razen tiste iz točke 1. Ta bistvena zahteva se razlikuje od pravne obveznosti izvedbe ocene tveganja za kibernetsko varnost, ki jo je treba opraviti v skladu s členom 13(2).

166. Kadar se vsa zadevna tveganja za kibernetsko varnost, povezana z izdelkom z digitalnimi elementi, obravnavajo z izvajanjem ustreznih ukrepov za izpolnitev veljavnih bistvenih zahtev, razen tiste iz točke 1, se šteje, da je bistvena zahteva iz točke 1 dela I Priloge I izpolnjena. Nasprotno pa morajo proizvajalci, kadar se v oceni tveganja za kibernetsko varnost ugotovijo dodatna tveganja, ki s takimi ukrepi niso v celoti obravnavana, za izdelek z digitalnimi elementi izvesti ustrezne ukrepe za obravnavo teh tveganj, da izpolnijo bistveno zahtevo iz točke 1 dela I Priloge I. V praksi se v večini primerov pričakuje, da skladnost z drugimi bistvenimi zahtevami privede do skladnosti s to zahtevo.

7.3 Ocena tveganja in potrebna skrbnost v zvezi z zunanjimi odvisnostmi in vgrajenimi sestavnimi deli

167. V aktu o kibernetski odpornosti sta določeni dve ločeni, vendar dopolnjujoči se obveznosti za proizvajalce v zvezi z obvladovanjem tveganj za kibernetsko varnost. Prvič, člen 13(2) od proizvajalcev zahteva, da izvedejo oceno tveganja za kibernetsko varnost za sam izdelek z digitalnimi elementi. Drugič, člen 13(5) nalaga obveznost potrebne skrbnosti v zvezi z vgrajenimi sestavnimi deli. Namen teh dveh obveznosti skupaj je zagotoviti, da izdelek z digitalnimi elementi ostane varen tudi, kadar se zanaša na rešitve za daljinsko obdelavo podatkov, storitve na daljavo ali sestavne dele programske opreme ali strojne opreme tretjih oseb.

168. Ocena tveganja za kibernetsko varnost se nanaša na prepoznavanje in obvladovanje ustreznih tveganj, ki lahko vplivajo na izdelek z digitalnimi elementi, vključno s tveganji, ki izvirajo zunaj samega izdelka, kot so zunanja omrežja, okoljski dejavniki ali drugi zunanji vidiki, ki bi lahko vplivali na izdelek z digitalnimi elementi ali na katerih izdelek temelji. Akt o kibernetski odpornosti v zvezi s takimi zunanjimi tveganji od proizvajalcev ne zahteva, naj nadzorujejo ali upravljajo zunanje okolje. Namesto tega morajo proizvajalci taka tveganja opredeliti in jih zmanjšati z zasnovo in razvojem samega izdelka z digitalnimi elementi. To bo vključevalo izpolnjevanje ustreznih bistvenih zahtev iz dela I Priloge I in po potrebi zagotavljanje informacij in navodil uporabnikom o tveganjih pri vgradnji ali uvedbi.

169. Proizvajalec lahko na primer ugotovi tveganje, da bi nepooblaščene osebe lahko med delovanjem izdelka pridobile dostop do zalednih sistemov, ki niso del samega izdelka z digitalnimi elementi, in izdelku z digitalnimi elementi poskusile poslati zlonamerne ukaze. Taki zaledni sistemi, kadar jih ni zasnoval in razvil proizvajalec ali niso bili zasnovani in razviti pod njegovo odgovornostjo ali kadar ne podpirajo ene od funkcij izdelka z digitalnimi elementi, niso rešitve za daljinsko obdelavo podatkov, zato za namene akta o kibernetski odpornosti ne spadajo v obseg izdelka z digitalnimi elementi. Vendar akt o kibernetski odpornosti od proizvajalca zahteva, da tveganje, ki ga lahko povzročijo, obravnava z ukrepi na ravni izdelka, kot so zahteva po kriptografski avtentikaciji ukazov na daljavo, preverjanje celovitosti sprememb konfiguracije ali ustvarjanje dnevnikov ali opozoril, pomembnih za varnost, kadar se zazna neobičajno vedenje. Podobno se lahko na podlagi akta o kibernetski odpornosti, kadar proizvajalec ugotovi tveganje, ki izhaja iz nerazpoložljivosti takšne zunanje storitve, na primer zaradi izpada električne energije ali okvare infrastrukture, od proizvajalca zahteva, da sprejme blažilne ukrepe na ravni izdelka za tveganja za kibernetsko varnost, na primer zagotovi, da zaradi izpada izdelek z digitalnimi elementi ne preide v stanje, ki ni varno. V takih primerih akt o kibernetski odpornosti ureja, kako se izdelek z digitalnimi elementi odziva na ta zunanja tveganja, ne nalaga pa obveznosti glede tega, kako se zaledna infrastruktura organizira, kadrovsko opremi ali upravlja, niti te infrastrukture ne obravnava kot dela izdelka z digitalnimi elementi.

170. Potrebna skrbnost se nanaša na elemente, ki so del samega izdelka z digitalnimi elementi, zlasti vgrajene sestavne dele programske ali strojne opreme, ki jih zagotovi tretja oseba. Proizvajalci morajo sprejeti ustrezne ukrepe za zagotovitev, da taki sestavni deli ne ogrožajo skladnosti izdelka z digitalnimi elementi z bistvenimi zahtevami. To je mogoče doseči le tako, da se določi, kaj izdelek z digitalnimi elementi potrebuje od svojih sestavnih delov, da bi izpolnil svoje cilje kibernetske varnosti, in da se na podlagi tveganja preveri, ali ti sestavni deli ustrezajo potrebam izdelka, kot je navedeno tudi v uvodni izjavi 34.

171. Proizvajalec mora v skladu s svojo oceno tveganja za kibernetsko varnost opredeliti zahteve, ki bi jih moral izpolnjevati vgrajeni sestavni del. Če se izdelek z digitalnimi elementi na primer zanaša na kriptografske funkcije, mehanizme za posodabljanje ali varne komunikacije, ki jih zagotavlja sestavni del, mora proizvajalec v okviru potrebne skrbnosti opredeliti te potrebe in preveriti, ali jih sestavni del izpolnjuje. Dokazila za ta namen so lahko dokumentacija, pridobljena od proizvajalca sestavnega dela, kot so tehnične specifikacije, varnostna dokumentacija ali ustrezna dokumentacija o skladnosti ali zagotovilu. Kadar je ustrezno, lahko proizvajalec izvede tudi preskuse, da preveri, ali ti sestavni deli ustrezno izvajajo zadevne funkcije. Čeprav je potrebna skrbnost ločena pravna obveznost, podpira in je podlaga za sposobnost proizvajalca, da dokaže skladnost izdelka z digitalnimi elementi kot celote z bistvenimi zahtevami.

172. Pri ocenjevanju tveganj za izdelek z digitalnimi elementi kot celoto je treba v oceni tveganja za kibernetsko varnost upoštevati elemente zunaj izdelka, kot so okoljski elementi, zunanja infrastruktura, drugi sistemi ali omrežja, in te elemente po potrebi obravnavati z ukrepi na ravni izdelka, da se zagotovi skladnost izdelka z digitalnimi elementi z bistvenimi zahtevami. Sestavne dele, ki so fizično ali logično vgrajeni v izdelek z digitalnimi elementi, vendar pridobljeni od tretje osebe, je treba prav tako upoštevati v okviru ocene tveganja. Vendar bi moral proizvajalec za namene skladnosti te sestavne dele obravnavati kot od zunaj dobavljene sestavne dele, katerih lastnosti se ob vgradnji preverijo s potrebno skrbnostjo, saj jih proizvajalec morda ni ponovno zasnoval ali ponovno razvil.

173. Enaka logika se uporablja med razvojem in vgradnjo sestavnih delov. Kadar proizvajalec sam razvija funkcije, mora neposredno izpolnjevati bistvene zahteve. Kadar proizvajalec vgradi sestavne dele, ki so jih razvili drugi, mora s potrebno skrbnostjo zagotoviti, da se te sestavne dele lahko uporablja na način, ki omogoča skladnost izdelka z digitalnimi elementi kot celote. V obeh primerih cilj ostaja isti: da izdelek z digitalnimi elementi, kot je dan na trg, dosega ustrezno raven kibernetske varnosti, kot se zahteva z aktom o kibernetski odpornosti, ob upoštevanju tveganj, ugotovljenih v oceni tveganja za kibernetsko varnost.

7.4 **Ponovna uporaba ocen tveganja in dokumentacije o skladnosti za družine izdelkov z digitalnimi elementi**

174. Proizvajalci lahko dajo na trg podobne izdelke z digitalnimi elementi, na primer različne različice, modele ali konfiguracije iste družine izdelkov. Kadar imajo taki izdelki z digitalnimi elementi enako arhitekturo, zasnovo, pomembno za varnost, in predvideni namen ter so izpostavljeni enakim tveganjem za kibernetsko varnost, akt o kibernetski odpornosti od proizvajalcev ne zahteva, da vsako različico obravnavajo kot povsem ločen izdelek z digitalnimi elementi za namene ocene tveganja in ugotavljanja skladnosti.

175. V takih primerih se lahko proizvajalci, če so vse zadevne različice ustrezno zajete z vidika ustreznih tveganj in bistvenih zahtev, oprejo na: (i) enotno oceno tveganja za kibernetsko varnost, izvedeno v skladu s členom 13(2) akta o kibernetski odpornosti; (ii) enoten sklop tehnične dokumentacije in (iii) enoten postopek ugotavljanja skladnosti. To omogoča tudi izdajo enotne EU izjave o skladnosti za skupino izdelkov z digitalnimi elementi, če so v njej jasno opredeljene različice izdelka, za katere se uporablja.

176. Odločilni dejavnik je, ali so razlike med različicami pomembne za kibernetsko varnost. Za razlike, ki ne vplivajo na lastnosti izdelka z digitalnimi elementi z vidika kibernetske varnosti, kot so razlike v barvi, fizični obliki, velikosti pomnilnika ali drugih značilnostih, ki niso pomembne za varnost, niso potrebne ločene ocene tveganja ali ugotavljanje skladnosti. Nasprotno pa se lahko različice v nekaterih primerih razlikujejo na načine, ki vplivajo na izpolnjevanje bistvenih zahtev, na primer zaradi različnih komunikacijskih vmesnikov, programskih skladov, mehanizmov za posodabljanje ali povezljivosti na daljavo. V teh primerih se morajo te razlike upoštevati v oceni tveganja in po potrebi pri ugotavljanju skladnosti ter v tehnični dokumentaciji.

177. Proizvajalci so še vedno odgovorni za zagotavljanje, da ocena tveganja in povezana dokumentacija natančno odražata izdelke z digitalnimi elementi, dane na trg. Kadar se z novo različico uvajajo nova tveganja za kibernetsko varnost ali spreminja način izpolnjevanja bistvenih zahtev, je treba obstoječo oceno tveganja in dokumentacijo o skladnosti ustrezno posodobiti. Na eno samo ugotavljanje skladnosti se je mogoče zanesti le, če se izdelki z digitalnimi elementi ne razlikujejo po lastnostih z vidika kibernetske varnosti.

8. **DALJINSKA OBDELAVA PODATKOV**

178. V členu 3(1) akta o kibernetski odpornosti je izdelek z digitalnimi elementi opredeljen kot „izdelek programske ali strojne opreme ter njegove rešitve za daljinsko obdelavo podatkov, vključno s sestavnimi deli programske ali strojne opreme, ki se dajejo na trg ločeno“. Glede na navedeno mora proizvajalec obravnavati izdelek z digitalnimi elementi kot celoto, vključno z njegovimi rešitvami za daljinsko obdelavo podatkov. Pri dokazovanju, da izdelek z digitalnimi elementi izpolnjuje bistvene zahteve iz Priloge I, je treba na primer upoštevati rešitve za daljinsko obdelavo podatkov, začenši z oceno tveganja (člen 13(2)). Enako velja pri obravnavi obveznosti v življenjskem ciklu, kot je poročanje o aktivno izrabljenih ranljivostih in resnih incidentih (člen 14).

179. Namen teh usmeritev je zagotoviti dodatno podporo proizvajalcem pri ugotavljanju, ali njihov izdelek z digitalnimi elementi vključuje rešitve za daljinsko obdelavo podatkov, kot so opredeljene v aktu o kibernetski odpornosti, in kako izpolniti obveznosti glede skladnosti v zvezi s tem. Po začetni analizi opredelitev in uvodnih izjav iz akta o kibernetski odpornosti bodo v teh usmeritvah navedena vprašanja, ki bodo proizvajalcem v pomoč pri pojasnjevanju, ali njihov izdelek z digitalnimi elementi vključuje rešitve za daljinsko obdelavo podatkov (glej oddelek *8.1 What is considered a remote data processing solution for a product with digital elements?*). Nato bodo podrobneje obravnavane tehnične posledice rešitve za daljinsko obdelavo podatkov in način ocenjevanja skladnosti z aktom o kibernetski odpornosti (glej oddelek *8.2 Practical and technical implications of remote data processing solutions and reliance on third-party solutions*).

180. Člen 3(2) namreč opredeljuje pojem „daljinska obdelava podatkov“ kot „obdelavo podatkov na daljavo, za katero je programsko opremo zasnoval in razvil proizvajalec ali je bila zasnovana in razvita pod njegovo odgovornostjo ter brez katere izdelek z digitalnimi elementi ne bi mogel opravljati ene od svojih funkcij“. Rešitev za daljinsko obdelavo podatkov je torej opredeljena kot element programske opreme („del elektronskega informacijskega sistema, ki ga sestavlja računalniška koda“, kot je opredeljeno v členu 3(4)) za obdelavo podatkov na daljavo. Ni namenjena temu, da bi v okviru izdelka z digitalnimi elementi vključevala strojno opremo, na kateri lahko temelji daljinska obdelava podatkov.

181. V uvodnih izjavah 11 in 12 so dodatna pojasnila, kako bi bilo treba razlagati ta pojem. V uvodni izjavi 11 je pojasnjeno, da je cilj vključitve rešitve za daljinsko obdelavo podatkov ta, da „proizvajalci take izdelke v celoti ustrezno zavarujejo, ne glede na to, ali se podatki obdelujejo ali shranjujejo lokalno na napravi uporabnika ali na daljavo s strani proizvajalca“. V njej je navedeno tudi, da „zahteve v zvezi z rešitvami za daljinsko obdelavo podatkov, ki spadajo na področje uporabe te uredbe, zato ne vključujejo tehničnih, operativnih ali organizacijskih ukrepov za obvladovanje tveganj za varnost omrežij in informacijskih sistemov proizvajalca kot celote“.

182. Iz uvodne izjave 11 torej izhaja, da namen zahtev iz akta o kibernetski odpornosti ni zajeti celotno infrastrukturo IT organizacije, temveč le sestavne dele programske opreme, ki omogočajo izvajanje rešitve za obdelavo podatkov. Notranji sistemi, povezani s človeškimi viri proizvajalca, njegovim obračunom plač, upravljanjem odnosov s strankami, cevovodi za neprekinjeno integracijo/neprekinjeno dostavo (CI/CD) ter distribucijo varnostnih posodobitev na robne lokacije, se na primer ne bi smeli šteti za rešitve za daljinsko obdelavo podatkov. V obseg izdelka z digitalnimi elementi, kot je zajet z aktom o kibernetski odpornosti, prav tako ne spadajo sistemi, povezani z revizijskimi dejavnostmi in dejavnostmi preskušanja, kot so penetracijsko testiranje, lov na grožnje in simuliranje kibernetskih napadov. Pomembno je opozoriti, da čeprav je izvajanje učinkovitih in rednih preverjanj in pregledov varnosti izdelka z digitalnimi elementi bistvena zahteva iz točke 3 dela II Priloge I k aktu o kibernetski odpornosti, to ne pomeni, da je treba take dejavnosti za izdelek z digitalnimi elementi šteti za rešitve za daljinsko obdelavo podatkov.

183. Uvodna izjava 12 se osredotoča na storitve v oblaku in podrobneje pojasnjuje okoliščine, v katerih bi se storitve v oblaku lahko štele za rešitve za daljinsko obdelavo podatkov. Uvodna izjava se zaključi z navedbo, da storitve računalništva v oblaku in modeli storitev v oblaku spadajo na področje uporabe Direktive (EU) 2022/2555 (direktiva NIS 2) ([28]), ki določa zahteve glede obvladovanja tveganj za kibernetsko varnost za ponudnike storitev računalništva v oblaku. Te zahteve so podrobneje določene v Izvedbeni uredbi Komisije (EU) 2024/2690 ([29]).

8.1 **Kaj se šteje za rešitev za daljinsko obdelavo podatkov pri izdelku z digitalnimi elementi?**

184. Opredelitev daljinske obdelave podatkov iz člena 3(2) torej temelji na treh elementih: (i) ali se obdelava podatkov izvaja „na daljavo“; (ii) ali brez take obdelave podatkov izdelek z digitalnimi elementi ne bi mogel opravljati ene od svojih funkcij in (iii) ali je programsko opremo zasnoval in razvil proizvajalec ali je bila zasnovana in razvita pod njegovo odgovornostjo. V naslednjih treh pododdelkih je vsak od teh elementov obravnavan podrobneje.

([28]) Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2) (UL L 333, 27.12.2022, str. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Izvedbena uredba Komisije (EU) 2024/2690 z dne 17. oktobra 2024 o določitvi pravil za uporabo Direktive (EU) 2022/2555 v zvezi s tehničnimi in metodološkimi zahtevami ukrepov za obvladovanje tveganj za kibernetsko varnost ter podrobnejšo opredelitvijo primerov, v katerih se incident šteje za pomembnega, kar zadeva ponudnike storitev DNS, registre TLD imen, ponudnike storitev računalništva v oblaku, ponudnike storitev podatkovnega centra, ponudnike omrežij za dostavo vsebin, ponudnike upravljanih storitev, ponudnike upravljanih varnostnih storitev, ponudnike spletnih tržnic, spletnih iskalnikov in platform za storitve družbenega mreženja ter ponudnike storitev zaupanja (UL L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1 *Pojem „na daljavo“*

185. Pojem „na daljavo“ iz člena 3(2) je pomemben, vendar ne zadostuje za ugotovitev, ali izdelek z digitalnimi elementi vključuje rešitve za daljinsko obdelavo podatkov. Poleg tega ni mogoče podati izčrpne opredelitve pojma „na daljavo“, saj bi lahko pod ta pojem spadale različne rešitve. Proizvajalec mora izvesti oceno za vsak primer posebej.

186. V uvodni izjavi 11 akta o kibernetski odpornosti so omenjeni podatki, ki se obdelujejo ali shranjujejo „na daljavo s strani proizvajalca“, v nasprotju s podatki, ki se obdelujejo ali shranjujejo „lokalno na napravi uporabnika“. Daljinska obdelava podatkov običajno poteka zunaj uporabniškega okolja izdelka z digitalnimi elementi ali operativnega okolja organizacije (za poklicnega uporabnika). To pa ne preprečuje, da bi obdelava potekala tudi blizu naprave („na robu“). Prenos podatkov je lahko žični (npr. ethernetni kabel) ali brezžični (npr. Wi-Fi, Bluetooth). Računalništvo v oblaku, vključno z robnim računalništvom, je tipičen primer obdelave podatkov „na daljavo“. Pri funkciji v oblaku, do katere uporabnik dostopa iz mobilne aplikacije, del obdelave podatkov na primer poteka v oblaku, zunaj uporabnikovega okolja.

187. Upoštevati je treba, da se rešitve za daljinsko obdelavo podatkov ne izvajajo nujno v infrastrukturi v oblaku tretje osebe. Daljinska obdelava podatkov, ki se izvaja na lokalnih strežnikih v prostorih proizvajalca, lahko prav tako pomeni rešitev za daljinsko obdelavo podatkov. Z drugimi besedami, rešitev, ki se izvaja v prostorih organizacije in v zasebnem oblaku, se lahko prav tako šteje za rešitev za daljinsko obdelavo podatkov kot rešitev, ki se izvaja v javnem oblaku in zunaj prostorov organizacije.

188. Dve odločilni in kumulativni vprašanji, ki določata, ali je obdelava podatkov zajeta z aktom o kibernetski odpornosti kot rešitev za daljinsko obdelavo podatkov, sta navedeni spodaj, v oddelkih *8.1.2* in *8.2*. Če je odgovor na obe vprašanji pritrdilen, se daljinska obdelava podatkov šteje za rešitev za daljinsko obdelavo podatkov.

8.1.2 *Ali brez take obdelave podatkov izdelek z digitalnimi elementi ne bi mogel opravljati ene od svojih funkcij?*

189. Kot je določeno v opredelitvi pojma „daljinska obdelava podatkov“ v členu 3(2), se obdelava podatkov na daljavo šteje za rešitev za daljinsko obdelavo podatkov, če brez take obdelave izdelek z digitalnimi elementi ne bi mogel opravljati ene od svojih funkcij. Pojem „funkcije“ iz te opredelitve ni omejen na „osnovno funkcijo“ ali „predvideni namen“ izdelka z digitalnimi elementi, saj akt o kibernetski odpornosti take omejitve ne določa. Funkcije na področju uporabe akta o kibernetski odpornosti so tako funkcije, ki neposredno izpolnjujejo predvideni namen izdelka z digitalnimi elementi z vidika uporabnikov, kot funkcije, ki podpirajo splošno delovanje izdelka.

190. Primeri funkcij, pri katerih lahko pride do obdelave podatkov na daljavo in pri katerih brez take obdelave izdelek z digitalnimi elementi ne bi mogel opravljati ene od svojih funkcij, so: (i) pošiljanje ukazov napravi; (ii) sinhronizacija datotek; (iii) uvajanje uporabnika; (iv) konfiguracija (personalizacija izdelka z digitalnimi elementi); (v) avtomatizirana distribucija posodobitev, vključno s posodobitvami funkcij in varnostnimi popravki; (vi) upravljanje identitete in dostopa.

191. V nekaterih primerih lahko uporabnik funkcijo uporablja tako na daljavo kot ročno (npr. prižig žarnice z aplikacijo ali ročno). Kljub tej možnosti se lahko obdelava podatkov, povezana z opravljanjem funkcije na daljavo, šteje za rešitev za daljinsko obdelavo podatkov. Opravljanje te funkcije na daljavo se prav tako šteje za del funkcij izdelka z digitalnimi elementi.

192. Nasprotno pa velja, da kadar lahko izdelek z digitalnimi elementi opravlja svoje funkcije tudi brez določene obdelave podatkov, se taka obdelava ne šteje za rešitev za daljinsko obdelavo podatkov v smislu akta o kibernetski odpornosti. To na primer vključuje analizo telemetričnih podatkov na daljavo, zbranih izključno za statistične namene ali prihodnji razvoj izdelka.

193. Toda proizvajalci bodo morda morali tudi takrat, kadar obdelava podatkov ne podpira neke funkcije izdelka z digitalnimi elementi, v okviru svoje ocene tveganja za kibernetsko varnost kljub temu preučiti, ali so s temi oddaljenimi sestavnimi deli povezana tveganja za izdelek z digitalnimi elementi (npr. glede na operativno okolje izdelka), in ta tveganja ustrezno zmanjšati (npr. z ukrepi za ublažitev na ravni izdelka).

194. Spletišča so poseben primer, ki zahteva dodatno pojasnitev, kot je razloženo tudi v *oddelku 2.1 Placing on the market*. Spletišča ne spadajo v obseg rešitve za daljinsko obdelavo podatkov, če ne podpirajo funkcije izdelka z digitalnimi elementi, kot je pojasnjeno v uvodni izjavi 11 akta o kibernetski odpornosti. Da bi se štelo, da spletišče spada v okvir rešitve za daljinsko obdelavo podatkov, ne zadostuje, da vsebuje informacije o izdelku z digitalnimi elementi, tudi če izdelek uporabnika preusmerja na tako spletišče. Preusmerjanje uporabnikov na zunanjo spletno stran, ki uporabnikom zagotavlja informacije in navodila, na primer ni rešitev za daljinsko obdelavo podatkov. Nasprotno pa lahko spletišče spada v okvir rešitve za daljinsko obdelavo podatkov, če omogoča ali podpira funkcijo izdelka z digitalnimi elementi. Portal za avtentikacijo, ki izdaja poverilnice ali žetone, potrebne za delovanje izdelka z digitalnimi elementi, bi se na primer štel za rešitev za daljinsko obdelavo podatkov (če so izpolnjena tudi druga merila iz opredelitve).

8.1.3 *Ali je programsko opremo zasnoval in razvil proizvajalec oziroma ali je bila zasnovana in razvita pod njegovo odgovornostjo?*

195. V opredelitvi pojma „daljinska obdelava podatkov“ iz člena 3(2) akta o kibernetski odpornosti je nadalje določeno, da mora programsko opremo za tako obdelavo podatkov na daljavo zasnovati in razviti proizvajalec ali da mora biti zasnovana in razvita pod njegovo odgovornostjo. Daljinska obdelava podatkov, ki jo je v celoti zasnoval in razvil proizvajalec (interno), bi se seveda štela za rešitev za daljinsko obdelavo podatkov. Tako bi bilo tudi, če se proizvajalec pri razvoju in zasnovi rešitve zanese na zunanjega ponudnika storitev (tj. „pod njegovo odgovornostjo“). Besedna zveza „pod njegovo odgovornostjo“ se nanaša na rešitve za obdelavo na daljavo, ki so prilagojene proizvajalcu. Gre za primere, v katerih proizvajalec ne samo podeljuje licenco za obstoječi izdelek z digitalnimi elementi ali storitev, ki jo ponudnik storitev ponuja svojim strankam, ali nekoliko spremenjene različice takega izdelka ali storitve. „[P]od njegovo odgovornostjo“ pomeni, da je programsko opremo izdelal izključno proizvajalec oziroma je bila izdelana v njegovem imenu na podlagi zasnov in specifikacij, ki jih je zagotovil.

196. Pri razumevanju rešitve za daljinsko obdelavo podatkov koncept „kdo upravlja rešitev“ ni odločilni dejavnik, saj se opredelitev v aktu o kibernetski odpornosti nanaša le na zasnovo in razvoj rešitve za daljinsko obdelavo podatkov. To je skladno s pristopom akta o kibernetski odpornosti, v skladu s katerim se zahteve in obveznosti nanašajo na proizvajalce, ne pa na delovanje izdelka z digitalnimi elementi. Če proizvajalci zasnujejo in razvijejo rešitve, ki jih nato upravlja tretja oseba, ostajajo odgovorni za skladnost z bistvenimi zahtevami iz akta o kibernetski odpornosti za izdelek z digitalnimi elementi, ki ga dajo na trg.

197. Treba je razlikovati med primeri, v katerih zasnovo in razvoj izvedejo proizvajalci (ali se izvedeta pod njihovo odgovornostjo), in primeri uporabe rešitev tretjih oseb, ki jih niso zasnovali in razvili proizvajalci (ali se niso zasnovale in razvile pod njihovo odgovornostjo). Kot primer je koristno preučiti najpogostejše modele storitev v oblaku, ki zagotavljajo različne stopnje uporabniškega nadzora in so navedeni tudi v uvodni izjavi 12 akta o kibernetski odpornosti, in sicer programska oprema kot storitev (SaaS), platforma kot storitev (PaaS) in infrastruktura kot storitev (IaaS).

198. Proizvajalec v primeru rešitve IaaS tretje osebe ne upravlja ali nadzoruje osnovnih fizičnih in virtualnih virov (kot sta osnovna strojna oprema in hipervizor ponudnika storitev v oblaku), lahko pa z uporabo takih virov uvaja in izvaja poljubno programsko opremo, kot so operacijski sistemi in aplikacije. Tako programsko opremo je zasnoval in razvil proizvajalec ali pa je bila zasnovana in razvita pod njegovo odgovornostjo ter se zato lahko šteje za rešitev za daljinsko obdelavo podatkov (če izpolnjuje druge elemente opredelitve).

199. Proizvajalec v primeru rešitve PaaS tretje osebe uvede svojo (ustvarjeno ali pridobljeno) aplikacijo z uporabo programskih jezikov in izvajalnih okolij, ki jih zagotavlja ponudnik storitev v oblaku, ter aplikacijo vgradi v svoj izdelek z digitalnimi elementi. Proizvajalec ima nadzor nad aplikacijo in morda nad konfiguracijskimi nastavitvami izvajalnega okolja. Aplikacijo je torej zasnoval in razvil proizvajalec ali pa je bila zasnovana in razvita pod njegovo odgovornostjo ter se zato lahko šteje za rešitev za daljinsko obdelavo podatkov (če izpolnjuje druge elemente opredelitve).

200. V primeru rešitve SaaS tretje osebe ponudnik te rešitve proizvajalcu ponudi v celoti razvito aplikacijo, ki se vgradi v proizvajalčev izdelek z digitalnimi elementi. Proizvajalec ima omejeno možnost upravljanja konfiguracijskih nastavitev aplikacije za posameznega uporabnika. Aplikacije torej ni zasnoval in razvil proizvajalec niti ni bila zasnovana in razvita pod njegovo odgovornostjo.

201. Vendar kadar se določeni elementi ne štejejo za rešitev za daljinsko obdelavo podatkov (npr. hipervizor v primeru IaaS tretje osebe, operacijski sistem v primeru rešitve PaaS tretje osebe ali SaaS tretje osebe), so pa vgrajeni v izdelek z digitalnimi elementi na način, ki vpliva na njegovo varnost, bi bilo treba take rešitve kljub temu obravnavati podobno kot sestavne dele tretjih oseb. Proizvajalec mora opredeliti in oceniti tveganja, povezana z vgradnjo teh elementov, ter jih obravnavati z izpolnjevanjem bistvenih zahtev za sam izdelek z digitalnimi elementi. Kadar je ustrezno, se to lahko podpre z varnostnimi funkcijami, ki jih ponudnik storitev v oblaku da na voljo v okviru svojega modela deljene odgovornosti, kadar proizvajalec te funkcije uporablja ali konfigurira za obravnavanje ugotovljenih tveganj. Poleg tega se pričakuje, da bo proizvajalec v zvezi z varnostjo teh sestavnih delov izpolnil obveznost, podobno obveznosti potrebne skrbnosti iz člena 13(5), na način, ki je sorazmeren s tveganjem, ki ga oddaljena rešitev pomeni za varnost izdelka z digitalnimi elementi.

202. Torej je mogoče povzeti:

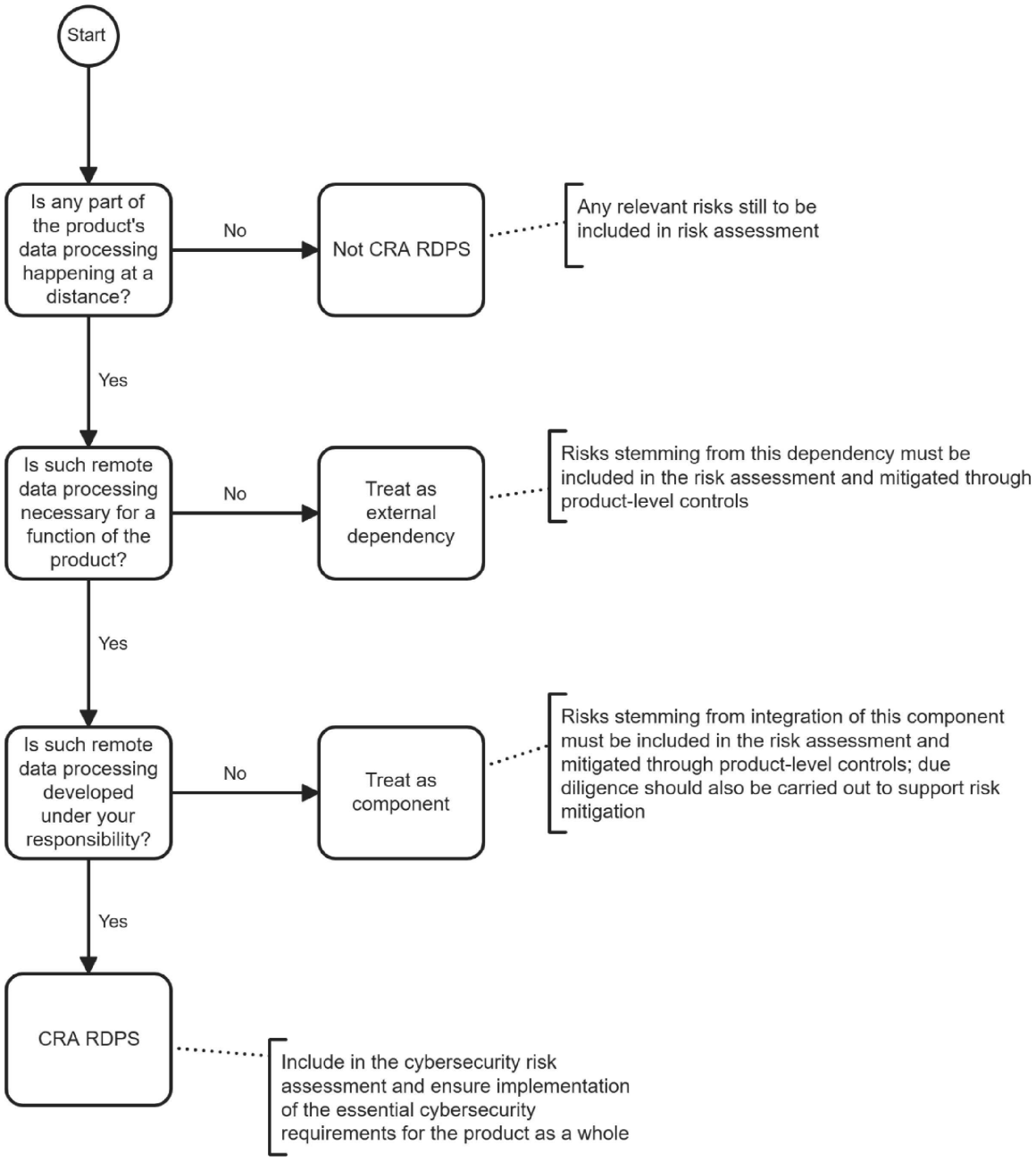
(a) Da bi se obdelava podatkov štela za rešitev za daljinsko obdelavo podatkov, mora biti odgovor na obe vprašanji iz oddelkov *8.1.2 Would the absence of such data processing prevent the product with digital elements from performing one of its* functions? in *8.1.3 Has the software been designed and developed by the manufacturer, or under its responsibility?* pritrdilen.

(b) Če je odgovor na vprašanje iz oddelka *8.1.2 Would the absence of such data processing prevent the product with digital elements from performing one of its* functions? nikalen, bi morali proizvajalci v okviru svoje ocene tveganja oceniti tveganja, ki izhajajo iz obstoja take obdelave podatkov.

(c) Če je odgovor na vprašanje iz oddelka *8.1.2 Would the absence of such data processing prevent the product with digital elements from performing one of its* functions? pritrdilen, odgovor na vprašanje iz oddelka *8.1.3 Has the software been designed and developed by the manufacturer, or under its responsibility?* pa nikalen, bi morali proizvajalci rešitev tretje osebe obravnavati kot sestavni del. Proizvajalci bi morali v okviru ocene tveganja oceniti tveganja, ki izhajajo iz vgradnje take rešitve, in jih ustrezno zmanjšati. Poleg tega bi morali ravnati s potrebno skrbnostjo.

Slika 9

Stiliziran diagram poteka za ugotavljanje, ali izdelek z digitalnimi elementi vsebuje rešitev za daljinsko obdelavo podatkov



8.2 Praktične in tehnične posledice rešitev za daljinsko obdelavo podatkov ter zanašanja na rešitve tretjih oseb

203. V aktu o kibernetski odpornosti se uporablja pristop, ki temelji na tveganju ter je določen v členu 13(2) in (3) ter v prvi bistveni zahtevi iz dela I Priloge I, v skladu s katero so „izdelki z digitalnimi elementi […] zasnovani, razviti in proizvedeni tako, da zagotavljajo ustrezno raven kibernetske varnosti glede na tveganja“. Zato bi bilo treba pri uporabi zahtev iz akta o kibernetski odpornosti za rešitve za daljinsko obdelavo podatkov in obravnavi tveganj, ki izhajajo iz storitev tretjih oseb, vgrajenih v izdelek z digitalnimi elementi, upoštevati pristop, ki temelji na tveganju.

204. Prvič, proizvajalci bi morali (i) v tehnični dokumentaciji navesti, da ima njihov izdelek z digitalnimi elementi rešitev za daljinsko obdelavo podatkov ali se zanaša na oddaljene rešitve tretjih oseb, ter (ii) take rešitve opisati. Če ista rešitev za daljinsko obdelavo podatkov podpira več izdelkov z digitalnimi elementi, jo je treba navesti v tehnični dokumentaciji vsakega izdelka. Dokumentacija o rešitvi za daljinsko obdelavo podatkov, ki podpira več izdelkov z digitalnimi elementi, iz enega postopka ugotavljanja skladnosti izdelka se lahko ponovno uporabi v drugem postopku.

205. Kot je navedeno v uvodni izjavi 11, bi morale biti rešitve za daljinsko obdelavo podatkov, ki so del izdelka z digitalnimi elementi in so zato predmet ugotavljanja skladnosti izdelka, omejene na tiste programske module, ki so odgovorni za funkcionalnost izdelka z digitalnimi elementi, in na vmesnike, ki jih ti moduli uporabljajo z zunanjimi storitvami. Dodatni zaledni sistemi, ki izvajajo nadaljnjo obdelavo in s katerimi izdelek z digitalnimi elementi ni v neposredni interakciji, se ne štejejo za rešitve za daljinsko obdelavo podatkov.

206. Kljub temu ti zaledni sistemi ostajajo zunanje odvisnosti, ki jih je treba oceniti v okviru ocene tveganja za kibernetsko varnost in zmanjšati z ukrepi na ravni izdelka. Proizvajalec bi moral v oceni tveganja namreč upoštevati: (i) tveganja, povezana z rešitvijo za daljinsko obdelavo podatkov; (ii) tveganja, povezana z zanašanjem na oddaljene rešitve tretjih oseb (podobno kot pri sestavnih delih tretjih oseb), in (iii) tveganja, povezana z okoljem izdelka (npr. osnovno strojno opremo). Proizvajalci bi morali za zmanjšanje teh tveganj izvajati varnostne kontrole na samem izdelku z digitalnimi elementi.

207. Poleg tega se lahko v okviru ugotavljanja skladnosti in/ali izpolnjevanja obveznosti potrebne skrbnosti v zvezi z oddaljenimi storitvami tretjih oseb v podporo oceni proizvajalca ponovno uporabi naslednji neizčrpen seznam dokazil o zanesljivosti:

(a) dokazila o izpolnjevanju obveznosti iz Izvedbene uredbe Komisije (EU) 2024/2690;

(b) dokazila o izpolnjevanju obveznosti iz Uredbe (EU) 2022/2554 (DORA);

(c) izjava o skladnosti ali certifikat, pridobljen v okviru evropske certifikacijske sheme za kibernetsko varnost (sprejete na podlagi Uredbe (EU) 2019/881 – akt o kibernetski varnosti);

(d) dokazila o skladnosti z ISO/IEC 27017:2015 ali ISO/IEC 27001:2022.

208. Proizvajalci pa morajo pri svojih interakcijah s tretjimi ponudniki oddaljenih storitev izvajati najprimernejše varnostne ukrepe na podlagi svoje ocene tveganja (in po potrebi ob podpori ponudnikovega modela deljene odgovornosti). Ti blažilni ukrepi bi morali vključevati varnostne kontrole za njihove izdelke z digitalnimi elementi in preverjanje varnostnih ukrepov, ki jih zagotavljajo sami tretji ponudniki (potrebna skrbnost). Eno od orodij za zmanjšanje takih tveganj je lahko vključitev varnostnih jamstev v sporazume o ravni storitve s tretjimi ponudniki, vključno z zagotovili, da ponudniki ustrezno obravnavajo ranljivosti. Večja sprememba rešitev, ki jih zagotavljajo tretji ponudniki oddaljenih storitev, se ne bi smela šteti za bistveno spremembo izdelka z digitalnimi elementi, saj ti elementi niso v odgovornosti proizvajalca. Vendar se proizvajalce spodbuja, naj v okviru svojih obveznosti potrebne skrbnosti in za ustrezno zmanjšanje tveganj, ki izhajajo iz uporabe tretjih ponudnikov, zagotovijo, da jih njihovi tretji ponudniki storitev v oblaku ustrezno obveščajo o spremembah, ki jih uvajajo v svojih rešitvah. Na podlagi takih informacij bodo proizvajalci morda morali revidirati svojo oceno tveganja. V posodobljeni oceni tveganja bi bilo treba upoštevati, ali tretji ponudniki storitev še vedno zagotavljajo zadostna jamstva glede kibernetske varnosti in ali so varnostne kontrole na ravni izdelka še vedno ustrezne. V nekaterih primerih bodo proizvajalci morda morali take kontrole spremeniti ali zamenjati tretje ponudnike storitev.

8.3 **Primeri uporabe rešitev za daljinsko obdelavo podatkov**

Da bi se proizvajalcem zagotovile dodatne praktične usmeritve, je v tem oddelku predstavljen niz izmišljenih primerov uporabe, v katerih so opisani vzorčni izdelki z digitalnimi elementi, ki se zanašajo na daljinsko obdelavo podatkov, in ponazorjeno, ali se taka obdelava šteje za rešitve za daljinsko obdelavo podatkov v smislu akta o kibernetski odpornosti.

8.3.1 *Aplikacija za mobilno bančništvo*

Finančni subjekt da na trg aplikacijo za mobilno bančništvo. Zaledni sistemi aplikacije med drugim podpirajo avtentikacijo, avtorizacijo, upravljanje računov in plačila. Finančni subjekt uporablja hibridno strategijo, ki temelji na lastni infrastrukturi in oddaljenih rešitvah tretjih oseb za podporo funkcionalnosti aplikacije. Med temi so:

Samo-gostovana infrastruktura, ki jo je razvil finančni subjekt:

— Stranka odpre aplikacijo za mobilno bančništvo, avtentikacija pa se izvede prek bančnega vmesnika, tj. samo-gostovane rešitve, ki jo razvil finančni subjekt sam in ki prejema zahtevke aplikacije ter vrača ustrezne odgovore. Bančni vmesnik preveri identiteto stranke s poizvedbo v sistemu za upravljanje računov in odobri dostop do aplikacije.

— Stranka prek aplikacije sproži nakazilo. Aplikacija posreduje navodilo bančnemu vmesniku, ki predloži ustrezno zahtevo sistemu evidenc.

— Sistem za upravljanje računov in sistem evidenc, ki sta samo-gostovana, vendar logično ločena od bančnega vmesnika, zabeležita transakcijo.

— Iz sistema evidenc se bančnemu vmesniku sporoči status transakcije, ta pa rezultat prikaže stranki.

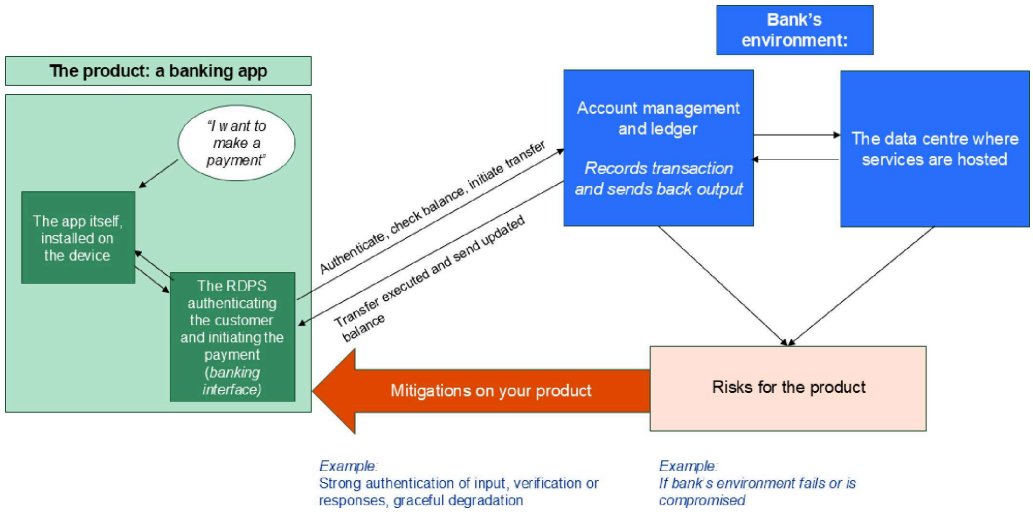
Posledice za rešitve za daljinsko obdelavo podatkov:

— Bančni vmesnik je potreben, da aplikacija izvaja svoje funkcije, in sicer avtentikacijo stranke, pošiljanje navodil stranke, vključno z navodili za plačilo in nakazilo, ter sporočanje nastalega statusa. Bančni vmesnik je bil zasnovan in razvit pod odgovornostjo proizvajalca. Ker je odgovor na obe vprašanji iz prejšnjih oddelkov pritrdilen, je treba bančni vmesnik šteti za rešitev za daljinsko obdelavo podatkov. Zato ga je treba vključiti v oceno tveganja za kibernetsko varnost in v izpolnjevanje bistvenih zahtev za izdelek z digitalnimi elementi kot celoto. Naknadno obdelavo navodila po predložitvi, zlasti evidentiranje transakcije v sistemih za upravljanje računov in evidenc ter poravnavo in kliring, izvajajo sistemi, s katerimi aplikacija ni v neposredni interakciji, zato ta obdelava ne pomeni rešitve za daljinsko obdelavo podatkov.

— Sistem za upravljanje računov in sistem evidenc se ne štejeta za rešitev za daljinsko obdelavo podatkov za bančno aplikacijo. Aplikacija z njima ni v neposredni interakciji (je pa v interakciji z bančnim vmesnikom, ki ta sistema uporablja). Čeprav je njuna razpoložljivost lahko potrebna za dokončanje funkcije, akt o kibernetski odpornosti zajema le tiste dele sistema, ki so v neposredni interakciji z izdelkom z digitalnimi elementi. Zato ne spadata v opredelitev rešitve za daljinsko obdelavo podatkov za namene akta o kibernetski odpornosti. Vendar ti sistemi ostajajo zunanje odvisnosti, ki lahko povzročijo znatna tveganja za kibernetsko varnost izdelka z digitalnimi elementi. Zaradi kompromitacije sistema evidenc bi lahko napadalec na primer vplival na rezultate transakcij, ki se nato prikažejo v aplikaciji. Zato mora proizvajalec ta tveganja opredeliti in oceniti v okviru ocene tveganja za kibernetsko varnost ter jih zmanjšati z ukrepi na ravni izdelka, kot so močna avtentikacija zalednih vmesnikov, zaščita celovitosti podatkov o transakcijah, varni komunikacijski kanali in preverjanje odgovorov, ki jih prejme aplikacija.

Slika 10

Stiliziran prikaz bančne aplikacije, ki se zanaša na rešitve za daljinsko obdelavo podatkov



SaaS tretje osebe za podporo strankam:

— Finančni subjekt v svojo aplikacijo vgradi rešitev za klepet za podporo strankam, ki jo je razvil in jo upravlja tretji ponudnik storitev; tretji ponudnik storitev je napisal kodo strežnika za klepet, izdelal uporabniški vmesnik in upravlja infrastrukturo, na kateri je klepet uveden (tj. model SaaS).

— Ko stranka vloži zahtevek za podporo, jo aplikacija poveže s storitvijo tretje osebe, da se vzpostavi seja klepeta in obravnava tok sporočil, ne da bi tretja oseba imela dostop do osrednjih bančnih sistemov.

Posledice za rešitve za daljinsko obdelavo podatkov:

— Rešitev za klepet za podporo je potrebna, da izdelek z digitalnimi elementi opravlja eno od svojih funkcij, vendar je ni zasnoval in razvil finančni subjekt niti ni bila zasnovana in razvita pod njegovo odgovornostjo; zato ni rešitev za daljinsko obdelavo podatkov. Treba pa bi jo bilo obravnavati kot sestavni del tretje osebe. Zanašanje na navedeno storitev tretje osebe lahko povzroči tveganja za kibernetsko varnost bančne aplikacije, na primer če bi napadalec uporabil kanal za klepet, da bi se izdajal za banko ali uporabnikom dostavil zlonamerno vsebino. Finančni subjekt mora ta tveganja upoštevati v svoji oceni tveganja za kibernetsko varnost in jih zmanjšati z ukrepi na ravni izdelka, kot so izolacija funkcije klepeta od osrednjih bančnih funkcij, nadzor podatkovnih tokov in preverjanje vsebine. Prav tako bi bilo treba s SaaS ravnati s potrebno skrbnostjo.

8.3.2 *Pametni termostat*

Pametni termostat uporabnikom omogoča, da temperaturo v svojem domu nadzorujejo prek mobilne aplikacije. Mobilna aplikacija in pametni termostat za izmenjavo podatkov (npr. zahteva za zvišanje temperature) in shranjevanje podatkov (npr. uporabniške nastavitve) uporabljata daljinsko obdelavo podatkov. Ti funkciji sta bili razviti in zasnovani pod odgovornostjo proizvajalca, vendar delujeta na osnovni fizični in virtualni infrastrukturi, ki jo zagotavlja tretja oseba (IaaS tretje osebe).

Pametni termostat brez daljinske obdelave podatkov ne bi mogel opravljati svojih pametnih funkcij, kar pomeni, da brez daljinske obdelave podatkov izdelek z digitalnimi elementi ne bi mogel opravljati ene ali več svojih funkcij. Poleg tega je bila programska oprema razvita in zasnovana pod odgovornostjo proizvajalca pametnega termostata. Zato se daljinska obdelava podatkov šteje za rešitev za daljinsko obdelavo podatkov, kot je opredeljena v aktu o kibernetski odpornosti.

Proizvajalec pametnega termostata mora za namene skladnosti z aktom o kibernetski odpornosti v tehnični dokumentaciji izdelka z digitalnimi elementi dokumentirati rešitve za daljinsko obdelavo podatkov in uporabo IaaS tretje osebe, vključno s podrobnostmi o pogodbeni storitvi. Proizvajalec mora te elemente upoštevati v oceni tveganja, ki vključuje predvideni namen in razumno predvidljivo uporabo izdelka z digitalnimi elementi. Proizvajalec izpolnjuje bistvene zahteve iz akta o kibernetski odpornosti na podlagi tveganj za rešitve za daljinsko obdelavo podatkov. Glede IaaS tretje osebe mora proizvajalec zagotoviti, da so varnostni ukrepi, ki jih zagotavlja tretji ponudnik storitev, ustrezni, in/ali sprejeti ustrezne ukrepe v zvezi z infrastrukturo. V prvem primeru bi lahko proizvajalec na primer zahteval dokazila, da so bile obveznosti iz direktive NIS 2 izpolnjene.

8.3.3 *E-bralnik*

Proizvajalec programske opreme za e-bralnik uporablja storitev shranjevanja SaaS tretje osebe za shranjevanje elektronskih knjig, ki so jih kupile stranke, in omogočanje dostopa strankam do njihovih knjig. Brez te storitve shranjevanja izdelek z digitalnimi elementi ne bi mogel opravljati ene od svojih funkcij, vendar storitve shranjevanja SaaS tretje osebe ni razvil proizvajalec niti ni bila razvita pod njegovo odgovornostjo; ponudnik SaaS jo da na voljo strankam za vse primere uporabe.

Storitev shranjevanja SaaS ne ustreza opredelitvi rešitve za daljinsko obdelavo podatkov. Vendar se proizvajalec e-bralnika za delovanje svojega izdelka z digitalnimi elementi zanaša na navedeno zunanjo storitev in mora zato povezana tveganja upoštevati v svoji oceni tveganja za kibernetsko varnost. Proizvajalec e-bralnika bi moral SaaS obravnavati kot sestavni del. Izvesti mora ustrezne varnostne ukrepe na ravni izdelka, kot so varna avtentikacija, šifriranje in zaščita celovitosti komunikacij s storitvijo shranjevanja. Potrebna skrbnost pri izbiri in vključevanju ponudnika SaaS bo prav tako pomagala proizvajalcu izpolniti obveznosti, da bo izdelek z digitalnimi elementi kot celota lahko izpolnjeval bistvene zahteve.

8.3.4 *Industrijski robot*

Naloga industrijskega robota je pobirati dele. Robot informacije, zbrane s kamerami, pošilja oddaljeni storitvi, ki jo je zasnoval in razvil proizvajalec. Ta storitev deluje na osnovni fizični in virtualni infrastrukturi, ki jo zagotovi tretji ponudnik storitev (IaaS tretje osebe). Storitev v oblaku izračuna položaj dela na podlagi posnetkov iz kamer in robotu pošilja ukaze za pobiranje delov.

Industrijski robot brez te obdelave podatkov ne bi mogel pobirati delov in s tem opravljati ene od svojih funkcij. Poleg tega je programsko opremo, ki teče na infrastrukturi, zasnoval in razvil proizvajalec. Programska oprema, ki jo je zasnoval in razvil proizvajalec, ustreza opredelitvi rešitve za daljinsko obdelavo podatkov.

Proizvajalec industrijskega robota mora v tehnični dokumentaciji izdelka z digitalnimi elementi dokumentirati rešitve za daljinsko obdelavo podatkov in uporabo IaaS tretje osebe (vključno s podrobnostmi o pogodbeni storitvi). Proizvajalec mora te elemente upoštevati tudi v oceni tveganja, ki vključuje predvideni namen in razumno predvidljivo uporabo izdelka z digitalnimi elementi. Proizvajalec izpolnjuje bistvene zahteve iz akta o kibernetski odpornosti za izdelek z digitalnimi elementi glede na tveganje, vključno z rešitvijo za daljinsko obdelavo podatkov. Potrebna skrbnost pri izbiri ponudnika IaaS bo prav tako pomagala proizvajalcu izpolniti obveznosti. Proizvajalec bi lahko na primer zahteval dokazila, da so bile obveznosti iz direktive NIS 2 izpolnjene.

8.3.5 *Mobilno omrežje*

Pametni telefon uporablja omrežje 5G, da svojim uporabnikom omogoča internetno povezavo, telefonske klice in sporočila (mobilna povezljivost). Mobilno omrežje so razvili in zasnovali telekomunikacijski operaterji. Omrežje vključuje male celice in telekomunikacijske stolpe ter drugo omrežno opremo.

Izdelek z digitalnimi elementi bi moral biti zmožen pravilno povezati se z omrežjem; to je ena od njegovih funkcij. Vendar za ugotavljanje, ali izdelek z digitalnimi elementi deluje pravilno, ni pomembno, ali omrežje deluje ali ne. Omrežje je zgolj komunikacijski kanal in ga izdelek z digitalnimi elementi ne potrebuje za opravljanje svoje funkcije „pravilnega povezovanja z omrežjem“. Prav tako se ethernetni kabel, usmerjevalnik ali signal brezžičnega omrežja ne šteje za obdelavo podatkov, brez katere izdelek z digitalnimi elementi ne bi mogel opravljati ene od svojih funkcij, temveč za sredstvo, ki omogoča komunikacijo/povezljivost.

Zato mobilno omrežje ne ustreza opredelitvi rešitve za daljinsko obdelavo podatkov. Omrežje se ne bi smelo obravnavati kot sestavni del tretje osebe, saj v izdelek z digitalnimi elementi ni vgrajena nobena programska oprema, temveč izdelek to omrežje zgolj uporablja. Zato za proizvajalca ne velja obveznost potrebne skrbnosti v zvezi s ponudnikom omrežja.

9. **DODATNI ELEMENTI**

9.1 **Obveznosti poročanja**

209. V skladu s členom 14(1) in (3) akta o kibernetski odpornosti mora proizvajalec sočasno obvestiti skupino CSIRT, ki je imenovana za koordinatorja, in agencijo ENISA o (i) vsaki aktivno izrabljeni ranljivosti, vsebovani v izdelku z digitalnimi elementi, ki jo ugotovi, in (ii) vsakem resnem incidentu, ki vpliva na varnost izdelka z digitalnimi elementi, s katerim se seznani.

210. V skladu s členom 69(3) in drugim stavkom člena 71(2) se obveznost ravnanja v skladu s členom 14 od 11. septembra 2026 uporablja za vse izdelke z digitalnimi elementi na področju uporabe akta o kibernetski odpornosti, vključno z izdelki z digitalnimi elementi, ki so bili dani na trg pred 11. decembrom 2027. Poleg tega se obveznosti poročanja v nasprotju z obveznostmi obravnavanja ranljivosti, ki trajajo le toliko časa, kolikor traja obdobje podpore izdelka, uporabljajo tudi po tem, ko izdelek z digitalnimi elementi ni več podprt. Če je bil izdelek z digitalnimi elementi dan na trg pred 11. decembrom 2027 ali se je njegovo obdobje podpore končalo, proizvajalcu ni treba izpolniti obveznosti obravnavanja ranljivosti iz dela II Priloge I.

211. Opozoriti je treba, da se obveznost obveščanja o takih dogodkih uporablja, ko se proizvajalec seznani s tem, da je ranljivost aktivno izrabljena ali da se je zgodil resen incident, zaradi katerega je ogrožena varnost njegovega izdelka z digitalnimi elementi. Usmeritve o tem, kdaj se šteje, da se je proizvajalec seznanil s tem, bi morale biti proizvajalcem v pomoč pri določitvi trenutka, ko začnejo teči veljavni roki za poročanje.

212. Za proizvajalce lahko veljajo primerljive obveznosti poročanja na podlagi različnih aktov EU. Da bi se zagotovila dosledna razlaga pojma „seznanjen“ in proizvajalcem olajšalo izpolnjevanje teh obveznosti, so te usmeritve usklajene z uvodno izjavo 31 Izvedbene uredbe Komisije (EU) 2024/2690 in oddelkom II(A) Usmeritev 9/2022 o obveščanju o kršitvi varnosti osebnih podatkov na podlagi splošne uredbe o varstvu podatkov.

213. V nekaterih primerih proizvajalec zazna sumljiv dogodek ali pa ga tretja oseba, kot je posameznik, stranka, subjekt, organ, medijska organizacija ali drug vir, opozori na morebiten incident ali ranljivost. V takih primerih bi moral proizvajalec sumljivi dogodek takoj oceniti, da ugotovi, ali pomeni aktivno izrabljeno ranljivost ali resen incident, ki vpliva na varnost izdelka z digitalnimi elementi. Zato se šteje, da se je proizvajalec seznanil, ko po taki prvotni oceni z razumno stopnjo gotovosti ugotovi, da: (i) se ranljivost v njegovem izdelku z digitalnimi elementi aktivno izrablja ali da (ii) je prišlo do resnega incidenta, zaradi katerega je bila ogrožena varnost njegovega izdelka z digitalnimi elementi.

214. Zato bo trenutek, ko se lahko šteje, da je proizvajalec seznanjen, odvisen od okoliščin posamezne aktivno izrabljene ranljivosti ali resnega incidenta. V nekaterih primerih bo že na samem začetku razmeroma jasno, da se ranljivost aktivno izrablja ali da resen incident vpliva na varnost izdelka z digitalnimi elementi. V drugih primerih lahko traja nekaj časa, da se ugotovi, ali ranljivost vpliva na izdelek z digitalnimi elementi in ali jo izkorišča zlonamerni akter oziroma ali incident vpliva na varnost izdelka z digitalnimi elementi. Vendar bi moral biti poudarek na takojšnjem ukrepanju za izvedbo prvotne ocene, da bi se ugotovilo, ali so taki pogoji dejansko izpolnjeni, zlasti kadar lahko ranljivost pomeni znatno tveganje, in če so, za sprejetje popravnih ukrepov in obveščanje v skladu z aktom o kibernetski odpornosti.

215. Poleg tega struktura obveznosti poročanja od proizvajalcev zahteva, da svoja obvestila s časom posodabljajo, ko njihove notranje preiskave napredujejo in se njihovo poznavanje aktivno izrabljene ranljivosti ali incidenta poglablja. Proizvajalci morajo brez nepotrebnega odlašanja in v vsakem primeru v 24 urah od seznanitve predložiti zgodnje opozorilo, ki vsebuje omejene informacije. Nato je treba v okviru obvestila, ki ga je treba predložiti brez nepotrebnega odlašanja in v vsakem primeru v 72 urah od seznanitve („obvestilo v 72 urah“), zagotoviti dodatne informacije. Popolno poročilo o aktivno izrabljenih ranljivostih je treba predložiti v 14 dneh po tem, ko je na voljo popravni ali blažilni ukrep, o resnih incidentih pa v enem mesecu po uradnem obvestilu v 72 urah.

216. Kot je opozorjeno tudi v oddelku *3.3.1 Sustained support and ensuring viability of FOSS*, morajo tudi upravljavci odprtokodne programske opreme poročati o aktivno izrabljenih ranljivostih v skladu s členom 24(3) ([30]). Ta obveznost se uporablja ob seznanitvi z aktivno izrabljeno ranljivostjo in ne zgolj, kadar obstaja ranljivost v kodni bazi proste in odprtokodne programske opreme, katere upravljavec je ta subjekt. Sestavni deli proste in odprtokodne programske opreme se nižje v verigi običajno vgrajujejo v druge izdelke z digitalnimi elementi, zato se bo v praksi upravljavec verjetno seznanil z aktivnim izrabljanjem prek poročil tretjih oseb, v katerih je ugotovljeno izrabljanje sestavnih delov proste in odprtokodne programske opreme, vgrajenih v druge izdelke z digitalnimi elementi. To se lahko zgodi na primer, kadar proizvajalec izdelka z digitalnimi elementi zazna aktivno izrabljanje sestavnega dela proste in odprtokodne programske opreme, vgrajene v njegov izdelek, in o tem poroča upravljavcu tega sestavnega dela; ali kadar uporabnik ali raziskovalec varnosti najde dokaze o izrabljanju sestavnega dela proste in odprtokodne programske opreme, vgrajene v izdelek z digitalnimi elementi, in o tem aktivnem izrabljanju poroča upravljavcu sestavnega dela.

217. Pojasniti je treba tudi, da proizvajalcu ni treba poročati o ranljivostih, v zvezi s katerimi je aktivno izrabljanje ugotovil že pred 11. septembrom 2026 (datumom, ko se začne uporabljati obveznost poročanja), saj se obveznost poročanja o aktivno izrabljanih ranljivostih uporablja, ko se proizvajalec z aktivnim izrabljanjem seznani. Akt o kibernetski odpornosti zato ne zahteva poročanja o takih ranljivostih za nazaj. Nasprotno pa se obveznost uporablja, kadar se je proizvajalec z ranljivostjo seznanil pred 11. septembrom 2026, vendar takrat ni bil seznanjen z njenim aktivnim izrabljanjem (bodisi ker do njega še ni prišlo bodisi ker se z njim ni seznanil). Če naknadno pride do aktivnega izrabljanja ali se proizvajalec z njim seznani po 11. septembru 2026, se ranljivost šteje za aktivno izrabljeno ranljivost, za katero velja obveznost poročanja.

218. Podobno mora proizvajalec poročati le o aktivno izrabljenih ranljivostih v svojem izdelku z digitalnimi elementi. Kadar aktivno izrabljena ranljivost izdelka z digitalnimi elementi izvira iz sestavnega dela tretje osebe, mora proizvajalec izdelka z digitalnimi elementi o tej aktivno izrabljeni ranljivosti predložiti obvestilo. Če pa je proizvajalec seznanjen, da sestavni del tretje osebe vsebuje ranljivost, vendar ranljivosti (i) ni mogoče izkoristiti v njegovem izdelku z digitalnimi elementi (npr. ker ranljiva koda ni dosegljiva) ali (ii) ni bila izrabljena v njegovem izdelku z digitalnimi elementi, se ta ranljivost ne šteje za aktivno izrabljeno ranljivost v njegovem izdelku z digitalnimi elementi, zato mu o njej ni treba obvezno poročati. Ta proizvajalec lahko kljub temu v skladu s členom 15 akta o kibernetski odpornosti o tej ranljivosti predloži obvestilo prostovoljno. Poleg tega mora v skladu s členom 13(6) izpolnjevati zahteve glede obravnavanja ranljivosti iz dela II Priloge I k aktu o kibernetski odpornosti ter ranljivost sporočiti osebi ali subjektu, ki sestavni del izdeluje ali vzdržuje, kot je dodatno pojasnjeno v oddelku *9.2.1 Reporting upstream and sharing security fixes*.

([30]) Kolikor upravljavec sodeluje pri razvoju izdelka z digitalnimi elementi.

219. Po seznanitvi z aktivno izrabljeno ranljivostjo ali resnim incidentom morajo proizvajalci v skladu s členom 14(8) obvestiti tudi prizadete uporabnike in, kadar je ustrezno, vse uporabnike. Če tega ne storijo pravočasno, lahko skupine CSIRT, ki so prejele obvestilo, uporabnikom posredujejo take informacije, kadar menijo, da so sorazmerne in potrebne za preprečevanje ali ublažitev učinka te ranljivosti ali incidenta.

220. V skladu s pristopom akta o kibernetski odpornosti, ki temelji na tveganju, je treba obveznost obveščanja uporabnikov iz člena 14(8) uporabljati na način, ki temelji na tveganju in je sorazmeren. Predložitev informacij o aktivno izrabljeni ranljivosti ali resnem incidentu še posebej ne pomeni, da morajo biti take informacije javno objavljene ali se razkriti neselektivno. Kadar je ustrezno in glede na naravo izdelka z digitalnimi elementi, prizadete uporabnike in morebitni učinek ranljivosti ali incidenta, lahko proizvajalci razkritje podrobnih informacij omejijo na zadevne uporabnike ali stranke. To velja zlasti za izdelke z digitalnimi elementi, ki se uporabljajo v občutljivih ali bistvenih okoljih, pri katerih bi lahko javno razkritje tehničnih podrobnosti samo po sebi povečalo tveganja za kibernetsko varnost ali olajšalo nadaljnje izrabljanje.

221. Ko je ranljivost ustrezno obravnavana ali ublažena, je lahko primerno širše razkritje. Tak primer je, kadar razkritje prispeva k povečanju splošne ozaveščenosti ali uporabnikom omogoča, da preverijo, ali njihovi izdelki z digitalnimi elementi niso več prizadeti. V takih primerih morata raven podrobnosti in čas vsakega širšega razkritja ostati sorazmerna, pri čemer je treba upoštevati preostala tveganja izrabljanja, naravo izdelka z digitalnimi elementi in interese zadevnih uporabnikov. Poleg tega točka 4 dela II Priloge I od proizvajalcev zahteva, da javno razkrijejo informacije o odpravljenih ranljivostih, ko je na voljo varnostna posodobitev.

9.2 **Obravnavanje ranljivosti**

9.2.1 *Poročanje navzgor v verigi in deljenje varnostnih popravkov*

222. Člen 13(6) akta o kibernetski odpornosti od proizvajalcev zahteva, da o ranljivostih v vgrajenih sestavnih delih obvestijo osebo ali subjekt, ki ta sestavni del izdeluje ali vzdržuje („poročanje navzgor v verigi“).

223. Proizvajalci morajo navzgor v verigi poročati le v zvezi z vgrajeno različico sestavnega dela. Kadar ima oseba ali subjekt, ki sestavni del izdeluje ali vzdržuje, vzpostavljene varnostne politike, postopke usklajenega razkrivanja ranljivosti ali namenske kanale za poročanje o ranljivostih, bi morali proizvajalci poročati v skladu z njimi, zlasti kadar bi prezgodnje razkritje nepopravljenih ranljivosti lahko povečalo tveganja za kibernetsko varnost. Da bi se zmanjšalo breme za vzdrževalce višje v verigi, zlasti v odprtokodnih projektih, proizvajalcem ni treba poročati navzgor v verigi, kadar lahko potrdijo, da je oseba ali subjekt, ki sestavni del izdeluje ali vzdržuje, že seznanjen z ranljivostjo. Proizvajalce se spodbuja, naj sprejmejo razumne ukrepe, da se prepreči predložitev podvojenih poročil, na primer tako, da pred poročanjem navzgor v verigi preverijo javno dostopne podatkovne zbirke ranljivosti, varnostna obvestila za posamezne projekte ali uveljavljene sledilnike težav.

224. Proizvajalci morajo navzgor v verigi poročati le o ranljivostih v samem vgrajenem sestavnem delu, ne pa o ranljivostih, ki so posledica integracije med sestavnim delom in drugo kodo, ki jo je razvil proizvajalec, ali vgradnje drugih sestavnih delov. Kljub temu lahko pride do primerov, ko vgradnja sestavnega dela v nek izdelek z digitalnimi elementi razkrije določena vedenja, interakcije ali značilnosti takega sestavnega dela, pomembne za varnost, ki sami zase niso bili očitni ali zlahka prepoznavni. V takih primerih se proizvajalce spodbuja, naj te informacije sporočijo osebi ali subjektu, ki sestavni del izdeluje ali vzdržuje, da bi se spodbujale dobre prakse obravnavanja ranljivosti, namenjene olajšanju učinkovitega odpravljanja ranljivosti in izboljšanju splošne varnosti ekosistema sestavnega dela.

225. Proizvajalcem pa prav tako ni treba poročati o ranljivosti navzgor v verigi, kadar sestavni del nima več vzdrževalca ali kadar se proizvajalec pri novih različicah ali varnostnih popravkih ne zanaša več na prvotnega vzdrževalca. V teh primerih se proizvajalca vseeno spodbuja, naj uporabnike takega sestavnega dela obvesti z razumnimi alternativnimi ukrepi, npr. prek obstoječih mehanizmov skupnosti (kot so poštni seznami ali prijave težav) ali prek javnih evidenc ranljivosti.

226. Proizvajalci, ki so razvili spremembo programske opreme za odpravo ranljivosti v vgrajenem sestavnem delu, morajo v skladu s členom 13(6) to spremembo programske opreme („varnostni popravek“) deliti z osebo ali subjektom, ki sestavni del izdeluje ali vzdržuje („deljenje navzgor v verigi“).

227. Kadar morajo proizvajalci v skladu s členom 13(6) deliti varnostni popravek, bi bilo treba popravek po potrebi zagotoviti v strojno berljivi obliki, na način, ki osebi ali subjektu, ki sestavni del izdeluje ali vzdržuje, omogoča, da ga zlahka preveri in, kadar je ustrezno, vgradi. Kadar je sestavni del sestavni del proste in odprtokodne programske opreme, bi bilo treba varnostni popravek deliti na način, ki je združljiv z licenco tega sestavnega dela, na primer tako, da se deli na podlagi iste licence ali licence, ki vzdrževalcu omogoča, da popravek distribuira na podlagi svoje licence. Kadar ima vzdrževalec takega sestavnega dela usmeritve o tem, kako bi bilo treba deliti varnostne popravke, bi jih moral proizvajalec upoštevati.

228. Vendar proizvajalci na podlagi akta o kibernetski odpornosti niso obvezani zagotoviti, da oseba ali subjekt, ki sestavni del izdeluje ali vzdržuje, nujno sprejme njihove varnostne popravke. Prav tako jim ni treba zagotoviti, da se ti popravki nujno vključijo v repozitorij kode sestavnega dela, na primer kadar bi vzdrževalec morda raje uporabil drugo možnost za odpravo težave. Podobno proizvajalci niso dolžni sprejeti predlaganega popravka, ki ga je razvil vzdrževalec sestavnega dela, in lahko težavo raje ublažijo na druge ustrezne načine.

229. V nekaterih primerih je oseba ali subjekt, ki sestavni del izdeluje ali vzdržuje, morda že zagotovil varnostni popravek za odpravo ranljivosti, vendar proizvajalec uporabi drugačno strategijo za zmanjšanje tveganja (na primer s spremembo druge konfiguracije). V takih primerih akt o kibernetski odpornosti od proizvajalca ne zahteva, da sporoči spremembo drugega dela sistema navzgor v verigi. Proizvajalca se vseeno spodbuja, naj to stori, kadar lahko s tem podpre osebo ali subjekt, ki vzdržuje sestavni del.

9.2.2 *Znane izrabljive ranljivosti*

230. Ena od bistvenih zahtev iz dela I Priloge I k aktu o kibernetski odpornosti določa, da morajo biti izdelki z digitalnimi elementi na podlagi ocene tveganja za kibernetsko varnost iz člena 13(2) in kadar je to ustrezno, dostopni na trgu brez znanih izrabljivih ranljivosti.

231. Člen 3(41) opredeljuje „izrabljivo ranljivost“ kot „ranljivost, ki jo lahko nasprotnik učinkovito uporabi v praktičnih pogojih delovanja“. Vseh ranljivosti ni mogoče izrabiti v praktičnih pogojih delovanja, nekatere ranljivosti pa je mogoče izrabiti le v teoretičnih pogojih (npr. v laboratoriju ali simulaciji) in/ali ne v pogojih, ki bi nastali v operativnem okolju izdelka z digitalnimi elementi.

232. Akt o kibernetski odpornosti od proizvajalcev zahteva, da imajo vzpostavljene ustrezne politike in postopke za obravnavo in odpravo morebitnih ranljivosti, ki jih sporočijo notranji ali zunanji viri (člen 13(8)). Vendar v njem ni izrecno določeno, kdaj bi bilo treba šteti, da je proizvajalec seznanjen z izrabljivo ranljivostjo, s čimer se sproži obveznost izpolnjevanja te bistvene zahteve v trenutku dajanja na trg.

233. Ranljivost bi bilo treba šteti za znano, kadar je navedena v ustreznih javno dostopnih podatkovnih zbirkah ranljivosti, kot je evropska podatkovna zbirka ranljivosti, vzpostavljena na podlagi člena 12(2) Direktive (EU) 2022/2555, ali v drugih pomembnih podatkovnih zbirkah ranljivosti.

234. Poleg tega je ranljivost lahko znana tudi, kadar je bil proizvajalec z njo seznanjen prek informacij, ki niso javne, na primer prek usklajenega razkritja s strani raziskovalca varnosti ali prek proizvajalčevega lastnega notranjega preskušanja in analize, tudi na primer pri uporabi storitev, podprtih z UI. Ranljivost je lahko znana tudi, kadar se je o njej javno in vidno poročalo v zanesljivih medijih, vključno s specializiranimi publikacijami o kibernetski varnosti ali splošnimi množičnimi mediji.

235. Vendar zgolj to, da se o ranljivosti poroča ali da je ugotovljena, samo po sebi ne pomeni, da jo je mogoče v praksi izrabiti ali da se nanaša na zadevni izdelek z digitalnimi elementi. Proizvajalec jo bo moral raziskati ter potrditi resničnost takih informacij in njihovo uporabnost za svoj izdelek z digitalnimi elementi. Zato lahko med prvim poročanjem o ranljivosti in njeno potrditvijo preteče določeno časovno obdobje. Kot je navedeno v oddelku *9.1 Reporting obligations*, bi moral biti poudarek na hitrem ukrepanju za preiskavo in odziv.

236. Poleg tega se v skladu s členom 13(1) obveznost izpolnjevanja bistvene zahteve iz dela I Priloge I za proizvajalce uporablja v trenutku dajanja na trg. V praksi se lahko zgodi, da se nove potencialno izrabljive ranljivosti odkrijejo v zadnjih fazah življenjskega cikla razvoja izdelka z digitalnimi elementi, tudi tik preden vstopi v distribucijsko verigo (in se torej da na trg).

237. Ker je obveznost dajanja izdelkov z digitalnimi elementi na trg brez znanih izrabljivih ranljivosti obveznost, ki temelji na tveganju, mora proizvajalec na podlagi ocene tveganja za kibernetsko varnost ugotoviti, ali je mogoče izdelek z digitalnimi elementi varno dati na trg v skladu z aktom o kibernetski odpornosti. Proizvajalec lahko tudi ugotovi, da je treba pred dajanjem izdelka z digitalnimi elementi na trg odpraviti novo ranljivost, ki je morda postala znana. Proizvajalci bi morali pri tej ugotovitvi upoštevati resnost, izrabljivost in morebitni vpliv ranljivosti ter tveganja, ki nastanejo za sam izdelek z digitalnimi elementi, ko je v uporabi. Upoštevajo lahko tudi tveganja zaradi odložitve izdaje izdelka do odprave ranljivosti, na primer ker se z novo izdajo obravnavajo tudi druge izrabljive ranljivosti ali ker je potrebna za nadaljnje delovanje kritičnih sistemov. V vsakem primeru za proizvajalca po dajanju izdelka z digitalnimi elementi na trg še naprej velja obveznost učinkovitega obravnavanja ranljivosti v skladu z zahtevami glede obravnavanja ranljivosti iz dela II Priloge I.

9.2.3 *Učinkovita in redna preverjanja ter pregledi*

238. Točka 3 dela II Priloge I od proizvajalcev zahteva, da v celotnem obdobju podpore izdelka z digitalnimi elementi izvajajo učinkovita in redna preverjanja ter preglede varnosti izdelkov z digitalnimi elementi. Izvajanje rednih preskusov ne pomeni, da je treba v fiksnih časovnih presledkih mehansko ponavljati nespremenjeni sklop preskusov. Pomeni redno pregledovanje, ali je treba zaradi novih podatkov, kot so novo ugotovljene grožnje ali novo odkrite ranljivosti, posodobiti obstoječe preskuse, in ustrezno izvajanje preskusov.

239. Pogostost, poglobljenost in vsebina pregleda bi morale biti sorazmerne s profilom tveganja za kibernetsko varnost izdelka z digitalnimi elementi, njegovim razvojem skozi čas in stanjem okolja groženj. Kadar se s pregledom ugotovijo pomembni novi podatki, ki vplivajo na nabor preskusov, bi bilo treba zasnovati nove ali spremenjene preskuse in jih izvesti na izdelku, da nobena ranljivost ne bi ostala neobravnavana. To lahko vključuje ponovno izvedbo obstoječih preskusov, kadar je zaradi spremembe izdelka z digitalnimi elementi takšna vrsta preverjanja ustrezna, na primer regresijsko preskušanje.

240. Kadar se s pregledom ne ugotovijo takšni podatki, ni treba zasnovati dodatnih preskusov. Druge obveznosti obravnavanja ranljivosti, vključno z obveznostjo obravnavanja in odpravljanja ranljivosti v zvezi s tveganji, se še naprej uporabljajo vzporedno.

9.3 **Medsebojni vpliv med to uredbo in drugo zakonodajo**

9.3.1 *Uredba (EU) 2019/2144 in Uredba (EU) št. 168/2013*

241. Člen 2(2), točka (c), akta o kibernetski odpornosti določa, da se Uredba ne uporablja za izdelke z digitalnimi elementi, za katere se uporablja Uredba (EU) 2019/2144. Uredba (EU) 2019/2144 se uporablja za „vozila kategorij M, N in O, kot so opredeljene v členu 4 Uredbe (EU) 2018/858, ter za sisteme, sestavne dele in samostojne tehnične enote, zasnovane in izdelane za taka vozila“.

242. Podobno so bili izdelki z digitalnimi elementi, ki spadajo na področje uporabe Uredbe (EU) št. 168/2013, z Delegirano uredbo Komisije (EU) 2025/1535 izključeni s področja uporabe akta o kibernetski odpornosti. Uredba (EU) št. 168/2013 se uporablja za vozila kategorije L in „za sisteme, sestavne dele in samostojne tehnične enote, dele in opremo, zasnovane in izdelane za taka vozila“ (člen 2(1)).

243. Akt o kibernetski odpornosti se ne uporablja za vozila, za katera se uporabljata navedeni uredbi. Poleg tega so potrebna dodatna pojasnila glede obsega izjeme za sisteme, sestavne dele, samostojne tehnične enote, dele in opremo (za namene tega oddelka: sestavni deli), ki so zasnovani in izdelani za taka vozila ter se štejejo za izdelke z digitalnimi elementi v smislu akta o kibernetski odpornosti.

244. Šteje se, da se akt o kibernetski odpornosti ne uporablja za take sestavne dele, če so zasnovani in izdelani izključno za vgradnjo v vozila, zajeta z uredbama (EU) 2019/2144 in (EU) št. 168/2013. To velja ne glede na to, ali proizvajalec navedenega sestavnega dela tega proda neposredno proizvajalcu vozila ali drugemu gospodarskemu subjektu v avtomobilski dobavni verigi, če je sestavni del jasno namenjen in primeren le za končno vgradnjo v ta vozila.

245. Nasprotno pa akt o kibernetski odpornosti velja za proizvajalca, ki prodaja generične sestavne dele, ki so izdelki z digitalnimi elementi in jih je mogoče vgraditi v različne vrste izdelkov, in ne izključno v vozila, zajeta z navedenima uredbama.

246. Ocena, ali je sestavni del dan na trg v smislu akta o kibernetski odpornosti, mora temeljiti na objektivnih pogojih, pod katerimi je omogočena njegova dostopnost. Kadar proizvajalec sestavni del, ki ni primeren izključno za končno vgradnjo v navedena vozila, ponuja prek distribucijskih kanalov, ki so odprti za stranke zunaj avtomobilske dobavne verige, kot so splošna maloprodajna mesta ali spletni prodajni kanali, ki sprejemajo naročila splošne javnosti, ta sestavni del spada na področje uporabe akta o kibernetski odpornosti, ne glede na izjave o njegovi predvideni uporabi. V takih okoliščinah ni mogoče šteti, da je sestavni del zasnovan in izdelan izključno za vgradnjo v vozila, zajeta z uredbama (EU) 2019/2144 in (EU) št. 168/2013, proizvajalec pa mora ravnati v skladu z aktom o kibernetski odpornosti. Nasprotno pa lahko uporaba omejenih distribucijskih kanalov med podjetji, omejenih na avtomobilsko dobavno verigo, kaže, da je zasnovan in izdelan izključno za tako vgradnjo.

9.3.2 *Veljavnost potrdil o EU-pregledu tipa (člen 69(1))*

247. V členu 69(1) akta o kibernetski odpornosti je navedeno, da „[p]otrdila o EU-pregledu tipa in sklepi o odobritvi, izdani v zvezi z zahtevami glede kibernetske varnosti za izdelke z digitalnimi elementi, za katere se uporablja druga harmonizacijska zakonodaja Unije, ki ni ta uredba, ostanejo veljavni do 11. junija 2028, razen če potečejo pred tem datumom ali če je drugače določeno v tej drugi harmonizacijski zakonodaji Unije, pri čemer v takem primeru ostanejo veljavni, kakor je določeno v navedeni zakonodaji.“

248. Nadaljnjo veljavnost takih potrdil in sklepov o odobritvi bi bilo treba razumeti kot omejeno na tveganja za kibernetsko varnost in ustrezne zahteve, zajete v zadevni harmonizacijski zakonodaji Unije, na podlagi katere so bili izdani. Proizvajalcem v obdobju veljavnosti iz člena 69(1) za ta tveganja zgolj za namene akta o kibernetski odpornosti ni treba ponovno oceniti ali ponovno dokazati skladnosti izdelkov z digitalnimi elementi, ki jih nameravajo dati na trg 11. decembra 2027 ali po tem datumu in do 11. junija 2028 ([31]). To velja za potrdila in sklepe o odobritvi, izdane v primerih, ko veljavna harmonizacijska zakonodaja Unije zahteva, da proizvajalec izvede postopek ugotavljanja skladnosti prek priglašenega organa, pa tudi v primerih, ko se je proizvajalec za to odločil prostovoljno.

249. Zato obstoj veljavnega potrdila ali sklepa o odobritvi na podlagi druge harmonizacijske zakonodaje Unije proizvajalcev ne oprošča obveznosti izvedbe celovite ocene tveganja za kibernetsko varnost na podlagi akta o kibernetski odpornosti (ali drugih obveznosti na njegovi podlagi). Namesto tega jim omogoča, da se v svojem postopku ugotavljanja skladnosti oprejo na obstoječe certifikate kot dokazila o skladnosti, kolikor so ustrezna tveganja za kibernetsko varnost že zajeta. Kadar potrdilo ali sklep o odobritvi na podlagi druge harmonizacijske zakonodaje Unije velja dlje od 11. junija 2028, se lahko proizvajalec kljub temu na tako potrdilo ali sklep za namene akta o kibernetski odpornosti sklicuje le do 11. junija 2028.

250. Kadar so v oceni tveganja za kibernetsko varnost, izvedeni v skladu s členom 13(2), ugotovljena dodatna tveganja, ki niso zajeta z zahtevami glede kibernetske varnosti, na katerih temelji obstoječe potrdilo ali sklep o odobritvi, proizvajalci ostanejo odgovorni za obravnavanje teh tveganj v skladu z aktom o kibernetski odpornosti. V takih primerih je za skladnost treba ugotovljene vrzeli oceniti in ublažiti, ne glede na nadaljnjo veljavnost obstoječega potrdila ali sklepa o odobritvi.

251. To je mogoče ponazoriti s primerom, ko za izdelek z digitalnimi elementi veljajo zahteve glede kibernetske varnosti, določene v Delegirani uredbi Komisije (EU) 2022/30 o dopolnitvi Direktive 2014/53/EU (delegirani akt direktive o radijski opremi), in je bilo na podlagi teh zahtev izdano potrdilo o EU-pregledu tipa ali sklep o odobritvi. V tem primeru potrdilo ali sklep v skladu s členom 69(1) ostane veljaven za tveganja za kibernetsko varnost, zajeta s tem potrdilom in povezana z bistvenimi zahtevami glede kibernetske varnosti iz Direktive 2014/53/EU (direktiva o radijski opremi).

252. V takih primerih proizvajalcem za namene akta o kibernetski odpornosti ni treba ponovno oceniti ali ponovno dokazati skladnosti v zvezi s tistimi tveganji, ki so že obravnavana s temi potrdili, dokler velja zadevno potrdilo ali sklep o odobritvi, v nobenem primeru pa ne po 11. juniju 2028. To na primer vključuje tveganja za kibernetsko varnost, povezana z zaščito omrežja, varstvom osebnih podatkov in zasebnosti ali preprečevanjem goljufij (kolikor so ta tveganja zajeta z navedenim potrdilom), na katere se nanašajo zahteve iz direktive o radijski opremi glede kibernetske varnosti in ki so upoštevana v postopku ugotavljanja skladnosti.

253. Kadar pa so v oceni tveganja za kibernetsko varnost, izvedeni v skladu s členom 13(2) akta o kibernetski odpornosti, ugotovljena dodatna tveganja za kibernetsko varnost, ki niso zajeta s temi potrdili, proizvajalci ostanejo odgovorni za obravnavanje teh tveganj v skladu z aktom o kibernetski odpornosti. To lahko na primer vključuje tveganja, povezana s postopki obravnavanja ranljivosti, najmanjšim obsegom podatkov in zmanjšanjem napadne površine, ali druge za izdelek značilne vidike kibernetske varnosti, ki jih navedena potrdila ne obravnavajo oziroma ki v nobenem primeru niso zajeta z bistvenimi zahtevami direktive o radijski opremi glede kibernetske varnosti.

254. Zato obstoj veljavnega potrdila o EU-pregledu tipa ali sklepa o odobritvi na podlagi direktive o radijski opremi za njene bistvene zahteve, povezane s kibernetsko varnostjo, sam po sebi ne dokazuje popolne skladnosti z aktom o kibernetski odpornosti. Namesto tega proizvajalcem omogoča, da se na navedeno potrdilo ali sklep oprejo kot na dokazilo o skladnosti za ustrezna tveganja, hkrati pa zagotovijo, da se vsa preostala ali na novo ugotovljena tveganja ocenijo in zmanjšajo v skladu z aktom o kibernetski odpornosti.

([31]) Za izdelke z digitalnimi elementi, dane na trg pred 11. decembrom 2027, se uporablja zakonodaja Unije, ki je veljala, ko so bili dani na trg, in če so bili skladni, se lahko prodajajo in dajo v obratovanje, razen če so bistveno spremenjeni 11. decembra 2027 ali po tem datumu. Za pojma „dajanje na trg“ in „omogočanje dostopnosti na trgu“ glej tudi oddelek *2.1 Placing on the market* tega dokumenta ter poglavje 2 Modrega vodnika.

255. Podobno velja, da kadar za izdelek z digitalnimi elementi veljajo bistvene zdravstvene in varnostne zahteve, povezane s kibernetsko varnostjo, določene v Uredbi (EU) 2023/1230 (uredba o strojih), ki se v celoti uporablja od 20. januarja 2027, in kadar je bilo na podlagi teh zahtev izdano potrdilo o EU-pregledu tipa ali sklep o odobritvi, ostane to potrdilo ali sklep o odobritvi v skladu s členom 69(1) akta o kibernetski odpornosti veljaven za tveganja za kibernetsko varnost, zajeta z uredbo o strojih.

256. To se zlasti nanaša na vidike kibernetske varnosti, povezane z zaščito pred okvaro ter varnostjo in zanesljivostjo krmilnih sistemov, kot je določeno v oddelkih 1.1.9 in 1.2.1 Priloge III k uredbi o strojih. Za ta tveganja proizvajalcem za namene akta o kibernetski odpornosti ni treba ponovno oceniti ali ponovno dokazati skladnosti, dokler velja zadevno potrdilo ali sklep o odobritvi, v nobenem primeru pa ne po 11. juniju 2028. To velja, če so bila ta tveganja obravnavana v okviru postopka ugotavljanja skladnosti na podlagi uredbe o strojih.

257. Kot pri zgoraj navedenih bistvenih zahtevah iz direktive o radijski opremi glede kibernetske varnosti velja, da kadar se v oceni tveganja za kibernetsko varnost, izvedeni v skladu s členom 13(2) akta o kibernetski odpornosti, ugotovijo dodatna tveganja za kibernetsko varnost, ki niso zajeta z zadevnim potrdilom, izdanim na podlagi uredbe o strojih, in ki so povezana z zahtevami navedene uredbe glede kibernetske varnosti, ostanejo proizvajalci odgovorni za obravnavanje teh tveganj v skladu z aktom o kibernetski odpornosti.