Eiropas Savienības
Oficiālais Vēstnesis

LV
C sērija

C/2026/6013

17.11.2026.

KOMISIJAS PAZIŅOJUMS

Komisijas norādījumi par to, kā piemērojama Regula (ES) 2024/2847 (Kibernoturības akts)

(C/2026/6013)

Saturs

Lappuse

1. IEVADS ... 3
   1.1. Kibernoturības akts ... 3
   1.2. Norādījumu mērķis ... 3
2. DARBĪBAS JOMA ... 4
   2.1. Laišana tirgū ... 4
   2.2. Programmatūra kā produkts ar digitāliem elementiem ... 5
   2.3. Datora kods ... 6
   2.4. Aparatūras un programmatūras kombinācija, kas veido produktu ar digitāliem elementiem ... 7
   2.5. Datu savienojums ... 8
   2.6. Kompleksas sistēmas ... 8
   2.7. Produkti ar digitāliem elementiem, kas projektēti pirms KNA piemērošanas sākuma ... 9
3. BRĪVI PIEEJAMA ATVĒRTĀ PIRMKODA PROGRAMMATŪRA ... 11
   3.1. Kā noteikt, vai brīvi pieejama atvērtā pirmkoda programmatūra ir personas atbildībā ... 12
   3.2. Kā noteikt, vai brīvi pieejama atvērtā pirmkoda programmatūra ir laista ES tirgū ... 13
      3.2.1. Cenas noteikšana ... 13
      3.2.2. Citu pakalpojumu monetizācija vai personas datu apstrādes izvirzīšana par lietošanas nosacījumu ... 13
      3.2.3. Atbalsta pakalpojumi ... 14
      3.2.4. Ziedojumi ... 15
      3.2.5. Brīvi pieejamas atvērtā pirmkoda programmatūras finansēšana ... 15
      3.2.6. Bezpeļņas struktūras, kas izveidotas bezpeļņas mērķu sasniegšanai ... 16
      3.2.7. Integrēšana, ko veic citi ražotāji ... 16
   3.3. Atvērtā pirmkoda programmatūras pārziņi ... 16
      3.3.1. Ilgstošs atbalsts un *FOSS* dzīvotspējas nodrošināšana ... 17
   3.4. Ieguldījuma sniedzēji un lietojumi lejasposmā ... 18
   3.5. Ilustratīvi scenāriji ... 19
4. BŪTISKAS MODIFIKĀCIJAS UN REZERVES DAĻAS ... 21
   4.1. Fizisks remonts ... 22
   4.2. Rezerves daļas ... 23
   4.3. Programmatūras atjauninājumi kā būtiskas modifikācijas ... 24

4.4. Būtiskas modifikācijas sekas 27
4.4.1. Būtiskas modifikācijas, ko veikusi persona, kura nav sākotnējais ražotājs 28
4.4.2. Būtiskas modifikācijas, ko veic sākotnējais ražotājs 29
5. ATBALSTA PERIODS 29
5.1. Būtiskas modifikācijas un atbalsta periods 31
6. NOZĪMĪGI UN KRITISKI SVARĪGI PRODUKTI AR DIGITĀLIEM ELEMENTIEM 32
6.1. Pamatfunkcionalitāte 33
6.2. Nozīmīgu un kritiski svarīgu produktu ar digitāliem elementiem atbilstības novērtēšana 36
6.3. Ietekme uz pieņēmumu par atbilstību 38
7. KIBERDROŠĪBAS RISKA NOVĒRTĒJUMS UN PRODUKTU AR DIGITĀLIEM ELEMENTIEM UN KOMPONENTU INTEGRĀCIJA 41
7.1. Par kiberdrošības risku izvērtēšanu un risināšanu 41
7.2. Produktus ar digitāliem elementiem projektē, izstrādā un ražo tā, lai tie nodrošinātu atbilstošu kiberdrošības līmeni, pamatojoties uz riskiem. 42
7.3. Riska novērtējums un pienācīga pārbaude attiecībā uz ārējām atkarībām un integrētiem komponentiem 42
7.4. Riska novērtējumu un atbilstības dokumentācijas atkārtota izmantošana produktu ar digitāliem elementiem saimēm 44
8. ATTĀLINĀTA DATU APSTRĀDE 44
8.1. Ko uzskata par attālinātas datu apstrādes risinājumu produktam ar digitāliem elementiem? 45
8.1.1. Jēdziens “no attāluma” 46
8.1.2. Vai šādas datu apstrādes neesība liegtu produktam ar digitāliem elementiem veikt kādu no savām funkcijām? 46
8.1.3. Vai programmatūru ir projektējis un izstrādājis ražotājs vai tas ir darīts ražotāja atbildībā? 47
8.2. Attālinātas datu apstrādes risinājumu praktiskās un tehniskās sekas un paļaušanās uz trešo personu risinājumiem 49
8.3. Attālinātas datu apstrādes risinājumu lietojumgadījumi 50
8.3.1. Mobilās bankas lietotne 51
8.3.2. Viedais termostats 52
8.3.3. E-lasītājs 53
8.3.4. Rūpniecības robots 53
8.3.5. Mobilo sakaru tīkls 53
9. PAPILDU ELEMENTI 54
9.1. Ziņošanas pienākumi 54
9.2. Ievainojamību novēršana 56
9.2.1. Ziņošana augšposmā un drošības labojumu kopīgošana 56
9.2.2. Zināmās izmantojamās ievainojamības 57
9.2.3. Efektīvi un regulāri testi un pārskati 58
9.3. Mijiedarbība ar citiem tiesību aktiem 59
9.3.1. Regula (ES) 2019/2144 un Regula (ES) Nr. 168/2013 59
9.3.2. ES tipa pārbaudes sertifikātu derīgums (69. panta 1. punkts) 59

1. **IEVADS**

1.1. **Kibernoturības akts**

1. Eiropas Parlamenta un Padomes Regula (ES) 2024/2847 (2024. gada 23. oktobris) par horizontālajām kiberdrošības prasībām attiecībā uz produktiem ar digitāliem elementiem un ar ko groza Regulas (ES) Nr. 168/2013 un (ES) 2019/1020 un Direktīvu (ES) 2020/1828 (Kibernoturības akts) ([1]) stājās spēkā 2024. gada 10. decembrī. Regulas mērķis ir stiprināt Savienības pieeju attiecībā uz kiberdrošību, pievērsties kibernoturībai Savienības līmenī un uzlabot iekšējā tirgus darbību, nosakot vienotu tiesisko regulējumu kiberdrošības pamatprasībām attiecībā uz produktu ar digitāliem elementiem laišanu Savienības tirgū, kā arī visā produkta ar digitāliem elementiem aprites ciklā.

2. Kibernoturības akta (KNA) pamatā ir ES jaunais tiesiskais regulējums (JTR), kas izklāstīts Eiropas Parlamenta un Padomes 2008. gada 9. jūlija Regulā (EK) Nr. 765/2008, ar ko nosaka akreditācijas un tirgus uzraudzības prasības attiecībā uz produktu tirdzniecību un atceļ Regulu (EEK) Nr. 339/93, un Eiropas Parlamenta un Padomes 2008. gada 9. jūlija Lēmumā Nr. 768/2008/EK par produktu tirdzniecības vienotu sistēmu un ar ko atceļ Padomes Lēmumu 93/465/EEK ([2]).

3. Tirgus uzraudzību un izpildes panākšanu veic valstu tirgus uzraudzības iestādes. Produktiem ar digitāliem elementiem, kas ietilpst KNA darbības jomā, piemēro Eiropas Parlamenta un Padomes Regulu (ES) 2019/1020 (2019. gada 20. jūnijs) par tirgus uzraudzību un produktu atbilstību un ar ko groza Direktīvu 2004/42/EK un Regulas (EK) Nr. 765/2008 un (ES) Nr. 305/2011. Komisija un Eiropas Savienības Kiberdrošības aģentūra (*ENISA*) atbalsta uzņēmējus un dalībvalstis KNA piemērošanā.

1.2. **Norādījumu mērķis**

4. KNA 26. panta 1. punktā Komisijai ir noteikts pienākums publicēt norādījumus, kas uzņēmējiem palīdz piemērot regulu, īpašu uzmanību pievēršot tam, lai mikrouzņēmumiem un mazajiem un vidējiem uzņēmumiem (MVU) atvieglotu atbilstības nodrošināšanu. KNA 26. panta 2. punktā ir noteikti minimālie aspekti, kas būtu jāaplūko norādījumos. Tie ir šādi: i) KNA darbības joma (it īpaši attālinātas datu apstrādes risinājumi un brīvi pieejama atvērtā pirmkoda programmatūra), ii) "atbalsta periodu" jēdziens, iii) KNA mijiedarbība ar citiem ES tiesību aktiem un iv) "būtiskas modifikācijas" jēdziens.

5. Komisija 2025. gada 3. decembrī publicēja bieži uzdoto jautājumu (BUJ) kopumu, kura mērķis ir palīdzēt uzņēmējiem sagatavoties KNA īstenošanai ([3]).

6. Šo norādījumu mērķis ir palīdzēt uzņēmējiem nodrošināt atbilstību KNA un atbalstīt tirgus uzraudzības iestāžu, paziņojošo iestāžu un paziņoto struktūru darbību, lai nodrošinātu KNA saskaņotu izpildes panākšanu visā Savienībā. Šo norādījumu mērķis nav aptvert visu KNA darbības jomu, bet gan skaidrot dažu galveno noteikumu pamatojumu un to, kā šos noteikumus varētu īstenot praksē. Šie norādījumi attiecas uz KNA un nav piemērojami citiem ES tiesību aktiem.

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

([2]) Komisijas 2026. gada darba programmā ir paredzēts nākt klajā ar "Eiropas produktu aktu", ar ko atjaunināt JTR un noteikumus par tirgus uzraudzību un standartizāciju: https://eur-lex.europa.eu/legal-content/LV/TXT/?uri=CELEX:52025DC0870.

([3]) BUJ var lejupielādēt Komisijas KNA īstenošanas tīmekļvietnē, īpašajā BUJ tīmekļlapā.

7. Sagatavojot šos norādījumus, notika plaša apspriešanās ar ieinteresētajām personām, tostarp ar ekspertu grupu produktu ar digitāliem elementiem kiberdrošības jautājumos ([4]), kā arī sabiedriskā apspriešana, kas notika no 2026. gada 3. marta līdz 13. aprīlim ([5]).

8. Šie norādījumi nav saistoši uzņēmējiem vai citiem aktoriem, uz kuriem attiecas KNA. Autoritatīvu KNA interpretāciju var sniegt tikai Eiropas Savienības Tiesa. Tomēr šajos norādījumos ir izklāstīta Komisijas KNA interpretācija ar mērķi atbalstīt atbilstības nodrošināšanu un veicināt regulas efektīvu īstenošanu. Turklāt norādījumos ir ietverti vairāki piemēri, kas ilustrē konkrētu noteikumu piemērošanu. Tomēr šie piemēri nav paredzēti, lai aizstātu izvērtējumu katrā konkrētā gadījumā, kas vienmēr būs vajadzīgs, lai ņemtu vērā katra gadījuma īpatnības.

9. Saskaņā ar KNA 26. pantu Komisija var apsvērt papildu norādījumu izdošanu, tostarp norādījumus, kas paredzēti ražotājiem, uz kuriem attiecas KNA un citi Savienības saskaņošanas tiesību akti, vai citi saistīti Savienības tiesību akti. Šie norādījumi var, piemēram, aplūkot jautājumus par KNA mijiedarbību ar Regulu (ES) 2024/1689, ar ko nosaka saskaņotas normas mākslīgā intelekta jomā (MI akts), un Regulu (ES) 2022/2554 par finanšu sektora digitālās darbības noturību (*DORA*).

2. **DARBĪBAS JOMA**

2.1. **Laišana tirgū**

10. KNA attiecas uz produktiem ar digitāliem elementiem, kas tiek darīti pieejami ES tirgū. KNA 3. panta 22. punktā jēdziens "darīt pieejamu tirgū" ir definēts kā "veicot komercdarbību, par maksu vai bez maksas piegādāt izplatīšanai vai izmantošanai Savienības tirgū produktu ar digitāliem elementiem". Saskaņā ar 3. panta 21. punktu produktu ar digitāliem elementiem laiž ES tirgū, kad tas pirmoreiz tiek darīts pieejams.

11. 2022. gadā publicētās "zilās rokasgrāmatas" par ES produktu noteikumu īstenošanu jaunākajā izdevumā (turpmāk – "zilā rokasgrāmata") ([6]) ir sniegti norādījumi, kas palīdz izprast ES produktu noteikumus un tos vienādi piemērot dažādos nozaru tiesiskajos regulējumos, kuri saskaņoti ar jauno tiesisko regulējumu (JTR), piemēram, KNA. Zilajā rokasgrāmatā ir norādīts, ka jēdzieni "laist tirgū" un "darīt pieejamu" ir jāsaprot kā tādi, kas attiecas uz "katru atsevišķi izgatavotu produktu, nevis uz produkta veidu, un nav būtiski, vai tas ir ražots kā atsevišķa vienība vai sērijveidā" (2.3. iedaļa).

12. Attiecībā uz "tradicionālākiem" JTR aptvertiem produktiem ar digitāliem elementiem, piemēram, tādiem aparatūras produktiem ar digitāliem elementiem kā mašīnas vai radioiekārtas, jēdziens "laišana tirgū" ir vispāratzīts, un zilajā rokasgrāmatā ir sniegti papildu norādījumi, kas palīdz precizēt, kad šādus produktus uzskata par laistiem tirgū. Zilās rokasgrāmatas 2.12. iedaļā ietvertajos "kopsavilkuma piemēros" ir sniegti papildu piemēri par jēdzienu "laišana tirgū".

13. Tomēr, ņemot vērā nemateriālu produktu ar digitāliem elementiem (piemēram, savrupās programmatūras) būtību, ir vajadzīgi papildu norādījumi par to, kad šādus produktus ar digitāliem elementiem uzskata par laistiem tirgū. Kad programmatūras ražošanas posms ir noslēdzies un produkts ar digitāliem elementiem tiek piedāvāts potenciālajiem lietotājiem ES tirgū, var uzskatīt, ka tā ražotājs ir izgatavojis vairākas viena un tā paša programmatūras produkta ar digitāliem elementiem kopijas un piegādājis tās izplatīšanai vai izmantošanai. Faktiski atšķirībā no materiāliem produktiem ar digitāliem elementiem uz savrupu programmatūru neattiecas fiziskās

([4]) Komisijas ekspertu grupu un citu līdzīgu struktūru reģistrā iekļautā ekspertu grupa produktu ar digitāliem elementiem kiberdrošības jautājumos.
([5]) Sabiedriskā apspriešana par Komisijas norādījumu projektu par Kibernoturības aktu.
([6]) Komisijas paziņojums ""Zilā rokasgrāmata" par ES produktu noteikumu īstenošanu, 2022. gads" 2022/C 247/01 (OV C 247, 29.6.2022., 1. lpp.).

ražošanas vai krājumu ierobežojumi: ikreiz, kad programmatūra tiek darīta pieejama lejupielādei vai izplatīšanai, lietotājam tiek izveidota jauna identiska kopija. Kamēr šī programmatūras versija netiek modificēta tā, ka tiek ietekmēta atbilstība KNA, uzskata, ka laišana ES tirgū ir notikusi brīdī, kad tā pirmoreiz piedāvāta izplatīšanai vai izmantošanai. Tāpēc šā programmatūras produkta ar digitāliem elementiem versijas turpmākas lejupielādes vai izplatīšanas iespēja ir uzskatāma par gadījumu, kad šis programmatūras produkts ar digitāliem elementiem tiek darīts pieejams ([7]).

14. Tādēļ būtu jāuzskata, ka savrups programmatūras produkts ar digitāliem elementiem ir laists tirgū, kad ir pabeigts tā ražošanas posms un šī programmatūra pirmoreiz tiek piegādāta izplatīšanai vai izmantošanai ES tirgū, veicot komercdarbību. Būtu jāuzskata, ka ražotājs vienlaikus ir laidis tirgū vairākas viena un tā paša programmatūras produkta ar digitāliem elementiem kopijas. Tāpēc, lai gan vairākas viena un tā paša programmatūras produkta kopijas joprojām ir atsevišķi produkti ar digitāliem elementiem, uzskata, ka tās tiek laistas tirgū vienlaikus neatkarīgi no tā, kad katra atsevišķā kopija tiek nodota citas fiziskas vai juridiskas personas valdījumā vai lietošanā. Savukārt, ja ražotājs dara programmatūru pieejamu dažādos variantos, kas atšķiras pēc tajos iekļautajiem komponentiem, konfigurācijām vai iespējotajām funkcijām (piemēram, versijas dažādām operētājsistēmām vai komplekti ar atšķirīgu funkciju kopumu), šos variantus nevar uzskatīt par vairākām viena un tā paša programmatūras produkta ar digitāliem elementiem kopijām. Tāpēc laišanas tirgū vajadzībām tie būtu jāuzskata par atsevišķiem produktiem ar digitāliem elementiem.

1. piemērs: 2028. gada 1. janvārī uzņēmums A savā tīmekļvietnē pirmoreiz piegādā izplatīšanai savas programmatūras X 1.0.0. versiju. Tajā pašā dienā 1. klients iegādājas programmatūras X versijas 1.0.0 kopiju. 2028. gada 15. janvārī 2. klients iegādājas programmatūras X versijas 1.0.0 kopiju. Abas programmatūras X versijas 1.0.0 kopijas tiek laistas tirgū 2028. gada 1. janvārī.

15. Ņemot vērā programmatūras izstrādes iteratīvo raksturu, būtu sīkāk jāprecizē, ka programmatūras produkta ar digitāliem elementiem turpmākās iterācijas uzskata par no jauna laistām tirgū, ja tās kvalificējas kā jau tirgū laista programmatūras produkta ar digitāliem elementiem būtiskas modifikācijas, kā norādīts KNA 41. apsvērumā. Iterācijām, kas nav uzskatāmas par būtiskām modifikācijām, ražotājam nav jāveic jauna atbilstības novērtēšanas procedūra, un tāpēc tās nemaina šīs programmatūras laišanas tirgū datumu. Sīkākus norādījumus par būtisku modifikāciju jēdzienu sk. 4. iedaļā *Būtiskas modifikācijas*.

2. piemērs: 2028. gada 1. janvārī uzņēmums A savā tīmekļvietnē pirmoreiz piegādā izplatīšanai programmatūras X 1.0.0. versiju. Tajā pašā dienā 1. klients iegādājas programmatūras X 1.0.0. versijas kopiju. 2028. gada 15. janvārī uzņēmums A izlaiž atjauninātu programmatūras X 1.0.1. versiju, kas nav būtiska modifikācija. 2028. gada 30. janvārī 2. klients iegādājas programmatūras X 1.0.1. versijas kopiju. Gan programmatūras X 1.0.0. versijas kopiju, gan 1.0.1. versijas kopiju uzskata par laistu tirgū 2028. gada 1. janvārī.

16. 13., 14. un 15. punktā izklāstītie norādījumi ir piemērojami tikai tiktāl, ciktāl produkts ar digitāliem elementiem ir savrupa programmatūra. Tas tā nav, piemēram, ja programmatūra ir apvienota ar aparatūru, kā aplūkots *2.4.* iedaļā *Aparatūras un programmatūras kombinācija, kas veido produktu* ar.

2.2. **Programmatūra kā produkts ar digitāliem elementiem**

17. KNA 3. panta 1. punktā produkts ar digitāliem elementiem ir definēts kā "programmatūras vai aparatūras produkts un tā attālinātās datu apstrādes risinājumi, ieskaitot programmatūras vai aparatūras komponentus, kas tiek laisti tirgū atsevišķi". Šādi produkti ar digitāliem elementiem ietilpst KNA darbības jomā, ja to paredzētais nolūks vai pamatoti paredzamais lietojums ietver tiešu vai netiešu loģisku vai fizisku datu savienojumu ar ierīci vai tīklu.

([7]) Saskaņā ar 13. panta 11. punktu ražotāji var uzturēt publiskus programmatūras arhīvus, tādējādi uzlabojot lietotāju piekļuvi iepriekšējām versijām. Šādos gadījumos lietotājus skaidri un viegli pieejamā veidā informē par riskiem, kas saistīti ar neatbalstītas programmatūras lietošanu.

18. Tāpēc KNA var aptvert virkni produktu ar digitāliem elementiem, tostarp: i) savrupo programmatūru, piemēram, lietotnes un datorprogrammas, neatkarīgi no tā, vai tās izplata digitāli vai fiziski, ii) aparatūru ar iegultu programmatūru (piemēram, lietu interneta ierīces, klēpjdatorus, planšetdatorus), iii) savrupo aparatūru (piemēram, integrālās shēmas, mātesplates) un iv) jebkādu atsevišķi piegādātas, bet kopīgai darbībai paredzētas aparatūras un programmatūras kombināciju.

19. Tāpēc savrupā programmatūra ietilpst KNA darbības jomā, ja to laiž tirgū kā produktu ar digitāliem elementiem. Ir lietderīgi nošķirt programmatūras produktus ar digitāliem elementiem, uz kuriem attiecas KNA, no attālināti sniegtiem pakalpojumiem, kas KNA darbības jomā neietilpst.

20. Lai programmatūra ietilptu KNA darbības jomā, programmatūras produkts ar digitāliem elementiem ir jāpiegādā lietotājam, lietotājam tas jāiegūst, un tas jāizmanto lietotāja pusē esošā elektroniskajā informācijas sistēmā vai kā tās daļa. Programmatūra, kas tiek lejupielādēta, instalēta vai citādi piegādāta lietotājam un tiek izpildīta lietotāja elektroniskajā informācijas sistēmā, atbilst šiem kritērijiem, tostarp, piemēram, ja tā ir pārlūkprogrammas paplašinājums vai ar tīmekļa tehnoloģijām izstrādāta lietojumprogramma, kas tiek piegādāta lokālai izpildei.

21. Savukārt programmatūra, kas tiek izpildīta attālināti un kurai lietotājs tikai piekļūst, šā iemesla dēļ vien nav produkts ar digitāliem elementiem. KNA 11. un 12. apsvērumos šis nošķirums ir skaidrots, norādot, ka attālināta apstrāde vai glabāšana KNA darbības jomā ietilpst tikai tiktāl, ciktāl tā ir nepieciešama, lai produkts ar digitāliem elementiem pildītu savas funkcijas (proti, saskaņā ar 3. panta 2. punktā definēto jēdzienu "attālināta datu apstrāde"), nevis pati par sevi kā produkts ar digitāliem elementiem. Tas parasti attiecas uz tīmekļa lietojumprogrammām, tostarp progresīvajām tīmekļa lietotnēm, ja tām piekļūst tikai ar tīmekļa pārlūkprogrammu. Tas pats attiecas uz tīmekļvietnēm: lai gan tīmekļvietnes tehniski ierobežotā apmērā var darboties un tikt izpildītas lietotāja ierīcē, no KNA 12. apsvēruma izriet, ka tīmekļvietnes pašas par sevi nav uzskatāmas par produktiem ar digitāliem elementiem un KNA darbības jomā ietilpst tikai tad, ja tās nodrošina produkta ar digitāliem elementiem funkcionalitāti, proti, tiktāl, ciktāl tās kvalificējamas kā attālināta datu apstrāde (kā sīkāk skaidrots *8.* iedaļā un it īpaši *8.1.2.* iedaļā *Vai šādas datu apstrādes neesība liegtu produktam ar digitāliem elementiem veikt kādu no savām funkcijām?).*

3. piemērs: mobilā lietotne, ko lietotājs lejupielādē no lietotņu veikala un instalē savā viedtālrunī, tiek piegādāta lietotājam un izpildīta lietotāja ierīcē, un tāpēc tā ir produkts ar digitāliem elementiem. Ja to laiž tirgū, veicot komercdarbību, tā var ietilpt KNA darbības jomā.

4. piemērs: datora lietojumprogramma, kas izveidota, izmantojot tīmekļa tehnoloģijas, bet ir ievietota pakotnē lokālai instalēšanai, tiek piegādāta lietotājam un izpildīta lietotāja ierīcē, tāpēc tā ir produkts ar digitāliem elementiem. Ja to laiž tirgū, veicot komercdarbību, tā var ietilpt KNA darbības jomā.

5. piemērs: tīmekļa lietojumprogramma, kurai lietotājs piekļūst tikai ar tīmekļa pārlūkprogrammu, nav produkts ar digitāliem elementiem. Ja vien tā neatbalsta produkta ar digitāliem elementiem funkcionalitāti, tā neietilpst KNA darbības jomā. Savukārt lietojumprogramma, kas lietotājam tiek piegādāta kā lokāli instalēts klients un tiek izpildīta lietotāja ierīcē, ir produkts ar digitāliem elementiem. Ja to laiž tirgū, veicot komercdarbību, tā var ietilpt KNA darbības jomā.

Ja šis klients, lai pildītu vienu vai vairākas savas funkcijas, izmanto attālinātu datu apstrādi, kas atbilst attālinātas datu apstrādes definīcijai, arī šī attālinātā datu apstrāde ir daļa no produkta ar digitāliem elementiem.

6. piemērs: tīmekļvietne, kas tikai sniedz informāciju tās apmeklētājiem un neatbalsta produkta ar digitāliem elementiem funkcionalitāti, pati par sevi nav produkts ar digitāliem elementiem. Tāpēc tā neietilpst KNA darbības jomā.

2.3. **Datora kods**

22. Ir lietderīgi arī precizēt, vai pirmkods var būt programmatūras produkts ar digitāliem elementiem. KNA programmatūra definēta kā "elektroniskās informācijas sistēmas daļa, kura sastāv no datora koda" (3. panta 4. punkts). Datora kods var būt i) mašīnkods, proti, binārā formātā rakstīts instrukciju kopums, ko tieši izpilda datora procesors, vai ii) pirmkods, t. i., programmēšanas valodā rakstīts instrukciju un priekšrakstu kopums, kas, lai dators to varētu izpildīt, ir jākompilē vai jāinterpretē. KNA noteiktā programmatūras definīcija aptver abus.

23. Atsevišķs jautājums ir par to, vai konkrēta datora koda piegāde ir uzskatāma par produkta ar digitāliem elementiem laišanu ES tirgū, jo, lai to šādi klasificētu, ir nepieciešama piegāde, veicot komercdarbību. Pirmkoda gadījumā tas bieži vien tā nav. Piemēram, fizisku vai juridisku personu, kas publiski pieejamos repozitorijos kopīgo brīvi pieejamu atvērtā pirmkoda datora kodu, KNA vajadzībām parasti neuzskata par tādu, kas šo kodu laiž ES tirgū (kā sīkāk aplūkots 3. iedaļā *Brīvi pieejama atvērtā pirmkoda* programmatūra). Nepabeigtu kodu, kas kopīgots produkta ar digitāliem elementiem projektēšanas un izstrādes posmā (piemēram, testēšanai vai pārskatīšanai), KNA vajadzībām arī neuzskata par laistu tirgū, jo tā ražošanas posms nav pabeigts. Tāpat KNA vajadzībām par laistu tirgū neuzskata paraugkodu vai demonstrācijas kodu, kas sniegts pamācību vai mācību materiālu ietvaros ([8]).

24. Savukārt, ja ražotājs saviem klientiem nodrošina datora kodu kā produktu ar digitāliem elementiem, šo kodu uzskata par laistu tirgū neatkarīgi no tā, vai tas ir mašīnkods vai pirmkods ([9]).

7. piemērs: Uzņēmums A licencē pirmkodu uzņēmumam B pielāgojamai iekšējai platformai un šo pirmkodu nodrošina teksta datnē. Pat ja uzņēmumam B šis pirmkods pirms lietošanas vēl ir jāpielāgo un jākompilē, uzņēmums A šo pirmkodu laiž tirgū, tāpēc uz uzņēmumu A attiecas KNA. Uzņēmums A nav atbildīgs par uzņēmuma B vēlāk veikto šā koda pielāgojumu un kompilācijas atbilstību KNA.

2.4. **Aparatūras un programmatūras kombinācija, kas veido produktu ar digitāliem elementiem**

25. Tas, vai programmatūra ir daļa no produkta ar digitāliem elementiem, būtu jānosaka nevis pēc tā, kā vai kad šī programmatūra tiek piegādāta lietotājam, bet gan pēc tā, vai, ņemot vērā produkta paredzēto nolūku un pamatoti paredzamo lietojumu, programmatūra ir nepieciešama, lai produkts ar digitāliem elementiem pildītu tam paredzētās funkcijas. Ja aparatūras produkts ar digitāliem elementiem ir projektēts darbam kopā ar konkrētu tā paša ražotāja nodrošinātu programmatūru, lai pildītu savas funkcijas, aparatūra un šī programmatūra kopā veido produktu ar digitāliem elementiem. Tādēļ programmatūra, kas vajadzīga produkta ar digitāliem elementiem darbināšanai, konfigurēšanai, vadīšanai vai lietošanai atbilstoši tā paredzētajam nolūkam, ir daļa no produkta ar digitāliem elementiem, pat ja tā iegūta pa atsevišķu kanālu (piemēram, lietotņu veikalā, izmantojot lejupielādes saiti vai citu digitālu kanālu pēc aparatūras produkta ar digitāliem elementiem laišanas tirgū). Tādējādi to laiž tirgū tajā pašā brīdī, kad tirgū laiž aparatūras produkta ar digitāliem elementiem vienības.

8. piemērs: Tīkla printeris tiek laists tirgū kā aparatūras produkts ar digitāliem elementiem, savukārt programmatūras draiveri, kas vajadzīgi drukas uzdevumu nosūtīšanai, ierīces konfigurēšanai un tās darbības pārvaldībai, tiek darīti pieejami lejupielādei ražotāja tīmekļvietnē. Lai gan printeris un draiveri tiek piegādāti pa dažādiem kanāliem, tie kopā veido vienu produktu ar digitāliem elementiem, printeri bez draiveriem nevar izmantot paredzētajam nolūkam.

9. piemērs: Lietotāja sirdsdarbības ātruma un aktivitātes mērīšanai tirgū tiek laista valkājama fitnesa ierīce, savukārt ražotāja nodrošināta viedtālruņa lietotne ir vajadzīga, lai attēlotu mērījumus, parādītu vēsturi un ļautu konfigurēt ierīci. Lai gan lietotne tiek lejupielādēta atsevišķi lietotņu veikalā, valkājamā ierīce un lietotne kopā veido vienu produktu ar digitāliem elementiem, jo tās ir projektētas un paredzētas kopīgai darbībai, lai nodrošinātu produkta ar digitāliem elementiem funkcionalitāti.

([8]) Būtu arī jāatgādina, ka 4. panta 3. punkts ļauj ražotājiem darīt pieejamu tirgū nepabeigtu programmatūru, kas neatbilst regulai, piemēram, alfa versijas, beta versijas vai izlaides kandidātus, ar noteikumu, ka nepabeigtā programmatūra tiek darīta pieejama tikai uz laiku, kas vajadzīgs tās testēšanai un atsauksmju apkopošanai.

([9]) No otras puses, jānorāda, ka produktatbildības tiesību izpratnē datora kods pats par sevi nav produkts, tādēļ ražotājus, kas šādu kodu laiž tirgū, nevar saukt pie atbildības saskaņā ar Direktīvu (ES) 2024/2853 (Produktatbildības direktīva). Minētās direktīvas 13. apsvērumā noteikts, ka "[t]omēr informācija nav uzskatāma par produktu, un tāpēc produktatbildības noteikumus nevajadzētu piemērot digitālo datņu saturam, piemēram, mediju datnēm, e-grāmatām vai programmatūras pirmkodam". Tas neizslēdz, ka ražotāji var būt atbildīgi saskaņā ar valsts deliktu tiesībām.

2.5. **Datu savienojums**

26. KNA 2. panta 1. punktā noteikts, ka šo regulu "piemēro produktiem ar digitāliem elementiem, kuri darīti pieejami tirgū un kuru paredzētais nolūks vai pamatoti paredzamais lietojums ietver tiešu vai netiešu loģisku vai fizisku datu savienojumu ar ierīci vai tīklu". Tādējādi KNA darbības jomas robežu nosaka nevis tikai elektronikas esība, bet produkta ar digitāliem elementiem spēja apmainīties ar digitālu informāciju.

27. Lai gan jēdzieni "loģiskais savienojums" un "fiziskais savienojums" ir definēti 3. pantā, KNA nav definēts ne "datu savienojums", ne "digitālie dati". Tāpēc, lai precizētu KNA darbības jomas robežu, ir lietderīgi izklāstīt, kā interpretējams datu savienojums. Šī robeža ir īpaši svarīga, lai nošķirtu produktus ar digitāliem elementiem, kuros izmanto tikai elektriskos signālus, no produktiem, kas piedalās digitālajā saziņā un tādējādi ir pakļauti kiberdrošības riskiem.

28. Visvienkāršākajā līmenī datu savienojums ietver informācijas pārraidi binārā formā, t. i., 0 un 1 secības veidā. Ar vienkāršu izvades ieslēgšanu un izslēgšanu (t. i., 0/1) pašu par sevi nepietiek, lai pastāvētu datu savienojums, ja šie stāvokļi nav paredzēti datu attēlošanai vai tos nenolasa digitālā ieeja. Lai pastāvētu datu savienojums, avotam binārie stāvokļi apzināti jāiekodē kā informācija, un galamērķī jābūt iespējai tos atkodēt kā informāciju. Citiem vārdiem sakot, ir jābūt sūtītājam, kas apzināti ģenerē digitālus simbolus saskaņā ar noteiktu shēmu, un uztvērējam, kas spēj interpretēt šos simbolus kā datus. Ja elektriskos vai elektroniskos signālus izmanto tikai funkcijas aktivizēšanai vai darbināšanai, nepārraidot digitāli kodētu informāciju, KNA vajadzībām datu savienojuma nav, un tādēļ produkts ar digitāliem elementiem neietilpst 2. panta 1. punkta darbības jomā.

2.6. **Kompleksas sistēmas**

29. KNA darbības jomā ietilpstošie produkti ar digitāliem elementiem var būt ne tikai atsevišķas ierīces vai programmatūras komponenti, bet arī kompleksas sistēmas, tostarp sistēmas, kas sastāv no vairākiem aparatūras un programmatūras elementiem, kuri darbojas kopā, lai pildītu noteiktu funkciju. Ja šādu sistēmu laiž tirgū kā vienu produktu ar digitāliem elementiem, tā ir produkts ar digitāliem elementiem KNA nozīmē.

30. Šādām kompleksām sistēmām bieži raksturīgi ilgstoši projektēšanas un izstrādes cikli, līgumi, kas var būt parakstīti pirms KNA piemērošanas sākuma, ilgs ekspluatācijas laiks un augsta tehniskā un organizatoriskā sarežģītības pakāpe. Šādas sistēmas, ko paredzēts laist tirgū pēc KNA piemērošanas sākuma, var balstīties uz komponentiem, kas laisti tirgū pirms KNA piemērošanas sākuma, uz jau stabili ieviestām arhitektūrām vai plaši izmantotiem sadarbspējas standartiem, tai skaitā standartiem, uz kuriem dotas atsauces citos ES tiesību aktos vai nozaru regulējumos. Tādēļ noteiktus šo sistēmu tehniskos raksturlielumus var būt grūti vai nesamērīgi mainīt, neietekmējot to paredzēto nolūku, drošumu, uzticamību vai sadarbspēju ar esošo infrastruktūru.

31. Šie raksturlielumi paši par sevi neizslēdz kompleksas sistēmas no KNA darbības jomas. Tie drīzāk ilustrē KNA uz riskiem balstītās pieejas piemērošanu, kas saskaņā ar KNA 13. panta 3. punktu ļauj pierādīt atbilstību dažādos veidos atkarībā no produkta ar digitāliem elementiem īpašībām un ierobežojumiem. Šie raksturlielumi ir daļa no produkta paredzētā nolūka un darbības konteksta, tāpēc tie ir būtiski, novērtējot atbilstību kiberdrošības pamatprasībām ("pamatprasības"). Konkrētāk, 55. apsvērumā ir skaidri atzīts, ka dažas pamatprasības var nebūt pilnībā saderīgas ar produkta ar digitāliem elementiem būtību. Piemēram, tā var būt tad, ja atbilstības nodrošināšana apdraudētu obligāto sadarbspējas prasību ievērošanu vai sistēmas pienācīgu darbību.

32. Attiecīgi ražotājiem ir jārisina kiberdrošības riski, pamatojoties uz 13. panta 2. punktā minēto kiberdrošības riska novērtējumu. Kā paskaidrots arī 55. apsvērumā, dažos gadījumos konkrētas pamatprasības nav piemērojamas vai tās nevar izpildīt, ieviešot jaunākajam tehnoloģiju līmenim atbilstošus drošības pasākumus, piemēram, sistēmas

paredzētā nolūka dēļ, kas prasa, lai produkts ar digitāliem elementiem mijiedarbotos ar esošajām atkarībām vai ievērotu konkrētas sadarbspējas prasības. Šādos gadījumos ražotājiem būtu jāidentificē un jādokumentē šie konkrētie ierobežojumi, jānovērtē saistītie riski un jāievieš piemēroti alternatīvi vai kompensējoši riska mazināšanas pasākumi, lai neapdraudētu produkta ar digitāliem elementiem drošību. Šajā nolūkā gan 31. pantā minētajai tehniskajai dokumentācijai, gan II pielikumā minētajai informācijai un norādījumiem lietotājam ir būtiska nozīme, lai pārredzami aprakstītu konstatētos ierobežojumus, saistītos kiberdrošības riskus un ieviestos riska mazināšanas pasākumus. Saskaņā ar pienākumu atbalsta periodā regulāri atjaunināt riska novērtējumu ražotājiem būtu arī periodiski jāpārvērtē, vai šādi ierobežojumi joprojām pastāv. Ja šādus ierobežojumus laika gaitā var atcelt vai samazināt, ražotājiem būtu attiecīgi jāatjaunina produkts ar digitāliem elementiem, lai pakāpeniski sasniegtu atbilstošu kiberdrošības līmeni ([10]).

10. piemērs: ražotājs laiž tirgū produktu ar digitāliem elementiem, kas sazinās ar ārējām sistēmām, izmantojot tīkla protokolu. Piemērojot pamatprasības, ražotājs, pamatojoties uz kiberdrošības riska novērtējumu, nosaka, ka droša sakaru protokola izmantošana ir nepieciešama, lai nodrošinātu to datu konfidencialitāti un integritāti, ar kuriem apmainās produkts ar digitāliem elementiem.

Tomēr tā paredzētais nolūks ietver sadarbspēju ar esošajām sistēmām, kas atbalsta tikai vecāku vai mazāk drošu protokolu. Šādos gadījumos ražotājs var izmantot šo protokolu, ja tas ir nepieciešams sadarbspējas nodrošināšanai, ar noteikumu, ka saistītie kiberdrošības riski tiek identificēti un mazināti ar citiem līdzekļiem.

Ja produkts ar digitāliem elementiem tehniski spēj atbalstīt gan drošo, gan mazāk drošo protokolu, ražotājam būtu jāievieš drošais protokols un jāiespējo tā izmantošana pēc noklusējuma. Mazāk drošo protokolu drīkstētu izmantot tikai tad, ja tas vajadzīgs sadarbspējas nodrošināšanai.

11. piemērs: rūpnieciskās automatizācijas sistēmas ražotājs pirms KNA piemērošanas sākuma iegādājas vairākus mikrokontrollerus. Ražotājs veic tās rūpnieciskās automatizācijas sistēmas kiberdrošības riska novērtējumu, kuru paredzēts laist tirgū pēc KNA piemērošanas sākuma. Pamatojoties uz šo kiberdrošības riska novērtējumu, ražotājs nekonstatē konkrētus kiberdrošības riskus, kas saistīti ar viena no šiem mikrokontrolleriem izmantošanu. Ražotājs to integrē savā rūpnieciskās automatizācijas sistēmā un nodrošina, ka produkts ar digitāliem elementiem kopumā (rūpnieciskās automatizācijas sistēma) atbilst pamatprasībām.

2.7. **Produkti ar digitāliem elementiem, kas projektēti pirms KNA piemērošanas sākuma**

33. Dažos gadījumos pēc tam, kad 2027. gada 11. decembrī sāk piemērot KNA, ražotājs laidīs tirgū produkta ar digitāliem elementiem vienības, kas ražotas atbilstoši tipam vai modelim, kurš projektēts un izstrādāts pirms KNA piemērošanas dienas. Šādos gadījumos atbilstība šai regulai ne vienmēr nozīmē, ka šīs produkta ar digitāliem elementiem vienības ir jāpārprojektē. Ražotājam saskaņā ar KNA 13. panta 2. punktu ir jāveic kiberdrošības riska novērtējums, lai, pamatojoties uz produkta ar digitāliem elementiem paredzēto nolūku un pamatoti paredzamo lietojumu, noteiktu, kuras no I pielikuma I daļā noteiktajām pamatprasībām šim produktam ar digitāliem elementiem ir piemērojamas un kā šīs prasības tiek īstenotas.

34. Ja šā riska novērtējuma rezultāti liecina, ka produktā ar digitāliem elementiem jau ir iestrādāti attiecīgi un efektīvi drošības pasākumi, kas novērš attiecīgos riskus, ražotājs var izmantot šos esošos pasākumus, lai pierādītu atbilstību KNA. KNA pats par sevi neuzliek pienākumu ieviest jaunas drošības funkcijas vai pārprojektēt produktu ar digitāliem elementiem, ja tas nav nepieciešams identificēto risku novēršanai.

([10]) Jānorāda, ka šajā punktā izklāstītie apsvērumi attiecīgā gadījumā var būt piemērojami visiem KNA darbības jomā ietilpstošajiem produktiem ar digitāliem elementiem, ne tikai "kompleksām sistēmām".

35. Tomēr uz ražotāju joprojām attiecas KNA noteiktie pienākumi. Tie ietver pienākumu pirms produkta ar digitāliem elementiem laišanas tirgū pārliecināties, ka ir veikta piemērojamā atbilstības novērtēšanas procedūra, sagatavota ES atbilstības deklarācija un uzlikta *CE* zīme. Atbilstība šīm prasībām nav atkarīga no tā, vai riska novērtējuma rezultātā bija jāmaina produkta ar digitāliem elementiem projektējums. Attiecībā uz produktiem ar digitāliem elementiem, kas projektēti pirms KNA piemērošanas dienas, bet laisti tirgū pēc šīs dienas, ja ražotājs nevar pierādīt, kā riska novērtējums ir ņemts vērā produkta ar digitāliem elementiem projektēšanas un izstrādes posmā, 13. panta 2. punktā noteiktais pienākums būtu jāsaprot kā prasība ražotājiem veikt kiberdrošības riska novērtējumu un, pamatojoties uz to, pierādīt, ka produktā ar digitāliem elementiem ir iestrādāti pienācīgi drošības pasākumi kiberdrošības risku mazināšanai, incidentu novēršanai un to ietekmes mazināšanai, tostarp attiecībā uz lietotāju veselību un drošību.

36. Attiecīgi produktus ar digitāliem elementiem, kas projektēti pirms KNA piemērošanas sākuma, var laist tirgū saskaņā ar KNA bez pārprojektēšanas, ja ražotājs, izmantojot kiberdrošības riska novērtējumu un tehnisko dokumentāciju, var pierādīt, ka produkts ar digitāliem elementiem, ņemot vērā tā paredzēto nolūku un pamatoti paredzamo lietojumu, nodrošina atbilstošu kiberdrošības līmeni un atbilst kiberdrošības pamatprasībām.

37. Turklāt ir lietderīgi precizēt atbilstības novērtēšanas pienākumu piemērošanu tādu produktu ar digitāliem elementiem ražotājiem, kurus laiž tirgū pēc KNA piemērošanas sākuma, bet kuri ražoti atbilstoši tipam vai modelim, kas projektēts un izstrādāts pirms šīs dienas. Saskaņā ar 13. panta 12. punktu ražotājam, izmantojot attiecīgo atbilstības novērtēšanas procedūru, ir jāpierāda, ka tā produkts ar digitāliem elementiem atbilst piemērojamajām kiberdrošības pamatprasībām, un attiecīgie pierādījumi jāiekļauj produkta tehniskajā dokumentācijā (VII pielikuma 6. punkts).

38. Tomēr šo prasību piemērošana ir jāinterpretē, ņemot vērā produkta ar digitāliem elementiem kiberdrošības riska novērtējumu un kiberdrošības riska profilu. It īpaši tādu produktu ar digitāliem elementiem gadījumā, kuri projektēti pirms KNA piemērošanas dienas (bet laisti tirgū pēc šīs dienas) un uz kuriem attiecas 32. panta 1. punktā minētās atbilstības novērtēšanas procedūras, ja riska novērtējums liecina, ka produktā ar digitāliem elementiem jau ir iestrādāti attiecīgi un efektīvi drošības pasākumi, kas novērš šā produkta riskus, pienākums atbilstības novērtēšanas procedūras ietvaros sniegt pierādījumus nebūtu jāsaprot kā prasība ražotājam iesniegt testu rezultātus par šādu produktu ar digitāliem elementiem sākotnējo projektēšanas un izstrādes posmu. Tas nebūtu nepieciešams, jo tādējādi netiktu palielināta paša produkta ar digitāliem elementiem drošība. Ja testi tomēr var būt nepieciešami, no ražotājiem nav sagaidāms, ka tie sniegs pierādījumus par testiem, kas veikti ar visiem produkta variantiem; šādus testus var grupēt pa produktu ar digitāliem elementiem saimēm, kā sīkāk aplūkots *7.4.* iedaļā *Riska novērtējumu un atbilstības dokumentācijas atkārtota izmantošana produktu ar digitāliem elementiem saimēm*.

39. Tomēr ražotājam būtu jāsniedz pierādījumi par to, kā tas ievēro I pielikuma II daļā noteiktos ievainojamību novēršanas procesus, jāatjaunina riska novērtējums saskaņā ar 13. panta 3. punktu un jāizpilda visi pārējie KNA noteiktie pienākumi, tostarp jāsniedz lietotājiem informācija un norādījumi saskaņā ar 13. panta 18. punktu.

12. piemērs: ražotājs laiž tirgū mikrokontrolleri, kas projektēts un izstrādāts pirms KNA piemērošanas dienas. Mikrokontrolleri ir paredzēts integrēt dažādos elektroniskos produktos ar digitāliem elementiem, tostarp produktos ar digitāliem elementiem, kuriem ir savienotības nodrošināšanas funkcijas.

Pirms jaunu mikrokontrollera vienību laišanas tirgū pēc KNA piemērošanas sākuma ražotājs saskaņā ar 13. panta 2. punktu veic kiberdrošības riska novērtējumu. Pamatojoties uz mikrokontrollera paredzēto nolūku un tā pamatoti paredzamo lietojumu, ražotājs identificē attiecīgos kiberdrošības riskus, piemēram, neatļautu piekļuvi, manipulācijas ar programmatūru vai datiem un pieejamo saskarņu ļaunprātīgu izmantošanu.

Riska novērtējuma rezultāti liecina, ka mikrokontrollerī jau tā sākotnējā projektējumā ir iestrādāti attiecīgi un efektīvi drošības pasākumi identificēto risku novēršanai. Tāpēc ražotājs secina, ka produkts ar digitāliem elementiem atbilst attiecīgajām I pielikuma I daļā noteiktajām pamatprasībām un ka nav nepieciešams to pārprojektēt vai ieviest papildu drošības funkcionalitāti.

Ja nav iespējams pierādīt, kā sākotnējā projektēšanas un izstrādes posmā tika ņemts vērā kiberdrošības riska novērtējums, ražotājs dokumentē aktuālu kiberdrošības riska novērtējumu un paskaidro, kā esošais projektējums un pasākumi mazina identificētos riskus. Ražotājam nav no jauna jāizveido vēsturiskā projektēšanas vai testēšanas dokumentācija, jo tas neveicinātu produkta ar digitāliem elementiem kiberdrošības uzlabošanu. Ja vairāki mikrokontrollera varianti ir balstīti uz vienu un to pašu projektējumu un tiem ir vienāds kiberdrošības riska profils, ražotājs var izmantot arī reprezentatīvus pierādījumus, kas attiecas uz attiecīgo produktu saimi.

Ražotājs arī nodrošina atbilstību I pielikuma II daļā noteiktajām ievainojamību novēršanas prasībām, tostarp uzturot procesus, lai pievērstos ievainojamībām un tās novērstu, un saskaņā ar 13. panta 3. punktu regulāri pārskatot kiberdrošības riska novērtējumu.

Šādos apstākļos mikrokontrolleri, kas projektēts pirms KNA piemērošanas dienas, var laist tirgū bez pārprojektēšanas, ja ražotājs, izmantojot kiberdrošības riska novērtējumu un tehnisko dokumentāciju, var pierādīt, ka tas, ņemot vērā tā paredzēto nolūku un pamatoti paredzamo lietojumu, nodrošina atbilstošu kiberdrošības līmeni un atbilst piemērojamajām kiberdrošības pamatprasībām.

3. **BRĪVI PIEEJAMA ATVĒRTĀ PIRMKODA PROGRAMMATŪRA**

40. Kā atgādināts *2.1.* iedaļā *Laišana tirgū*, KNA attiecas uz produktiem ar digitāliem elementiem, kas, veicot komercdarbību, pirmoreiz tiek darīti pieejami ES tirgū (t. i., tiek "laisti tirgū"), kā arī uz katru turpmāku gadījumu, kad tas pats produkts ar digitāliem elementiem tiek darīts pieejams tirgū. Zilajā rokasgrāmatā (2.2. iedaļa) ir precizēts, ka "komercdarbība" ir jāsaprot kā preču nodrošināšana komerciālām darbībām par maksu vai bez maksas, un to var novērtēt tikai katrā gadījumā atsevišķi, ņemot vērā piegādes regularitāti, produkta īpašības, piegādātāja nodomus u. c.

41. Piegādi, veicot komercdarbību, raksturo virkne apstākļu, kas plaši dokumentēti zilajā rokasgrāmatā un atgādināti KNA 15. apsvērumā. Šādi apstākļi var būt tieša cenas noteikšana, kā arī "cenas noteikšana par tehniskā atbalsta pakalpojumiem, ja to ar nolūku izteikt naudas izteiksmē dara ne tikai faktisko izmaksu atgūšanai, piemēram, nodrošinot programmatūras platformu, ar kuras palīdzību ražotājs monetizē citus pakalpojumus, kā lietošanas nosacījumu izvirzot personas datu apstrādi tādu iemeslu dēļ, kas nav tikai programmatūras drošības, savietojamības vai sadarbspējas uzlabošana, vai pieņemot ziedojumus, kas pārsniedz uz produkta ar digitāliem elementiem projektēšanu, izstrādi un piegādi attiecināmās izmaksas" (15. apsvērums) ([11]).

42. Tomēr KNA ņem vērā "brīvi pieejamas atvērtā pirmkoda programmatūras" (*FOSS*) izstrādes un publicēšanas dažādo veidu īpatnības un sniedz norādījumus, kas palīdz noteikt, vai *FOSS* KNA nozīmē ir tirgū laists produkts ar digitāliem elementiem (t. i., piegādāts, veicot komercdarbību). Kā paskaidrots 18. apsvērumā, "tāpēc, nosakot šīs darbības komerciālo vai nekomerciālo raksturu, nevajadzētu ņemt vērā tikai apstākļus, kādos produkts ar digitāliem elementiem ir izstrādāts, vai to, kā šī izstrāde ir finansēta". Konkrētāk, "lai panāktu skaidru nošķiršanu starp izstrādes un piegādes posmu, (..) par komercdarbību nebūtu jāuzskata tādu produktu ar digitāliem elementiem nodrošināšana, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra un kurus to ražotāji nemonetizē".

([11]) Būtu arī jāatgādina, ka, lai gan produkti ar digitāliem elementiem bieži tiek monetizēti (arī) ar personas datu apstrādi, personas datu aizsardzība ir pamattiesības un tāpēc personas datus nevar uzskatīt par preci, kā norādīts 24. apsvērumā Eiropas Parlamenta un Padomes 2019. gada 20. maija Direktīvā (ES) 2019/770 par dažiem digitālā satura un digitālo pakalpojumu piegādes līgumu aspektiem (OV L 136, 22.5.2019., 1. lpp., ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Tāpēc ir lietderīgi i) precizēt, kas ir *FOSS*, ii) precizēt, kad uzskata, ka par to ir atbildīga fiziska vai juridiska persona, un iii) sniegt piemērus, kas ieinteresētajām personām palīdz saprast, kad *FOSS* izplatīšana ir uzskatāma par laišanu tirgū. Ja *FOSS* netiek laista tirgū, tā neietilpst KNA darbības jomā, izņemot gadījumu, kad to publicē juridiska persona, kas atbilst 3. panta 14. punktā noteiktajai "atvērtā pirmkoda programmatūras pārziņa" (turpmāk "pārzinis") definīcijai. Tādā gadījumā uz šo juridisko personu attiecas tikai 24. pantā noteiktie pienākumi.

44. KNA 3. panta 48. punktā *FOSS* ir definēta kā "programmatūra, kuras pirmkods tiek atklāti kopīgots un kura ir pieejama saskaņā ar brīvi pieejamu atvērtā pirmkoda licenci, kas nodrošina visas tiesības padarīt to brīvi pieejamu, lietojamu, modificējamu un tālāk izplatāmu". Lai gan šajos norādījumos nav norādītas konkrētas brīvi pieejama atvērtā pirmkoda licences, kas atbilst 3. panta 48. punktā noteiktajai definīcijai, no minētās normas formulējuma izriet, ka KNA vajadzībām par *FOSS* kvalificējama tikai programmatūra, kas kumulatīvi izpilda divus nosacījumus: i) programmatūrai jābūt darītai pieejamai saskaņā ar brīvi pieejamu atvērtā pirmkoda licenci, kas piešķir visu 3. panta 48. punktā minēto tiesību kopumu, un ii) tās pirmkodam jābūt atklāti kopīgotam.

45. Prasība, ka licencē jāparedz, ka programmatūra ir "brīvi pieejama, lietojama, modificējama un tālāk izplatāma", atspoguļo *FOSS* tradicionālo izpratni, proti, lietotājiem jāspēj piekļūt pirmkodam, izmantot to bez nepamatotiem ierobežojumiem, modificēt un tālāk izplatīt oriģinālās vai modificētās versijas. Tādēļ piekļuve pirmkodam ir nepieciešams priekšnoteikums pārējo tiesību īstenošanai: bez piekļuves pirmkodam praksē nav iespējams programmatūru modificēt vai jēgpilni atkalizmantot.

46. Tomēr 3. panta 48. punkts neaprobežojas tikai ar licences noteikumiem, jo tajā skaidri prasīts, lai pirmkods "tiek atklāti kopīgots". Jēdziens "atklāti kopīgots" nozīmē, ka pirmkods ir jādara publiski pieejams (vai nu augšposmā, vai arī lejasposmā), nevis tikai jānodrošina ierobežotā veidā vai ar nosacījumiem. Attiecīgi programmatūra, kas tiek izplatīta saskaņā ar brīvi pieejamu atvērtā pirmkoda licenci, bet kuras pirmkods tiek kopīgots (vai to atļauts kopīgot) tikai ar maksājošiem klientiem vai ierobežotu lietotāju grupu, nav uzskatāma par *FOSS* 3. panta 48. punkta nozīmē. Tāpēc KNA vajadzībām par *FOSS* būtu jāuzskata tikai tāda programmatūra, kuras pirmkods ir publiski pieejams un kura licencēta saskaņā ar brīvi pieejamu atvērtā pirmkoda licenci, kas piešķir visu 3. panta 48. punktā minēto tiesību kopumu.

3.1. **Kā noteikt, vai brīvi pieejama atvērtā pirmkoda programmatūra ir personas atbildībā**

47. KNA nosaka galvenos pienākumus uzņēmējiem, kas piegādā produktus ar digitāliem elementiem ES tirgū. Tajā ražotājs ir definēts kā fiziska vai juridiska persona, kas ar savu nosaukumu vai preču zīmi piegādā produktu ar digitāliem elementiem un dara to, veicot komercdarbību, (tādējādi laižot produktu tirgū). Līdzīgi importētājs ir ES iedibināta fiziska vai juridiska persona, kas piegādā ārpus ES iedibinātas personas produktu ar digitāliem elementiem un dara to, veicot komercdarbību, (tādējādi laižot to tirgū). Pārziņu pienākumi attiecas uz juridisko personu, kas piegādā komerciālai darbībai paredzētu *FOSS* ([12]), bet KNA nozīmē to nelaiž tirgū.

48. Tāpēc, lai noteiktu, vai fiziska vai juridiska persona laiž *FOSS* ES tirgū, vispirms ir jānoskaidro, vai šī fiziskā vai juridiskā persona *FOSS* patiešām piegādā. Lai pareizi noteiktu KNA paredzētos piemērojamos pienākumus, ir būtiski noskaidrot, vai fiziskā vai juridiskā persona patiešām veic *FOSS* piegādi. Faktiski, kā atgādināts 18. apsvērumā, KNA neattiecas uz fiziskām vai juridiskām personām, kas ar pirmkodu sniedz ieguldījumu produktos ar digitāliem elementiem, kuri kvalificējami kā *FOSS* un par kuriem tās nav atbildīgas.

([12]) Tas ir nepieciešams, bet ne pietiekams nosacījums, lai juridiska persona kvalificētos kā atvērtā pirmkoda programmatūras pārzinis, jo 3. panta 14. punktā noteiktajā definīcijā paredzēti papildu nosacījumi kvalificēšanai par pārzini.

49. Ņemot vērā *FOSS* izstrādes īpatnības, kas bieži ietver vairākus ieguldījuma sniedzējus, decentralizētus sadarbības modeļus un ieguldījuma nošķiršanu no lēmumu pieņemšanas, ir lietderīgi precizēt, ka *FOSS* uzskata par tādu, kas ir to fizisko vai juridisko personu "atbildībā", kuras to publicē un īsteno galveno kontroli pār tās izstrādi, laidieniem un lēmumiem par izplatīšanu (šādas personas bieži dēvē par "uzturētājiem"). Personas, kas ar pirmkodu sniedz ieguldījumu, bet nekontrolē laidienus, ceļvežus vai pārvaldības lēmumus, uzskata par "ieguldījuma sniedzējiem"; šādos gadījumos *FOSS* nav viņu atbildībā, lai gan viņi tajā ir snieguši ieguldījumu ar kodu. Ar tehnisku piekļuves tiesību esību vien, piemēram, ar tiesībām iesniegt izmaiņas ("commit access"), nepietiek, lai konstatētu, ka *FOSS* ir attiecīgās personas atbildībā; atbildība gulstas uz tiem, kas publicē un kontrolē *FOSS*.

13. piemērs: Individuāls izstrādātājs vai uzņēmuma darbinieks FOSS *projektam iesniedz "pull" vai "merge" pieprasījumu, kurā ietverts drošības ielāps vai jauna funkcija. Projekta uzturētāji kodu pārskata, pieņem un apvieno galvenajā repozitorijā, pēc tam iekļaujot to jaunā laidienā. Šajā situācijā persona, kas iesniedza "pull" pieprasījumu, ir "ieguldījuma sniedzējs", un uz to KNA neattiecas. Lai gan šī persona ar pirmkodu ir sniegusi ieguldījumu, tā neīsteno galveno kontroli pār lēmumiem par izstrādi, laidieniem vai izplatīšanu.*

3.2. **Kā noteikt, vai brīvi pieejama atvērtā pirmkoda programmatūra ir laista ES tirgū**

50. Kad konstatēts, ka *FOSS* ir fiziskas vai juridiskas personas atbildībā, jānoskaidro, vai šī persona to piegādā, veicot komercdarbību, tādējādi to laižot tirgū.

3.2.1. *Cenas noteikšana*

51. Ja fiziska vai juridiska persona, kas piegādā *FOSS*, nosaka cenu par pašu programmatūru (piemēram, par iepriekš kompilētām binārajām datnēm), šī persona laiž tirgū produktu ar digitāliem elementiem. Tādēļ persona, kas laiž tirgū *FOSS*, saskaņā ar KNA ir ražotājs.

52. Bieži *FOSS* ražotāji šai programmatūrai nodrošina arī bezmaksas versijas (bieži sauktas par "kopienas" versijām), kuru koda bāze ir (gandrīz) identiska maksas versijai. Tomēr šie produkti ar digitāliem elementiem ir atšķirīgi produkti: maksas versija tiek kaut kādā veidā monetizēta (piemēram, nosakot cenu vai izmantojot citus šajā iedaļā aplūkotos līdzekļus), tāpēc to uzskata par laistu tirgū un ražotājam rodas attiecīgie pienākumi. Bez maksas nodrošinātā versija (jeb kopienas versija) netiek monetizēta, tādēļ KNA vajadzībām to neuzskata par laistu tirgū. Tas pats attiecas uz gadījumu, kad maksas versija ir "uzlabota" komerciāla versija, kas paplašina bez maksas nodrošinātās versijas koda bāzi vai iekļauj šo versiju plašākā produktā ar digitāliem elementiem (piemēram, "atvērtā kodola" (*open-core*) modelī).

53. Ja kopienas versiju piegādā juridiska persona, uz šo juridisko personu attiecībā uz bez maksas piegādāto versiju (kopienas versiju) attiecas arī pārziņiem noteiktie pienākumi. Ja šī persona ir fiziska persona, bez maksas nodrošinātā versija (kopienas versija) neietilpst KNA darbības jomā.

3.2.2. *Citu pakalpojumu monetizācija vai personas datu apstrādes izvirzīšana par lietošanas nosacījumu*

54. Fiziska vai juridiska persona, kas publicē *FOSS*, var arī tikt uzskatīta par tādu, kas to laiž tirgū (t. i., piegādā, veicot komercdarbību), ja tā nodrošina programmatūru, ar kuras palīdzību monetizē citus produktus ar digitāliem elementiem vai pakalpojumus, vai ja tā kā lietošanas nosacījumu pieprasa personas datu apstrādi tādu iemeslu dēļ, kas nav tikai programmatūras drošības, savietojamības vai sadarbspējas uzlabošana.

14. piemērs: fiziska vai juridiska persona publicē brīvi pieejamu atvērtā pirmkoda tiešsaistes tirdzniecības vietas lietojumprogrammu. Lietojumprogramma ir pieejama bez maksas un ļauj lietotājiem ar tās starpniecību iegādāties preces vai pakalpojumus. Lietojumprogramma ļauj personai, kas to publicējusi, monetizēt citus produktus ar digitāliem elementiem un ar tās starpniecību piedāvātos pakalpojumus (piemēram, ar reklāmu, komisijas maksām vai abonēšanas maksām). Tādēļ uzskata, ka lietojumprogramma ir laista tirgū, veicot komercdarbību.

15. piemērs: fiziska vai juridiska persona publicē brīvi pieejamu atvērtā pirmkoda VPN. Lietojumprogramma ir pieejama bez maksas, bet tā ļauj lietotājiem par maksu piekļūt papildu serveriem vai īpaši piešķirtām IP adresēm. Šī lietojumprogramma ļauj attiecīgajai personai monetizēt citus ar tās starpniecību piedāvātos pakalpojumus, tādēļ uzskata, ka tā ir laista tirgū, veicot komercdarbību.

16. piemērs: Fiziska vai juridiska persona publicē brīvi pieejamu atvērtā pirmkoda fizisko aktivitāšu uzskaites lietojumprogrammu. Lietojumprogramma ir pieejama bez maksas, bet tās lietošana ir atkarīga no lietotāju personas datu apstrādes tādiem nolūkiem kā mērķorientēta reklāma vai analītika, kas nav saistīta ar programmatūras drošību, savietojamību vai sadarbspēju. Tā kā šāda datu apstrāde tiek prasīta kā lietošanas nosacījums, uzskata, ka lietojumprogramma ir laista tirgū, veicot komercdarbību.

3.2.3. *Atbalsta pakalpojumi*

55. Tas vien, ka fiziska vai juridiska persona, kas publicē *FOSS*, piedāvā arī ar to saistītus maksas atbalsta pakalpojumus, pats par sevi nenozīmē, ka produkts ar digitāliem elementiem tiek piegādāts, veicot komercdarbību. Atbalsta pakalpojumi var ietvert tādas darbības kā konsultācijas, apmācība vai profesionāli pakalpojumi, kas saistīti ar programmatūras lietošanu, dokumentāciju, konfigurēšanu un ieviešanu klienta vidē.

56. Izšķirošais faktors ir tas, vai piekļuve pašai *FOSS* (t. i., produkta ar digitāliem elementiem nodrošināšana), tostarp tās uzturēšanai, ir atkarīga no atlīdzības, nevis tas vien, ka saistībā ar brīvi pieejamu produktu ar digitāliem elementiem tiek piedāvāti profesionāli pakalpojumi, kā norādīts KNA 18. apsvērumā ("par komercdarbību nebūtu jāuzskata tādu produktu ar digitāliem elementiem nodrošināšana, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra un kurus to ražotāji nemonetizē"). Ja *FOSS* var brīvi lejupielādēt un instalēt un lietotāji var pēc izvēles atsevišķi iegādāties profesionālos pakalpojumus, šo *FOSS* neuzskata par laistu tirgū.

57. Savukārt dažos gadījumos piekļuve konkrētai produkta ar digitāliem elementiem versijai, tostarp noteiktām priekšrocībām, piemēram, tehniskajai palīdzībai vai veiktspējas optimizācijai, ir atkarīga no atlīdzības. Šādos gadījumos tā ir monetizēta produkta ar digitāliem elementiem nodrošināšana, veicot komercdarbību, tādēļ šo produktu uzskata par laistu tirgū. Tas ietver gadījumus, kad maksas izdevums vai uzņēmumiem paredzēta versija tiek darīta pieejama saskaņā ar komerclīgumu neatkarīgi no tā, vai funkcionāli līdzvērtīga programmatūra ir pieejama arī bez maksas saskaņā ar brīvi pieejamu atvērtā pirmkoda licenci.

17. piemērs: fiziska vai juridiska persona publicē brīvi pieejamu atvērtā pirmkoda operētājsistēmu un piedāvā šīs operētājsistēmas maksas versiju, kas ietver atbalsta pakalpojumus, piemēram, tehnisko palīdzību vai veiktspējas optimizāciju. Operētājsistēmas maksas versiju uzskata par laistu tirgū, veicot komercdarbību.

18. piemērs: fiziska vai juridiska persona publicē brīvi pieejamu atvērtā pirmkoda komandrindas rīku. Rīks ir brīvi pieejams, un ikviens to var lejupielādēt un instalēt. Šī fiziskā vai juridiskā persona atsevišķi piedāvā profesionālus pakalpojumus, piemēram, izvēles konsultācijas lietotāju apmācībai un atbalstam rīka instalēšanā un lietošanā. Šo FOSS *KNA nozīmē neuzskata par laistu tirgū.*

58. It īpaši fizisku personu publicētas *FOSS* gadījumā tehniskās palīdzības piedāvāšana komplektā ar piekļuvi produktam ar digitāliem elementiem joprojām nebūtu uzskatāma par komercdarbību, ja, kā norādīts KNA 15. apsvērumā, noteiktā cena paredzēta tikai faktisko izmaksu atgūšanai. Šādas faktiskās izmaksas ietver dažādas ar programmatūras projektēšanu, izstrādi un uzturēšanu saistītas izmaksas, tostarp saprātīgus personas iztikas izdevumus. Tādēļ fizisku personu, kas publicē *FOSS* un piedāvā tehnisko palīdzību, lai segtu savas izmaksas un saņemtu taisnīgu atlīdzību, šā iemesla dēļ vien neuzskata par tādu, kas šo programmatūru laiž ES tirgū.

59. Fizisku vai juridisku personu, kas piedāvā tehnisko palīdzību saistībā ar *FOSS*, par kuru tā nav atbildīga, neuzskata par tādu, kas šo programmatūru laiž tirgū, izņemot gadījumu, kad šī persona, sniedzot šādu palīdzību, saskaņā ar 22. pantu būtiski modificē *FOSS*.

19. piemērs: pakalpojumu sniedzējs nepublicē FOSS*, bet palīdz klientam to instalēt klienta lokālajā serverī. Tas tiek darīts, neveicot šīs* FOSS *būtisku modifikāciju. Tāpēc pakalpojumu sniedzēju neuzskata par tādu, kas* FOSS *laiž tirgū.*

3.2.4. *Ziedojumi*

60. Fiziskas vai juridiskas personas, kas publicē *FOSS* projektus, parasti nodrošina iespēju šīs programmatūras lietotājiem brīvprātīgi ziedot naudu, lai pateiktos projekta publicētājam(-iem) un palīdzētu nodrošināt projekta aktīvu uzturēšanu.

61. Kā norādīts KNA 15. apsvērumā, "ziedojumu pieņemšana bez nodoma gūt peļņu nebūtu jāuzskata par komercdarbību". Tas vien, ka tiek iekļauta saite uz ziedojumu platformu vai līdzīgs ziedojumu vākšanas rīks, nebūtu jāuzskata par nodomu gūt peļņu, pat ja ziedojumos savāktā summa pārsniedz ar produkta ar digitāliem elementiem projektēšanu, izstrādi un nodrošināšanu saistītās izmaksas. Tas ietver saprātīgu atlīdzību ieguldījuma sniedzējiem, kurus nolīgusi juridiska persona, un/vai fiziskas personas saprātīgus iztikas izdevumus. Ziedojumu apmērs pēc savas būtības laika gaitā svārstās, tāpēc, novērtējot, vai *FOSS*, kas tiek monetizēta tikai ar ziedojumiem, ir uzskatāma par laistu tirgū, ir jāpieļauj zināma elastība. Tāpēc maz ticams, ka *FOSS*, ko atbalsta tikai ar ziedojumiem, KNA nozīmē tiks uzskatīta par laistu tirgū.

20. piemērs: fiziska vai juridiska persona publicē FOSS *rīku publiskā tiešsaistes repozitorijā, ļaujot ikvienam to lejupielādēt, lietot, modificēt un tālāk izplatīt saskaņā ar brīvi pieejamu atvērtā pirmkoda licenci. Publicētājs aicina lietotājus brīvprātīgi ziedot, izmantojot ziedojumu platformu, lai atbalstītu projekta turpmāku izstrādi un uzturēšanu. Piekļuve programmatūrai, tās pirmkodam un atjauninājumiem nav atkarīga no ziedojuma veikšanas. Šo* FOSS *neuzskata par piegādātu, veicot komercdarbību, un KNA nozīmē neuzskata par laistu tirgū.*

62. Tomēr ir gadījumi, kad ar ziedojumiem atbalstītu *FOSS* var uzskatīt par laistu tirgū. Tāds ir gadījums, kad, vispusīgi izvērtējot apstākļus, ziedojumi faktiski ir līdzvērtīgi cenas noteikšanai par piekļuvi produktam ar digitāliem elementiem vai noteiktām tā funkcijām. Tas it īpaši var būt gadījumā, kad piekļuve *FOSS*, būtiskām funkcijām vai atjauninājumiem praksē ir atkarīga no ziedojuma veikšanas vai ziedojumi ir saistīti ar līgumiskiem labumiem vai ekskluzīvām priekšrocībām, kas pārsniedz kopienas dalībniekiem parasti pieejamās priekšrocības.

21. piemērs: fiziska vai juridiska persona publicē programmatūras produktu ar digitāliem elementiem saskaņā ar brīvi pieejamu atvērtā pirmkoda licenci, bet lejupielādējamus laidienus un drošības atjauninājumus nodrošina tikai lietotājiem, kuri ziedo. Lietotājiem, kuri neziedo, nav piekļuves programmatūras pašreizējajai versijai.

Šajā gadījumā ziedojumi de facto *ir nosacījums piekļuvei produktam ar digitāliem elementiem un tādējādi ir pielīdzināmi cenas noteikšanai. Tādēļ šo* FOSS *KNA nozīmē uzskata par laistu tirgū.*

22. piemērs: fiziska vai juridiska persona dara FOSS *pirmkodu publiski pieejamu, bet iepriekš kompilētas binārās datnes, regulārus atjauninājumus un garantētus drošības labojumus nodrošina tikai ziedotājiem. Šajā gadījumā ziedojumi ir saistīti ar piekļuvi būtiskiem produkta ar digitāliem elementiem aspektiem un ir atlīdzība par šā produkta piegādi. Tādējādi tiek uzskatīts, ka šī* FOSS *ir laista tirgū, veicot komercdarbību.*

3.2.5. *Brīvi pieejamas atvērtā pirmkoda programmatūras finansēšana*

63. Tas vien, ka trešā persona ir apmaksājusi, sponsorējusi vai citādi finansējusi *FOSS* izstrādi, pats par sevi nenosaka, vai šī *FOSS* tiek laista tirgū. *FOSS* ekosistēmā ir ierasta prakse, ka individuāli izstrādātāji, fondi vai kopienas saņem finansējumu no uzņēmumiem, publiskām struktūrām vai citiem sponsoriem, lai izstrādātu konkrētas funkcijas, labotu kļūdas vai uzturētu kritiski svarīgus komponentus. Šāds finansējums var izpausties dažādos veidos, tostarp kā dotācijas, atlīdzība par kļūdu atklāšanu, sponsorēšana, pakalpojumu līgumi vai apmaksāti izstrādes darbi.

64. Kā jau minēts, KNA 18. apsvērumā ir precizēts, ka, nosakot šīs darbības komerciālo raksturu, nebūtu jāņem vērā tikai apstākļi, kādos produkts ar digitāliem elementiem ir izstrādāts, vai tas, kā šī izstrāde ir finansēta.

65. Tāpēc, ja *FOSS* tiek atklāti kopīgota un darīta brīvi pieejama visiem, lai tai varētu piekļūt, to izmantot, modificēt un tālāk izplatīt, faktam, ka komercsubjekts, iespējams, ir finansējis šo projektu, nevajadzētu ietekmēt vērtējumu par to, vai programmatūra ir laista tirgū. Faktiski, ja minētā *FOSS* nav citādi monetizēta, to neuzskata par laistu tirgū. Ja uzņēmums, kas finansēja *FOSS* izstrādi (tāpat kā jebkurš cits uzņēmums), integrē to savā produktā ar digitāliem elementiem, tam ir jāveic pienācīga pārbaude saskaņā ar KNA 13. panta 5. punktu.

23. piemērs: individuāls izstrādātājs publicē FOSS *projektu un aktīvi to uztur. Ražotājs A lūdz individuālo izstrādātāju pievienot šai* FOSS *konkrētu funkciju un finansē tās izstrādi. Izstrādātājs pievieno funkciju* FOSS *koda bāzei, atklāti to kopīgojot un darot brīvi pieejamu visiem, lai tai varētu piekļūt, to izmantot, modificēt un tālāk izplatīt. Netiek uzskatīts, ka individuālais izstrādātājs ir laidis šo* FOSS *tirgū. Ja ražotājs integrē* FOSS *savā produktā ar digitāliem elementiem, tam ir jāveic pienācīga pārbaude saskaņā ar 13. panta 5. punktu.*

3.2.6. *Bezpeļņas struktūras, kas izveidotas bezpeļņas mērķu sasniegšanai*

66. Ja juridiska persona, kas publicē *FOSS*, ir bezpeļņas organizācija, kas "izveidota tā, lai nodrošinātu, ka visi ieņēmumi pēc izmaksu segšanas tiek izmantoti bezpeļņas mērķu sasniegšanai" (KNA 18. apsvērums), tās publicēto *FOSS* neuzskata par laistu tirgū. Ja šī juridiskā persona atbilst "pārziņa" definīcijai, uz to attiecas attiecīgie pienākumi (KNA 24. pants).

24. piemērs: juridiska persona publicē brīvi pieejamu atvērtā pirmkoda pārlūkprogrammu, kas tiek tieši monetizēta, izmantojot partnerības ar meklētājprogrammām, taču visi tās ieņēmumi pēc izmaksu segšanas tiek izmantoti bezpeļņas mērķiem. Pārlūkprogrammu neuzskata par laistu tirgū KNA nozīmē. Uz juridisko personu, kas to publicē, attiecas pārziņiem piemērojamie pienākumi.

3.2.7. *Integrēšana, ko veic citi ražotāji*

67. Dažos gadījumos *FOSS* publicē skaidri identificējama fiziska vai juridiska persona, bet šī *FOSS* ir "paredzēta, lai citi ražotāji to integrētu savos produktos ar digitāliem elementiem". Šādos gadījumos minēto *FOSS* neuzskata par laistu ES tirgū, izņemot gadījumus, kad persona, kas to publicē (t. i., sākotnējais ražotājs), to arī monetizē, kā izklāstīts šo norādījumu iepriekšējās iedaļās.

68. Ja minētā *FOSS* netiek laista tirgū, uz juridisko personu, kas to publicē, attiecas pārziņa pienākumi, ja tā ilgstoši sniedz atbalstu saskaņā ar "pārziņa" definīciju.

25. piemērs: juridiska persona publicē FOSS *bibliotēku lietotāja saskarņu izveidei. Tā nemonetizē šīs bibliotēkas piegādi, bet integrē bibliotēku vienā no saviem produktiem ar digitāliem elementiem (ko savukārt laiž tirgū). Bibliotēku neuzskata par laistu tirgū KNA nozīmē, bet tā ir paredzēta integrēšanai produktos ar digitāliem elementiem. Juridiskā persona, kas to publicē, ir tās pārzinis.*

26. piemērs: juridiska persona laiž tirgū operētājsistēmu un publicē arī FOSS *bibliotēkas, kas kalpo par atsauces implementācijām šīs operētājsistēmas lietotājiem. Juridiskā persona nemonetizē* FOSS *bibliotēkas, kas paredzētas integrēšanai citos produktos ar digitāliem elementiem. Juridiskā persona, kas tās publicē, ir šo* FOSS *bibliotēku pārzinis.*

3.3. **Atvērtā pirmkoda programmatūras pārziņi**

69. KNA ievieš jaunu juridisko kategoriju "atvērtā pirmkoda programmatūras pārzinis", ņemot vērā "to, cik svarīgi kiberdrošībai ir daudzi produkti ar digitāliem elementiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra, kura ir publicēta, bet nav darīta pieejama tirgū [KNA] nozīmē" (KNA 19. apsvērums).

70. Dažos gadījumos *FOSS* publicē, bet KNA nozīmē nedara pieejamu tirgū juridiska persona, kuras "nolūks vai mērķis ir sistemātiski un ilgstoši sniegt atbalstu [*FOSS*] (..) izstrādei, kas kvalificējam[a] kā brīvi pieejama atvērtā pirmkoda programmatūra un paredzēt[a] komerciālai darbībai, un kura nodrošina minēto produktu dzīvotspēju" (KNA 3. panta 14. punkts). Šādos gadījumos uz šo juridisko personu attiecas pārziņa pienākumi.

71. Pārzinis ir definēts kā "juridiska persona, kura nav ražotājs", jo ražotājs pēc definīcijas ir fiziska vai juridiska persona, kas produktus ar digitāliem elementiem laiž tirgū ("tirgo tos") ar savu vārdu vai preču zīmi. Juridiska persona var būt pārzinis tikai attiecībā uz produktiem ar digitāliem elementiem, kas kvalificējami kā *FOSS* un kas ir publicēti, bet nav darīti pieejami tirgū KNA nozīmē. Tāpēc "pārziņa" jēdziens attiecas uz konkrētiem *FOSS* gadījumiem, kas "galu galā ir paredzēti komerciālai darbībai, piemēram, integrēšanai komercpakalpojumos vai naudas izteiksmē izteiktos produktos ar digitāliem elementiem" (KNA 19. apsvērums) ([13]), bet nav darīti pieejami tirgū KNA nozīmē un kuriem juridiskā persona, kas publicē minēto *FOSS*, nodrošina sistemātisku atbalstu.

72. Tas, ka juridiskā persona ir vienas konkrētas *FOSS* pārzinis, nenozīmē, ka tā noteikti ir arī citu tās publicēto *FOSS* pārzinis. Tāpat tas, ka juridiskā persona ir vienas konkrētas *FOSS* ražotājs, nenozīmē, ka tā nevar būt citu *FOSS* pārzinis. Tas ietver arī viena un tā paša *FOSS* "kopienas" versiju nodrošināšanu, kā aprakstīts *3.2.1.* iedaļā *Cenas noteikšana*.

73. Tāpēc juridiska persona var vienlaikus būt vienas konkrētas *FOSS* pārzinis (ja pārzinis sistemātiski un ilgstoši sniedz atbalstu un nodrošina programmatūras dzīvotspēju) un citas konkrētas *FOSS* ražotājs (ja tā to laiž tirgū). Citiem vārdiem sakot, vienai un tai pašai juridiskajai personai attiecībā uz dažādiem *FOSS* projektiem var būt jāpilda dažādas lomas.

74. Attiecībā uz katru konkrēto *FOSS*, ko tā publicē, juridiskajai personai būs jānoskaidro, vai minētā *FOSS* tiek uzskatīta par laistu tirgū KNA nozīmē. Ja tā ir, juridiskā persona ir šīs programmatūras ražotājs. Ja *FOSS* neuzskata par laistu tirgū, juridiskā persona var būt tās pārzinis, ja programmatūra ir paredzēta komerciālai darbībai un juridiskā persona to uztur saskaņā ar pārziņa definīciju ([14]).

3.3.1. *Ilgstošs atbalsts un* FOSS *dzīvotspējas nodrošināšana*

75. 19. apsvērumā ir paskaidrots, ka ilgstoša atbalsta sniegšana produkta ar digitāliem elementiem izstrādei cita starpā var ietvert: i) programmatūras izstrādes sadarbības platformu mitināšanu un pārvaldību, ii) pirmkoda vai programmatūras mitināšanu, iii) tādu produktu ar digitāliem elementiem pārvaldību vai vadību, kuri kvalificējami kā *FOSS*, un iv) šādu produktu ar digitāliem elementiem izstrādes vadību.

76. Tas var attiekties, piemēram, uz juridisku personu, kas izstrādā *FOSS* integrēšanai savos produktos ar digitāliem elementiem un pēc tam to publicē, nelaižot to tirgū. Tas ir aplūkots arī *3.2.7.* iedaļā *Integrēšana, ko veic* citi ražotāji. Šajā gadījumā juridiskā persona nav programmatūras ražotājs, bet var būt tās pārzinis. Turklāt, kā paskaidrots arī iepriekšējās iedaļās, juridisku personu, kas publicē viena un tā paša *FOSS* bezmaksas (vai kopienas) versiju un monetizētu versiju, uzskata par bezmaksas (vai kopienas) versijas pārzini un monetizētās versijas ražotāju.

77. Tāpat juridiska persona, kas monetizē *FOSS*, bet ir bezpeļņas struktūra, kuras ieņēmumi pēc izmaksu segšanas tiek izmantoti bezpeļņas mērķu sasniegšanai (un tāpēc tās *FOSS* netiek laista tirgū KNA nozīmē, kā aplūkots *3.2.6.* iedaļā *Bezpeļņas struktūras*), ir tās publicētās *FOSS* pārzinis.

78. Turklāt daži fondi piedāvā sadarbības platformas ar dažādiem pārvaldības veidiem, kas ļauj ražotājiem regulāri piedalīties *FOSS* izstrādē un/vai ko ražotāji regulāri finansē. Šādi fondi ir uzskatāmi par pārziņiem attiecībā uz konkrētu *FOSS*, kas paredzēta komerciālai darbībai un kurai fonds sniedz ilgstošu atbalstu. Tomēr, kā paskaidrots *3.3.* iedaļā *Atvērtā pirmkoda programmatūras* pārziņi, uz šādu fondu var neattiekties nekādi KNA pienākumi attiecībā uz citu konkrētu *FOSS*, ko tas mitina, ja tas attiecīgajai *FOSS* nesniedz sistemātisku atbalstu, nenodrošina tās dzīvotspēju un/vai attiecīgā programmatūra nav paredzēta komerciālai darbībai.

([13]) Šis jēdziens ir ietverts arī formulējumā "paredzēts komerciālai darbībai", kas iekļauts KNA 3. panta 14. punktā sniegtajā "atvērtā pirmkoda programmatūras pārziņa" definīcijā.

([14]) Juridiskajai personai var arī nebūt nekādu KNA noteiktu pienākumu, ja: i) konkrēta *FOSS* nav laista tirgū KNA nozīmē un ii) juridiskā persona attiecībā uz šo konkrēto *FOSS* neatbilst pārziņa definīcijai.

79. "Ilgstošā atbalsta" veids, ko fondi un līdzīgas organizācijas sniedz konkrētiem *FOSS* projektiem, var ievērojami atšķirties. Piemēram, dažas juridiskās personas sniedz tikai netehnisku atbalstu, piemēram, pārvalda projektu zīmolus, nosaka pārvaldības noteikumus, organizē kopienas pasākumus vai vāc ziedojumus. Citas vienības nodrošina arī projekta darbībai nepieciešamo pamata IT infrastruktūru, piemēram, mitina pirmkoda repozitorijus, nodrošina versiju kontroles sistēmas vai ģenerē parakstīšanas atslēgas. Citas savukārt sniedz vēl plašāku atbalstu, aktīvi nodrošinot projektam inženiertehniskos resursus, piemēram, nodarbinot izstrādātājus, koordinējot izstrādes darbus, pārskatot vai apvienojot kodu, pārvaldot laidienus vai apstrādājot ziņojumus par ievainojamībām un drošības ielāpus. Lai gan visām juridiskajām personām, kas saskaņā ar KNA kvalificējas kā pārziņi, ir jāievēro 24. panta 1. un 2. punktā noteiktie pienākumi, tas, cik lielā mērā uz tām attiecas 14. panta 1., 3. un 8. punktā noteiktie pienākumi, saskaņā ar 24. panta 3. punktu ir atkarīgs no to sniegtā atbalsta veida.

80. Piemēram, pārzinis, kas sniedz tikai netehnisku atbalstu, pēc definīcijas nav iesaistīts produkta ar digitāliem elementiem izstrādē, un tāpēc tam nav jāziņo par aktīvi izmantotām ievainojamībām. Minētais pārzinis arī nenodrošina tīklu un informācijas sistēmas šādu produktu ar digitāliem elementiem izstrādei, un tāpēc tam nav jāziņo *ENISA* un *CSIRT* par nopietniem incidentiem vai jāinformē ietekmētie lietotāji. Tomēr, ja pārzinis uzzina par aktīvi izmantotu ievainojamību (piemēram, saņemot ziņojumu no ārējiem avotiem, piemēram, pētniekiem drošības jomā), tam saskaņā ar savu kiberdrošības politiku būtu jākopīgo šī informācija ar produkta ar digitāliem elementiem uzturētājiem. Produktu ar digitāliem elementiem uzturētājiem un/vai pārziņiem būtu arī jāapsver iespēja brīvprātīgi ziņot par ievainojamību saskaņā ar 15. pantu.

81. No otras puses, ja pārzinis nodrošina pamatā esošo IT infrastruktūru konkrētiem produktiem ar digitāliem elementiem, tam saskaņā ar 14. panta 3. punktu ir jāpaziņo *ENISA* un *CSIRT* par jebkādiem nopietniem incidentiem, kas saistīti ar minēto infrastruktūru un kas ietekmē produktu ar digitāliem elementiem drošību. Attiecīgā gadījumā tam ir arī jāinformē visi lietotāji (piemēram, ar vispārīgu paziņojumu). Kā norādīts iepriekšējā punktā, lai gan pārzinim nav jāziņo par aktīvi izmantotām ievainojamībām, par kurām tas uzzina, tam būtu jāveicina pareiza ievainojamību novēršana un jāapsver brīvprātīga ziņošana saskaņā ar 15. pantu.

82. Visbeidzot, ja pārzinis konkrētiem produktiem ar digitāliem elementiem nodrošina arī inženiertehniskos resursus, tam ir pienākums: i) saskaņā ar 14. panta 1. punktu paziņot par aktīvi izmantotām ievainojamībām, par kurām tas uzzina, un ii) attiecīgā gadījumā informēt visus lietotājus. Ciktāl pārzinim ir arī tiešas attiecības ar ietekmētajiem lietotājiem, tam saskaņā ar 14. panta 8. punktu ir arī pienākums tos informēt tieši.

83. Ja vienība pārtrauc ilgstoši un sistemātiski sniegt atbalstu konkrētai *FOSS*, tā var vairs neatbilst pārziņa definīcijai, un tāpēc uz to var vairs neattiekties attiecīgie pienākumi. Šādos gadījumos minētā vienība ir aicināta skaidri informēt par sava statusa maiņu attiecībā uz konkrēto *FOSS*.

84. Noteiktās situācijās vienība, kas bijusi konkrēta projekta pārzinis, var nolemt šo projektu tieši monetizēt, tādējādi laižot tirgū produktu ar digitāliem elementiem, kā rezultātā tai kļūst piemērojami KNA noteiktie ražotāja pienākumi. Šādos apstākļos minēto vienību uzskata par produkta ar digitāliem elementiem ražotāju no dienas, kad tā to laiž tirgū (bet ne attiecībā uz agrākām versijām, kuru pārzinis tā bija).

3.4. **Ieguldījuma sniedzēji un lietojumi lejasposmā**

85. Kā jau minēts *3.1. iedaļā Kā noteikt, vai brīvi pieejama atvērtā pirmkoda programmatūra ir personas atbildībā*, KNA ir precizēts, ka to nepiemēro "fiziskām vai juridiskām personām, kas ar pirmkodu sniedz ieguldījumu produktos ar digitāliem elementiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra un par kuriem tās nav atbildīgas" (KNA 18. apsvērums).

86. Arī tādu produktu ar digitāliem elementiem ražotāji, kas savos produktos ar digitāliem elementiem integrē *FOSS* komponentus, nekļūst atbildīgi par šo komponentu individuālo atbilstību KNA, pat ja ražotāji sniedz pirmkodu to uzturēšanai.

87. Tāpat tas vien, ka ražotāji integrē *FOSS* komponentus savos (monetizētajos) produktos ar digitāliem elementiem, neietekmē minētā *FOSS* komponenta statusu saskaņā ar KNA. Tādu *FOSS* komponentu uzturētājiem, kuri netiek laisti tirgū, nav pienākumu attiecībā uz citām vienībām, kas šādus komponentus var integrēt savos produktos ar digitāliem elementiem. Tas, vai KNA attiecas uz konkrētu *FOSS* komponentu, ir atkarīgs tikai no tā, vai fiziskā vai juridiskā persona, kas to publicē, to laiž tirgū.

88. Tomēr tādu produktu ar digitāliem elementiem ražotājiem, kuros integrēti *FOSS* komponenti, ir jāievēro KNA prasības attiecībā uz saviem produktiem ar digitāliem elementiem. Tiem saskaņā ar 13. panta 5. punktu ir arī pienācīgas pārbaudes pienākums attiecībā uz integrētajiem *FOSS* komponentiem. Turklāt tiem saskaņā ar 13. panta 6. punktu ir jāziņo par integrēto komponentu ievainojamībām un jākopīgo drošības labojumi. Sīkākus norādījumus par šo tematu sk. *9.2.1.* iedaļā *Ziņošana augšposmā un drošības labojumu kopīgošana*.

3.5. **Ilustratīvi scenāriji**

89. Tālāk dotie piemēri ir pilnīgi hipotētiski, un to vienīgais mērķis ir ilustrēt dažādus gadījumus, kas izskaidroti iepriekšējās iedaļās.

27. piemērs: individuāls izstrādātājs A ir izstrādājis FOSS. *Izstrādātājs A publicē šo* FOSS *ar savu vārdu vai preču zīmi, bet neiekasē maksu par tās izmantošanu. Programmatūra tiek atklāti kopīgota un ir brīvi pieejama visiem, lai tai varētu piekļūt, to lietot, modificēt un izplatīt tālāk. Izstrādātājs A iekļauj arī saiti uz platformu brīvprātīgu ziedojumu vākšanai.*

Uzņēmumi B, C un D integrē šo FOSS *savos produktos ar digitāliem elementiem. Lai atbalstītu pastāvīgu uzturēšanu, uzņēmumi B, C un D veic brīvprātīgus ziedojumus izstrādātājam A. Šie ziedojumi ļauj izstrādātājam A turpināt aktīvi uzturēt projektu.*

Minētā FOSS *netiek laista tirgū KNA nozīmē. Izstrādātājam A nav nekādu KNA noteiktu pienākumu. Uzņēmumiem B, C un D, integrējot minēto* FOSS *savos produktos ar digitāliem elementiem, saskaņā ar 13. panta 5. punktu ir jāveic pienācīga pārbaude.*

28. piemērs: bezpeļņas fonds F publicē FOSS *komponentu integrēšanai citos komerciālos produktos ar digitāliem elementiem. Fonds F apņemas ilgstoši sniegt atbalstu minētajai* FOSS, *lai nodrošinātu tās dzīvotspēju un ieviešanu.* Uzņēmumi A, B un C integrē šo FOSS savos produktos ar digitāliem elementiem. *Uzņēmumi A un B brīvprātīgi atvēl daļu savu izstrādātāju darba laika fonda F* FOSS *projektu, tai skaitā minētās* FOSS, *izstrādei un uzturēšanai.*

Tā kā fonds F ir bezpeļņas struktūra, kas izveidota tā, ka tās ieņēmumi pēc izmaksu segšanas tiek izmantoti bezpeļņas mērķu sasniegšanai, FOSS *neuzskata par laistu tirgū KNA nozīmē. Fonds F ir* FOSS *pārzinis, un uz to attiecas attiecīgie 24. pantā noteiktie pienākumi. Uzņēmumiem A, B un C, integrējot minēto* FOSS *savos produktos ar digitāliem elementiem, saskaņā ar 13. panta 5. punktu ir jāveic pienācīga pārbaude.*

29. piemērs: uzņēmums A ir izstrādājis FOSS *komponentu integrēšanai savos produktos ar digitāliem elementiem. Tas arī publicē šo* FOSS *atsevišķi ar savu nosaukumu vai preču zīmi un aktīvi uztur to. Tomēr tas neiekasē maksu par tās izmantošanu un nemonetizē to citos veidos. Uzņēmumi B, C un D integrē šo* FOSS *savos produktos ar digitāliem elementiem un brīvprātīgi atvēl daļu savu izstrādātāju darba laika tās uzturēšanai.*

Minēto FOSS *neuzskata par laistu tirgū KNA nozīmē. Uzņēmums A nav tās ražotājs, bet ir tās pārzinis. Uzņēmumiem B, C un D, integrējot* FOSS *savos produktos ar digitāliem elementiem, saskaņā ar 13. panta 5. punktu ir jāveic pienācīga pārbaude.*

30. piemērs: uzņēmums A publicē FOSS *ar savu nosaukumu vai preču zīmi un piedāvā to maksas versijā, kas ietver konkrētas priekšrocības, piemēram, tehnisko palīdzību vai veiktspējas optimizāciju. Uzņēmumu B, C un D izstrādātāji piedalās* FOSS *uzturēšanā, taču tā joprojām ir uzņēmuma A kontrolē.*

Uzņēmumu A uzskata par šīs FOSS *ražotāju* ([15]). *Uz uzņēmumiem B, C un D neattiecas KNA noteiktie pienākumi attiecībā uz konkrēto* FOSS. *Ja tie integrē minēto* FOSS *savos produktos ar digitāliem elementiem, tiem ir jāveic pienācīga pārbaude saskaņā ar 13. panta 5. punktu.*

31. piemērs: uzņēmums A publicē FOSS *ar savu nosaukumu vai preču zīmi un pastāvīgi to uztur, lai nodrošinātu tās ilgtermiņa dzīvotspēju un dotu iespēju šo programmatūru integrēt citu uzņēmumu produktos ar digitāliem elementiem. Uzņēmums A neiekasē maksu par tās izmantošanu, neapstrādā personas datus, ko tas ievāc ar produkta ar digitāliem elementiem starpniecību, un nepārdod ar* FOSS *publicēšanu saistītus atbalsta pakalpojumus.*

Uzņēmums B sniedz ieguldījumu ar kodu un izstrādātāju darba laiku FOSS *uzturēšanā, bet neizplata to komerciāli. Uzņēmums B piedāvā tehniskā atbalsta pakalpojumus neatkarīgi no* FOSS *izplatīšanas. Uzņēmums A tiek uzskatīts par attiecīgās* FOSS *pārzini, savukārt uzņēmumam B attiecībā uz šo* FOSS *nav KNA noteikto pienākumu.*

32. piemērs: FOSS *komponentu publicē bezpeļņas struktūra, kas izveidota tā, lai nodrošinātu, ka visi ieņēmumi pēc izmaksu segšanas tiek izmantoti bezpeļņas mērķu sasniegšanai. Šī struktūra sniedz ilgstošu atbalstu, lai nodrošinātu projekta ilgtermiņa dzīvotspēju. Uzturēšanu finansē no publiskā finansējuma, piemēram, pētniecības dotācijām. Papildu izstrādes darbi, tai skaitā jaunu funkciju izstrāde, tiek finansēti no ziedojumiem un konkrētu projektu ietvaros, kurus īsteno partnerībā ar ražotājiem, kuri integrē minēto* FOSS *savos produktos ar digitāliem elementiem. Šādas funkcijas tiek iekļautas* FOSS *koda bāzē.*

Bezpeļņas struktūru, kas publicē FOSS, *uzskata par attiecīgā* FOSS *komponenta pārzini. Ražotājs, kas ir sniedzis ieguldījumu konkrētu funkciju izstrādē, nekļūst par minētā* FOSS *komponenta ražotāju. Ja ražotājs integrē minēto* FOSS *komponentu savā produktā ar digitāliem elementiem, tam ir jāveic pienācīga pārbaude saskaņā ar 13. panta 5. punktu.*

33. piemērs: bezpeļņas struktūra, kas izveidota tā, lai nodrošinātu, ka visi ieņēmumi pēc izmaksu segšanas tiek izmantoti bezpeļņas mērķu sasniegšanai, publicē FOSS *programmatūras izstrādes komplektu (*SDK*) un nodrošina tā pastāvīgu uzturēšanu.* SDK *tiek atklāti kopīgots un ir brīvi pieejams visiem, lai tam varētu piekļūt, to izmantot, modificēt un tālāk izplatīt. Finansējumu nodrošina no biedru naudām, ko maksā bezpeļņas struktūrai, savukārt dalīborganizāciju nodarbinātie izstrādātāji sniedz ieguldījumu ar kodu un citiem resursiem* SDK *izstrādē. Ražotāji izmanto SDK kā komponentu citu produktu ar digitāliem elementiem izstrādei.*

Bezpeļņas struktūra, kas publicē šo SDK, *ir tā pārzinis. Fonda biedri nav atbildīgi par* SDK *atbilstību KNA. Ja ražotāji izmanto* SDK, *lai izveidotu paši savu produktu ar digitāliem elementiem, tiem ir jāveic pienācīga pārbaude saskaņā ar 13. panta 5. punktu.*

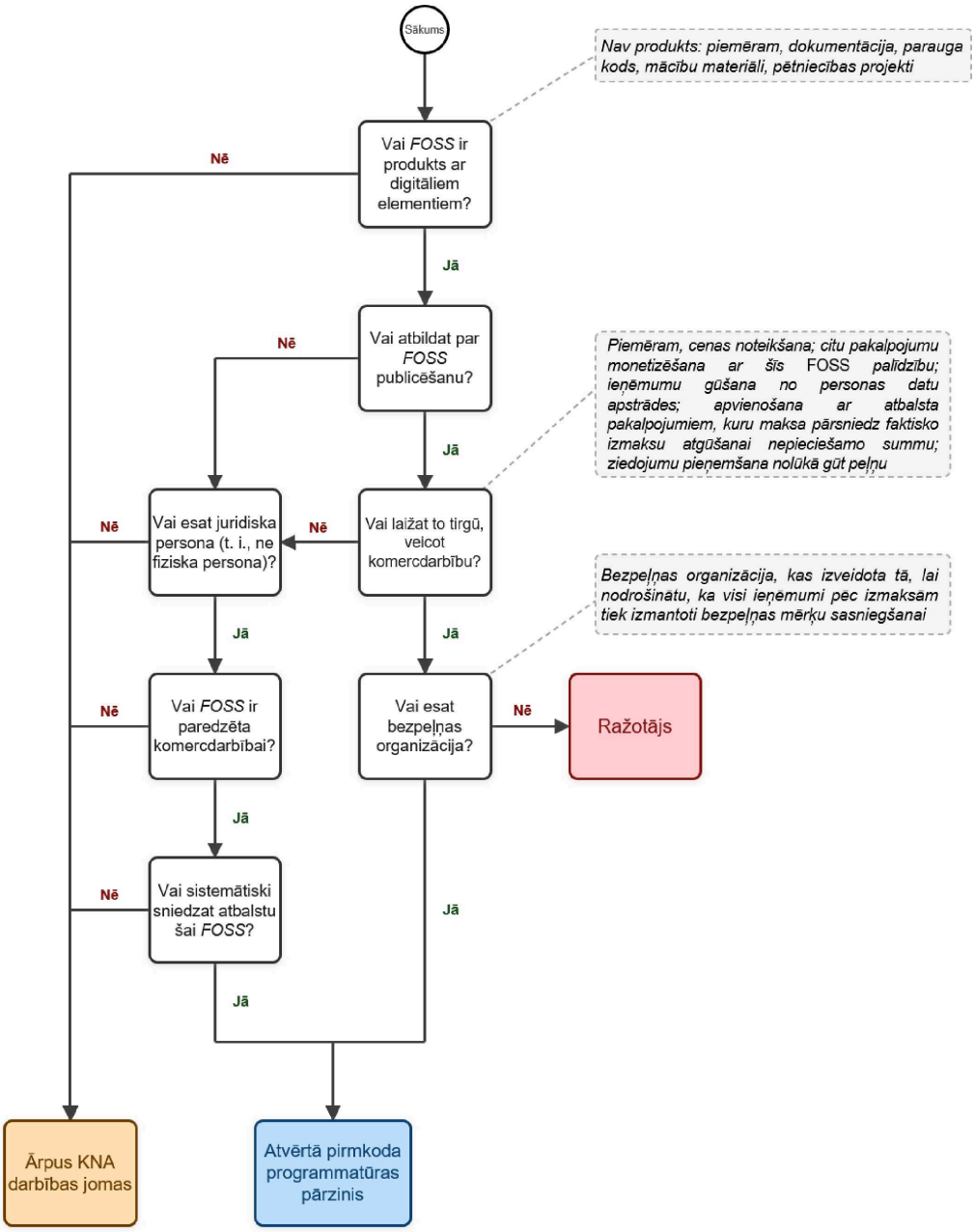
34. piemērs: individuāls izstrādātājs publicē FOSS *bibliotēku publiskā pakotņu repozitorijā konkrētai programmēšanas valodai un aktīvi to uztur. Pakotnes dokumentācijā izstrādātājs pievieno saiti ziedojumu vākšanai. Ražotājs bez maksas lejupielādē šo bibliotēku no repozitorija un integrē to savā produktā ar digitāliem elementiem.*

Individuālajam izstrādātājam un pakotņu repozitorijam nav nekādu KNA noteikto pienākumu. Ražotājam, kas integrē bibliotēku, jāveic pienācīga pārbaude saskaņā ar 13. panta 5. punktu.

([15]) Ja vien uzņēmums A nav bezpeļņas struktūra, kas izveidota tā, lai nodrošinātu, ka visi ieņēmumi pēc izmaksu segšanas tiek izmantoti bezpeļņas mērķu sasniegšanai; tādā gadījumā tas būtu attiecīgās *FOSS* pārzinis.

1. attēls

Stilizēta blokshēma par KNA darbības jomu attiecībā uz brīvi pieejamu atvērtā pirmkoda programmatūru



4. BŪTISKAS MODIFIKĀCIJAS UN REZERVES DAĻAS

90. KNA 3. panta 30. punktā "būtiska modifikācija" ir definēta kā tādas produkta ar digitāliem elementiem izmaiņas pēc laišanas tirgū, kas i) ietekmē produkta atbilstību I pielikuma I daļā noteiktajām kiberdrošības pamatprasībām vai ii) izraisa izmaiņas paredzētajā nolūkā, par kuru ir saņemts produkta ar digitāliem elementiem novērtējums.

91. Būtiskas modifikācijas jēdziens ir svarīgs, lai vairākos gadījumos noteiktu KNA paredzētos pienākumus, tostarp šādos:

a) saskaņā ar 21. pantu importētājs vai izplatītājs, kas veic jau tirgū laista produkta ar digitāliem elementiem būtisku modifikāciju, tiek uzskatīts par tā ražotāju;

b) saskaņā ar 22. pantu par tā ražotāju uzskata jebkuru fizisku vai juridisku personu, kas veic produkta ar digitāliem elementiem būtisku modifikāciju un dara to pieejamu tirgū;

c) saskaņā ar 69. panta 2. punktu jebkuru fizisku vai juridisku personu, kas pēc 2027. gada 11. decembra veic būtisku modifikāciju produktam ar digitāliem elementiem, kurš laists tirgū pirms 2027. gada 11. decembra, un laiž to tirgū, uzskata par tā ražotāju;

d) attiecībā uz tādu produktu ar digitāliem elementiem ražotājiem, kas laisti tirgū pēc 2027. gada 11. decembra, – lai noteiktu, vai attiecībā uz produktu ar digitāliem elementiem ir jāveic jauna atbilstības novērtēšanas procedūra sakarā ar izmaiņām, kas veiktas pēc minētā datuma, it īpaši ņemot vērā programmatūras izstrādes iteratīvo raksturu.

92. Tāpēc ir svarīgi sniegt norādījumus, lai palīdzētu uzņēmējiem saprast, kad aparatūras vai programmatūras modifikācijas ir uzskatāmas par būtiskām modifikācijām.

4.1. **Fizisks remonts**

93. Kā norādīts KNA 42. apsvērumā, "[j]a uz produktu ar digitāliem elementiem attiecas "atjaunošana", "uzturēšana" un "remontēšana", kā definēts Eiropas Parlamenta un Padomes Regulas (ES) 2024/1781 2. panta 18., 19. un 20. punktā, tad tas ne vienmēr izraisa produkta būtisku modifikāciju, piemēram, ja paredzētais lietojums un funkcijas netiek mainītas un netiek ietekmēts riska līmenis. Tomēr ražotāja veikta produkta jaunināšana varētu izraisīt izmaiņas produkta projektēšanā un izstrādē un tādējādi varētu ietekmēt produkta paredzēto nolūku un atbilstību šajā regulā noteiktajām prasībām." Tas atbilst zilās rokasgrāmatas 2.1. iedaļai, kurā atgādināts, ka "[p]roduktu, kurš pēc nodošanas ekspluatācijā ir ievērojami izmainīts vai kuram veikts kapitālais remonts, lai mainītu tā sākotnējo darbību, uzskata par jaunu produktu, ja: i) ir mainīti tā sākotnējie darbības raksturlielumi, mērķis vai tips, neparedzot to sākotnējā riska novērtējumā; ii) ir mainījusies bīstamības būtība vai palielinājies riska līmenis saistībā ar attiecīgajiem Savienības saskaņošanas tiesību aktiem; kā arī iii) produkts ir darīts pieejams (vai nodots ekspluatācijā, ja piemērojamie tiesību akti attiecas arī uz nodošanu ekspluatācijā). Tas ir jāizvērtē katrā gadījumā atsevišķi, jo īpaši ņemot vērā konkrēto tiesību aktu mērķi un to produktu veidu, uz kuriem minētie tiesību akti attiecas."

94. Atjaunošanas, uzturēšanas vai remontēšanas darbības, kuru rezultātā tiek fiziski modificēti tirgū jau laisti produkti ar digitāliem elementiem, ne vienmēr ir uzskatāmas par būtiskām modifikācijām. Tāpēc būtu jāveic katra atsevišķa gadījuma novērtējums, lai pārliecinātos, vai šāda fiziska modifikācija ietekmē produkta ar digitāliem elementiem atbilstību I pielikuma I daļas pamatprasībām vai izraisa izmaiņas produkta paredzētajā nolūkā, uz kuru attiecas kiberdrošības riska novērtējums.

95. Bojātu daļu vai nolietotu elementu aizstāšana ar daļām ar labāku veiktspēju (piemēram, tehnikas progresa dēļ vai tāpēc, ka vecā daļa vairs netiek ražota) pati par sevi nerada remontētā produkta ar digitāliem elementiem būtisku modifikāciju. Būtiska modifikācija rodas tikai tad, ja veiktspējas izmaiņas vai remontētā produkta ar digitāliem elementiem darbības veids i) ietekmē tā atbilstību pamatprasībām vai ii) izraisa paredzētā nolūka izmaiņas, kas nebija aptvertas riska novērtējumā.

35. piemērs: datora servera ražotājs veic remontu, aizstājot bojātu RAM *moduli ar jaunu, veiktspējīgāku moduli. Servera atbilstība pamatprasībām netiek ietekmēta. Serveris darbojas labāk, bet tā jaunā veiktspēja joprojām ir servera paredzētā lietojuma robežās, kas ņemtas vērā kiberdrošības riska novērtējumā. Datora serveri neuzskata par būtiski modificētu.*

4.2. **Rezerves daļas**

96. KNA 2. panta 6. punktā ir noteikts, ka KNA nepiemēro rezerves daļām, ar kurām paredzēts aizstāt identiskus komponentus un kuras ražotas saskaņā ar tādām pašām specifikācijām kā minētie komponenti. Turklāt 29. apsvērumā ir noteikts, ka atbrīvojums attiecas gan uz rezerves daļām tādiem produktiem ar digitāliem elementiem, kas darīti pieejami pirms KNA piemērošanas sākuma, gan uz rezerves daļām, kurām jau ir veikta regulā noteiktā atbilstības novērtēšanas procedūra.

97. KNA 2. panta 6. punktā paredzētais atbrīvojums būtu jāsaprot tā, ka to piemēro tikai tad, ja rezerves daļa tiek īpaši piegādāta, lai remontētu jau tirgū laistu produktu ar digitāliem elementiem vai pagarinātu tā ilgizturību (neatkarīgi no tā, vai produkts laists tirgū pirms vai pēc 2027. gada 11. decembra). Ja produktu ar digitāliem elementiem piegādā kā savrupu produktu bez jebkādas saiknes ar iepriekš pastāvējuša produkta ar digitāliem elementiem uzturēšanu vai remontēšanu, to laiž tirgū KNA nozīmē, un tas nebūtu jāuzskata par rezerves daļu, uz kuru attiecas 2. panta 6. punkts. Uzturēšanas vai remontēšanas nolūkam vajadzētu būt skaidri saprotamam no piegādes konteksta, piemēram, pasūtījumā vai komercpiedāvājumā identificējot produktu ar digitāliem elementiem vai produktu saimi vai piegādājot rezerves daļu pa pēcpārdošanas vai servisa kanāliem. Šādi pamatojoši pierādījumi būtu arī jāglabā pieejami tirgus uzraudzības iestādēm. Tas vien, ka produktu ar digitāliem elementiem tehniski varētu izmantot kāda komponenta aizstāšanai, ja nav šādu apstākļu, nav pietiekams iemesls, lai uz to attiecinātu minēto atbrīvojumu.

98. Tādējādi, ja rezerves daļa ir identiska komponentam, kas jau ir iekļauts produktā ar digitāliem elementiem, kurš vai nu laists tirgū pirms KNA piemērošanas dienas, vai laists tirgū atbilstoši KNA, uz pašu rezerves daļu KNA neattiecas.

99. Novērtējot, vai rezerves daļa būtu jāuzskata par identisku komponentam, galvenā uzmanība būtu jāpievērš tās funkcionālajai lomai produktā ar digitāliem elementiem un īpašībām, kas var būt būtiskas kiberdrošībai. Lai gan vienmēr ir jāizvērtē katrs gadījums atsevišķi, atšķirības, kas neietekmē komponenta drošības raksturlielumus vai kiberdrošības riska profilu, pašas par sevi neliedz šai rezerves daļai ietilpt KNA 2. panta 6. punkta darbības jomā.

100. Turpretī atšķirības komponenta kiberdrošībai būtiskās īpašībās, piemēram, algoritmos, protokolos, kriptogrāfijas mehānismos, piekļuves kontroles funkcijās vai citās ar drošību saistītās īpašībās, var nozīmēt, ka jauno daļu nevar uzskatīt par identisku komponentam, kuru ar to paredzēts aizstāt.

101. Ja rezerves daļa nav identiska sākotnējam komponentam, tā pati par sevi ir produkts ar digitāliem elementiem, un tāpēc uz to attiecas KNA. Šādos gadījumos atbilstība pamatprasībām jānovērtē, ņemot vērā nomaiņas komponenta paredzēto nolūku. Īpaši svarīga ir nomaiņas komponenta funkcija nodrošināt saderību vai sadarbspēju ar esošu produktu ar digitāliem elementiem, tostarp tad, ja minētais produkts ar digitāliem elementiem ir laists tirgū pirms KNA piemērošanas sākuma. Ja minētā paredzētā nolūka vai tehnisko ierobežojumu dēļ konkrētas pamatprasības nav iespējams saprātīgi izpildīt, ražotājam tas ir jāatspoguļo kiberdrošības riska novērtējumā un jāīsteno atbilstoši alternatīvi vai kompensējoši riska mazināšanas pasākumi, lai neapdraudētu produkta ar digitāliem elementiem drošību. Kā aplūkots arī *2.6.* iedaļā *Kompleksas sistēmas*, gan tehniskajai dokumentācijai, gan lietotājam paredzētajai informācijai un norādījumiem ir būtiska nozīme, lai pārredzami aprakstītu konstatētos ierobežojumus, ar tiem saistītos kiberdrošības riskus un īstenotos riska mazināšanas pasākumus. Kā paskaidrots *4.1.* iedaļā *Fizisks remonts*, bojātu daļu vai nolietotu elementu aizstāšana ar labākas veiktspējas daļām pati par sevi nerada remontētā produkta ar digitāliem elementiem būtisku modifikāciju.

36. piemērs: ražotājs ir laidis ES tirgū savienotus kontrollerus. Vienā gadījumā kontrolleris tika laists tirgū 2026. gadā, pirms KNA piemērošanas dienas. Citā gadījumā kontrolleris tika laists tirgū 2028. gadā atbilstoši KNA. 2028. gadā abu veidu kontrolleros sabojājas digitālo sakaru modulis. Ražotājs kā rezerves daļu piegādā nomaiņas moduli, kas ir identisks sākotnējam modulim un ražots saskaņā ar tādām pašām specifikācijām.

Abos gadījumos nomaiņas modulis ietilpst 2. panta 6. punktā paredzētā atbrīvojuma darbības jomā. Uz pašu rezerves daļu KNA neattiecas, lai gan tā ir produkts ar digitāliem elementiem, jo tā aizstāj identisku komponentu produktā ar digitāliem elementiem. Remonts nav produkta ar digitāliem elementiem būtiska modifikācija.

37. piemērs: ražotājs 2026. gadā pirms KNA piemērošanas dienas laida ES tirgū savienotu rūpniecisko kontrolleri. 2028. gadā šajā kontrollerī sabojājas sakaru mikroshēma. Tā kā ražotājs šo mikroshēmu vairs neražo, tas kā rezerves daļu piegādāja jaunāku mikroshēmu ar līdzvērtīgu funkcionalitāti, bet atšķirīgu kriptogrāfisko implementāciju un atjauninātu drošās sāknēšanas mehānismu, lai saglabātu saderību un nodrošinātu turpmāku darbību.

Šādā gadījumā nomaiņas mikroshēmu nevar uzskatīt par identisku, jo atšķirības kriptogrāfiskajā implementācijā un drošās sāknēšanas mehānismā ietekmē mikroshēmas kiberdrošības īpašības. Tāpēc uz to neattiecas 2. panta 6. punktā paredzētais atbrīvojums, un tā ir produkts ar digitāliem elementiem, uz kuru attiecas KNA. Nomaiņas daļas atbilstība jānovērtē, ņemot vērā tās paredzēto nolūku, tostarp tās lomu sadarbspējas nodrošināšanā ar produktu ar digitāliem elementiem, kas laists tirgū pirms KNA piemērošanas sākuma.

38. piemērs: ražotājs 2028. gadā atbilstoši KNA laiž tirgū viedās ēkas kontrolleri. 2029. gadā šajā kontrollerī sabojājas bezvadu modulis. Tā kā ražotājs šo moduli vairs neražo, tas kā rezerves daļu piegādā jaunu moduli, kas veic to pašu funkciju, izmantojot tos pašus sakaru protokolus un drošības mehānismus, bet ir balstīts uz citu mikroshēmojumu un kam ir atjaunināta aparātprogrammatūra, kura nemaina kiberdrošībai būtiskās īpašības.

Šādā gadījumā nomaiņas moduli var uzskatīt par identisku. Tāpēc uz moduli attiecas 2. panta 6. punktā paredzētais atbrīvojums un KNA uz to neattiecas.

102. Atbrīvojumu attiecībā uz rezerves daļām piemēro neatkarīgi no tā, vai rezerves daļa aizstāj komponentu produktā ar digitāliem elementiem vai veselu produktu ar digitāliem elementiem, kas pats ir daļa no lielāka produkta, arī tad, ja minēto lielāko produktu ar digitāliem elementiem veido vairāki integrēti komponenti, ar nosacījumu, ka nomaiņas daļa tiek īpaši piegādāta kā rezerves daļa, kā paskaidrots iepriekšējos punktos.

*39. piemērs: 2027. gadā ražotājs laiž tirgū rūpnieciskās automatizācijas sistēmu, kurā kā viens no komponentiem ir integrēts programmējams loģiskais kontrolleris (*PLC*). 2031. gadā sabojājas* PLC *centrālais procesors (*CPU*). Ražotājs piedāvā divas remontēšanas iespējas: i) rezerves* CPU *bloka piegādi, ko var uzskatīt par identisku sākotnēji uzstādītajam* CPU*, vai ii) pilna rezerves* PLC *piegādi, ko var uzskatīt par identisku sākotnēji uzstādītajam* PLC*. Abos gadījumos nomaiņas daļu piegādā kā rezerves daļu, izmantojot ražotāja pēcpārdošanas servisa kanālu, un skaidri identificē rūpnieciskās automatizācijas sistēmu, kurai nomaiņas daļa paredzēta. Abos gadījumos nomaiņas daļa ietilpst 2. panta 6. punktā paredzētā atbrīvojuma darbības jomā neatkarīgi no tā, vai tiek aizstāts* PLC *komponents vai* PLC *kopumā.*

4.3. **Programmatūras atjauninājumi kā būtiskas modifikācijas**

103. Programmatūras izstrāde pēc būtības ir iteratīva, un tirgū jau laistie programmatūras produkti ar digitāliem elementiem tiek bieži un pastāvīgi atjaunināti. Šajā kontekstā ir lietderīgi sniegt papildu norādījumus, lai noteiktu, kad programmatūra uzskatāma par būtiski modificētu. Šādi norādījumi it īpaši ir paredzēti, lai palīdzētu programmatūras produktu ar digitāliem elementiem ražotājiem, kuri veic izmaiņas savos produktos, noteikt, vai minētās izmaiņas ir uzskatāmas par būtisku modifikāciju.

104. 39. apsvērumā ir norādīts, ka produkts ar digitāliem elementiem tiek būtiski modificēts, ja izmaiņas maina kiberdrošības riska līmeni un ja ražotājs šādu mainītu vai papildu risku nav ņēmis vērā savā riska novērtējumā un līdz ar to arī pamatprasību īstenošanā. Tāpēc ražotājam katrā atsevišķā gadījumā būtu jānovērtē, vai programmatūras atjauninājums rada jaunus vai palielinātus kiberdrošības riskus un vai šādi riski jau ir ņemti vērā tā riska novērtējumā.

105. Ja ražotājs produktā ar digitāliem elementiem ievieš jaunas funkcijas, kuru rezultātā mainās produkta paredzētais nolūks kopumā, visticamāk, ražotājs šādas izmaiņas savā riska novērtējumā nav ņēmis vērā. Šādos apstākļos izmaiņas parasti būtu uzskatāmas par būtisku modifikāciju.

40. piemērs: ražotājs laiž tirgū infopaneli, kas vāc datus no iekārtām un parāda tendences un brīdinājumus bez iespējas kontrolēt šādas iekārtas. Pēc tam ražotājs izstrādā jaunu minētā infopaneļa versiju, ieviešot funkcijas, kas ļauj tam kontrolēt iekārtas, tostarp pielāgot darbības parametrus un pēc kļūmēm iekārtas atkārtoti iedarbināt. Šo izmaiņu rezultātā infopaneļa paredzētais nolūks ir mainījies ārpus riska novērtējumā paredzētā tvēruma: no situācijas apzināšanās rīka tas ir kļuvis par produktu ar digitāliem elementiem, kas paredzēts citu ierīču darbības kontrolei. Tāpēc infopanelis ir būtiski modificēts.

41. piemērs: ražotājs laiž tirgū patērētājiem paredzētu lietojumprogrammu, kuras nolūks ir organizēt un attēlot personas datus, piemēram, e-pasta vēstules, ziņojumus vai dokumentus, un nodrošināt meklēšanas un filtrēšanas pamatfunkcijas. Pēc tam ražotājs ievieš atjauninājumu, kas ļauj lietojumprogrammai automātiski analizēt lietotāja saturu, lai veidotu uzvedības profilus un bez lietotāja iejaukšanās pieņemtu automatizētus lēmumus, kuri ietekmē satura prioritātes noteikšanu, slēpšanu vai ieteikšanu. Šo izmaiņu rezultātā programmatūras paredzētais nolūks mainās no lietotāja kontrolēta informācijas pārvaldības rīka uz automatizētu lēmumu pieņemšanas sistēmu, kas riska novērtējumā nebija paredzēta. Tāpēc lietojumprogramma ir būtiski modificēta.

106. Tomēr tajā pašā laikā ir iespējams, ka ražotājs pakāpeniski ievieš jaunas funkcijas, kas jau ir iekļautas tā riska novērtējumā vai kas pašas par sevi nemaina produkta ar digitāliem elementiem kiberdrošības riska profilu. Tā var būt, piemēram, gadījumā, ja ražotājs ir paredzējis šo funkciju izstrādi, jau aprakstījis un novērtējis ar tām saistītos riskus un īstenojis piemērotus riska mazināšanas pasākumus, lai nodrošinātu turpmāku atbilstību pamatprasībām. Tas var attiekties arī uz gadījumiem, kad ar jaunajām funkcijām netiek ieviestas izmaiņas, kas rada jaunus vai palielinātus riskus. Tāpēc šāda veida atjauninājumi nebūtu jāuzskata par būtiskām modifikācijām, jo tie nepalielina kiberdrošības risku un līdz ar to nemaina pamatprasību īstenošanu.

42. piemērs: ziņapmaiņas lietotne sākotnēji tiek izlaista versijā, kuras funkcionalitāte aprobežojas ar divpusēju ziņapmaiņu. Ražotāja riska novērtējums aptver grupu ziņapmaiņas vēlāku ieviešanu, tai skaitā, piemēram, ziņojumu maršrutēšanas sarežģītības palielināšanos. Vēlākā atjauninājumā ražotājs pievieno grupas tērzēšanas funkciju, kā arī administratora vadīklas un moderēšanas rīkus, kas jau bija paredzēti un novērtēti sākotnējā projektējumā. Atjauninājumā tiek ieviestas funkcijas, kas ietilpst sākotnējā paredzētā nolūka un riska novērtējuma tvērumā. Tāpēc ziņapmaiņas lietojumprogramma nav būtiski modificēta.

43. piemērs: ražošanas uzraudzības sistēma tiek laista tirgū ar infopaneļiem, kam iespējots tikai lasīšanas režīms, savukārt sistēmas arhitektūrā ir automatizēti kontroles elementi, taču tie joprojām ir atspējoti. Ražotāja riska novērtējumā ir skaidri aplūkota automatizētu vadības kontūru turpmāka aktivizēšana, tai skaitā ar slēgta kontūra vadību saistītie kiberdrošības riski, kā arī aizsardzības pasākumi, piemēram, operatora kontroles pārņemšanas mehānismi un bezatteices stāvokļi. Vēlākā atjauninājumā ražotājs iespējo automatizētās vadības funkcijas un aktivizē sākotnēji novērtētos aizsardzības pasākumus. Tāpēc ražošanas uzraudzības sistēma nav būtiski modificēta.

107. Savukārt pat ierobežotas vai šķietami nelielas jaunas funkcijas var radīt būtiskus kiberdrošības riskus, kas ietekmē atbilstību pamatprasībām. Tāpēc, novērtējot būtisku modifikāciju, nebūtu jāņem vērā izmaiņu mērogs vai sarežģītība, bet gan to iespējamā nelabvēlīgā ietekme uz produkta ar digitāliem elementiem kiberdrošības riska profilu un līdz ar to uz pamatprasību īstenošanu.

44. piemērs: ražotājs ievieš lietojumprogrammas atjauninājumu, pievienojot funkciju "atcerēties mani" jeb pastāvīgas pieteikšanās funkciju, kas lietotāja ērtībai lokāli glabā autentifikācijas pilnvaras. Lai gan funkcionalitātes tvērums ir ierobežots, tā rada jaunus ar autentifikācijas pilnvaru zādzību, neatļautu piekļuvi un sesijas pārņemšanu saistītus riskus, kas nebija ņemti vērā riska novērtējumā. Tāpēc atjauninājums ietekmē atbilstību pamatprasībām. Programmatūras lietojumprogramma ir būtiski modificēta.

45. piemērs: ražotājs esošam programmatūras produktam ar digitāliem elementiem pievieno jaunu reģistrēšanas un diagnostikas funkciju, kas ļauj eksportēt detalizētus sistēmas žurnālus traucējummeklēšanas nolūkā. Lai gan funkcionalitāte šķiet neliela, tās rezultātā sensitīvi darbības dati tiek vākti un glabāti nešifrētā formātā, radot datu izpaušanas riskus, kas iepriekš nebija novērtēti vai mazināti. Tāpēc izmaiņas var būtiski ietekmēt produkta ar digitāliem elementiem kiberdrošības riska profilu. Programmatūras produkts ar digitāliem elementiem ir būtiski modificēts.

108. Saskaņā ar KNA 39. apsvērumu drošības atjauninājumi parasti nav uzskatāmi par būtiskām modifikācijām, jo to galvenais mērķis ir samazināt kiberdrošības riska līmeni, kas saistīts ar produktu ar digitāliem elementiem. Tāpēc drošības atjauninājums, kas nemaina minētā produkta paredzēto nolūku un nerada jaunus kiberdrošības riskus, nebūtu jāuzskata par būtisku modifikāciju, pat ja minētais atjauninājums var ieviest būtiskas tehniskas izmaiņas. Tas attiecas arī uz gadījumiem, kad noteiktas funkcijas tiek mainītas vai ierobežotas vienīgi tādēļ, lai novērstu identificētās ievainojamības un nodrošinātu turpmāku atbilstību pamatprasībām.

46. piemērs: ražotājs ievieš drošības atjauninājumu ar mērķi novērst ievainojamību produkta ar digitāliem elementiem koda bāzē, labojot ievades validācijas kļūdu, kas varētu izraisīt bufera pārpildi, vai novēršot loģikas nepilnību, kas ļauj apiet autentifikāciju nepienācīgas sesijas pilnvaru validācijas dēļ. Atjauninājums maina programmatūras iekšējo implementāciju, neietekmējot produkta paredzēto nolūku un neradot jaunu pakļautību kiberdraudiem. Šāda atjauninājuma vienīgais mērķis ir samazināt kiberdrošības risku. Drošības atjauninājumu nevajadzētu uzskatīt par būtisku modifikāciju.

47. piemērs: ražotājs ievieš drošības atjauninājumu, kas stiprina esošās drošības konfigurācijas, piemēram, pastiprinot ugunsmūra noteikumus, atspējojot neizmantotos tīkla portus, mainot noklusējuma administratora paroles politiku vai padarot daudzfaktoru autentifikāciju obligātu, ja šāda funkcionalitāte jau bija pieejama vai paredzēta. Lai gan atjauninājums var ietekmēt to, kā lietotāji konfigurē produktu ar digitāliem elementiem vai piekļūst tam, tas nemaina tā paredzēto nolūku un ir paredzēts vienīgi tā drošības stāvokļa uzlabošanai. Drošības atjauninājumu nevajadzētu uzskatīt par būtisku modifikāciju.

48. piemērs: ražotājs laiž tirgū programmatūras produktu ar digitāliem elementiem, kas sakarus aizsargā, izmantojot konfigurējamu šifrēšanas sistēmu, kura atbalsta vairākus kriptogrāfijas algoritmus un atslēgu lielumus, kā aprakstīts produkta tehniskajā dokumentācijā un riska novērtējumā. Riska novērtējums aptver visas produktā ar digitāliem elementiem nodrošinātās kriptogrāfijas iespējas un paredz, ka nākotnē no noteiktiem algoritmiem būs jāatsakās. Riska novērtējums ietver arī riska mazināšanas pasākumus, piemēram, kriptogrāfisko elastību, iekšēju atslēgu pārvaldību un saderības testēšanu. Reaģējot uz jaunākajiem norādījumiem kriptogrāfijas jomā, ražotājs ievieš drošības atjauninājumu, kas atspējo novecojušu algoritmu un aktivizē spēcīgāku, jau atbalstītu alternatīvu, neieviešot jaunas ārējas atkarības un nemainot datu plūsmas. Tā kā ar atjauninājumu tiek īstenots drošības pasākums, kas bija paredzēts un novērtēts jau sākotnējā projektējumā, un tas nerada jaunus kiberdrošības riskus, drošības atjauninājums nebūtu jāuzskata par būtisku modifikāciju.

109. Turpretī drošības atjauninājumu var uzskatīt par būtisku modifikāciju, ja, neraugoties uz tā drošības mērķi, atjauninājuma rezultātā tiek mainīts produkta ar digitāliem elementiem paredzētais nolūks, pārsniedzot sākotnēji paredzēto, vai tiek radīti jauni vai palielināti kiberdrošības riski. Tas var būt, piemēram, gadījumā, kad atjauninājums būtiski maina minētā produkta robežas vai atkarību struktūru tādā veidā, kas nav paredzēts riska novērtējumā, piemēram, būtiski mainot datu plūsmas vai pievienojot jaunas no ārpuses pieejamas saskarnes.

49. piemērs: ražotājs laiž tirgū programmatūras produktu ar digitāliem elementiem, kas paredzēts, lai nodrošinātu lokālu datņu šifrēšanu lietotāja ierīcē glabātiem datiem, ļaujot lietotājiem pēc pieprasījuma šifrēt un atšifrēt datnes. Pēc tam, kad ir atklāta ievainojamība šifrēšanas darbplūsmā, ražotājs ievieš drošības atjauninājumu, kas izņem lokālās šifrēšanas funkciju un tā vietā pieprasa, lai visas datnes tiktu augšupielādētas, glabātas un apstrādātas ražotāja pārvaldītā attālinātās šifrēšanas pakalpojumā. Šo izmaiņu rezultātā produkts ar digitāliem elementiem vairs neveic lokālo šifrēšanu, kā sākotnēji bija paredzēts, bet gan darbojas kā attālinātās šifrēšanas un datu apstrādes pakalpojums. Lai gan atjauninājums tiek ieviests drošības apsvērumu dēļ, tas būtiski maina minētā produkta paredzēto nolūku tādā veidā, kas nav paredzēts riska novērtējumā, un tāpēc tas ir kvalificējams kā būtiska modifikācija.

50. piemērs: ražotājs laiž tirgū programmatūras produktu ar digitāliem elementiem, kas sakaru aizsardzībai starp produkta ar digitāliem elementiem komponentiem izmanto jau stabili ieviesušos šifrēšanas protokolu un iekšēji pārvaldītu atslēgu aprites ciklu. Reaģējot uz nesen konstatētajām kriptogrāfijas nepilnībām, ražotājs ievieš drošības atjauninājumu, kas aizstāj esošo šifrēšanas mehānismu ar citu protokolu, kurā prasīts izmantot ārēju atslēgu pārvaldības pakalpojumu, ko pārvalda trešā persona. Šo izmaiņu rezultātā būtiski mainās produkta ar digitāliem elementiem atkarības un datu plūsmas – tiek ieviestas jaunas ārējās saskarnes un rodas atkarība no trešo personu pakalpojumiem, kas nebija ņemti vērā riska novērtējumā. Lai gan atjauninājumu nosaka drošības apsvērumi, tas rada jaunus kiberdrošības riskus un tāpēc ir kvalificējams kā būtiska modifikācija.

110. Kā norādīts iepriekš 104. punktā, tas, vai programmatūras atjauninājums ir būtiska modifikācija, būtu jānovērtē katrā gadījumā atsevišķi. Veicot šo novērtējumu, ražotāji cita starpā var izvērtēt, vai programmatūras atjauninājums:

a) rada jaunus apdraudējuma vektorus, piemēram, papildu saskarnes, saziņas kanālus, izpildvides vai ārējas atkarības, kuru dēļ var īstenoties apdraudējumi;

b) dara iespējamus jaunus uzbrukuma scenārijus, tostarp, piemēram, jaunus veidus, kā varētu rasties neatļauta piekļuve produktam ar digitāliem elementiem vai tā apstrādātajiem datiem, manipulācijas ar tiem, iejaukšanās tajos vai to ļaunprātīga izmantošana;

c) maina iepriekš identificētu uzbrukuma scenāriju iespējamību, piemēram, samazinot to izmantošanai nepieciešamās pūles vai speciālās zināšanas, palielinot risku saistībā ar neuzticamiem aktoriem vai vājinot esošos aizsardzības pasākumus;

d) maina iepriekš identificētu uzbrukuma scenāriju iespējamo ietekmi, tai skaitā, piemēram, ietekmēto datu vai funkciju tvērumu, darbības, drošuma vai ekonomisko seku smagumu vai spēju atklāt un ierobežot incidentu vai atgūties no tā.

111. Dažos gadījumos programmatūras atjauninājums nerada jaunus apdraudējuma vektorus, nepadara iespējamus jaunus uzbrukuma scenārijus un būtiski nemaina iepriekš identificētu uzbrukuma scenāriju iespējamību vai ietekmi. Tas var liecināt, ka atjauninājums nerada jaunus vai palielinātus kiberdrošības riskus, ar noteikumu, ka riska novērtējuma pamatā esošie pieņēmumi un riska mazināšanas pasākumi joprojām ir derīgi un efektīvi. Tāpēc atjauninājums, visticamāk, nav kvalificējams kā būtiska modifikācija.

112. Savukārt cits programmatūras atjauninājums var radīt jaunus apdraudējuma vektorus, darīt iespējamus jaunus uzbrukuma scenārijus vai būtiski mainīt esošo uzbrukuma scenāriju iespējamību vai ietekmi. Šādos gadījumos ražotājam būtu atkārtoti jānovērtē produkta ar digitāliem elementiem kiberdrošības riski un jānosaka, vai pamatprasības joprojām tiek izpildītas, tai skaitā, vai atjauninājums rada jaunus vai palielinātus riskus, kas nav paredzēti riska novērtējumā.

113. Tas, vai programmatūras atjauninājums ir kvalificējams kā būtiska modifikācija, ir svarīgi, nosakot, vai piemērojami konkrēti KNA paredzētie pienākumi, kā izklāstīts 91. punktā. Tomēr neatkarīgi no minētās kvalifikācijas ražotāji joprojām ir atbildīgi par programmatūras atjauninājumu un savu produktu ar digitāliem elementiem drošības garantēšanu atbalsta periodā saskaņā ar KNA I pielikuma II daļā noteiktajām ievainojamību novēršanas prasībām. Turklāt neatkarīgi no tā, vai programmatūras atjauninājumi ir kvalificējami kā būtiskas modifikācijas, ražotājiem saskaņā ar 13. panta 7. punktu un 31. panta 2. punktu ir pienākums uzturēt riska novērtējumu un tehnisko dokumentāciju precīzu, pilnīgu un pastāvīgi atjauninātu.

4.4. **Būtiskas modifikācijas sekas**

114. Sekas, ko rada būtiska modifikācija, kuru veic persona, kas nav tirgū jau laista produkta ar digitāliem elementiem sākotnējais ražotājs, ir aplūkotas KNA 21. un 22. pantā. 21. pants attiecas uz importētājiem un izplatītājiem, savukārt 22. pants attiecas uz jebkuru fizisku vai juridisku personu, kas nav ražotājs, importētājs vai izplatītājs.

115. Ja būtisko modifikāciju veic produkta ar digitāliem elementiem sākotnējais ražotājs, sekas izriet no KNA 41. apsvērumā minētā vispāratzītā būtiskas modifikācijas jēdziena un ir sīkāk izklāstītas zilās rokasgrāmatas 2.1. iedaļā. Minētajā iedaļā ir noteikts, ka produkts, kam pēc laišanas tirgū ir veiktas būtiskas izmaiņas vai kapitālais remonts, ir uzskatāms par jaunu produktu, ja tā sākotnējais sniegums, nolūks vai tips ir mainīts, ir mainījies apdraudējuma raksturs vai ir palielinājies riska līmenis un produkts ar digitāliem elementiem ir darīts pieejams tirgū.

116. Tāpēc vispāratzītās sekas ir tādas, ka tad, ja produkta ar digitāliem elementiem modifikācija ir uzskatāma par būtisku modifikāciju un modificētais produkts ar digitāliem elementiem tiek darīts pieejams tirgū, KNA vajadzībām to uzskata par jaunu produktu ar digitāliem elementiem. Tādējādi būtiski modificētā produkta darīšana pieejamu tirgū ir jauna laišana tirgū. Tas ir spēkā neatkarīgi no tā, vai būtisko modifikāciju veic sākotnējais ražotājs vai cita persona. Lai nodrošinātu KNA vienādu un samērīgu piemērošanu dažādām personu kategorijām, kas var veikt būtisku modifikāciju, nākamajās apakšiedaļās aplūkoti pienākumi, kuri rodas personai, kas veic būtisko modifikāciju, ja būtiski modificētais produkts ar digitāliem elementiem tiek laists tirgū. Sekas attiecībā uz produkta ar digitāliem elementiem atbalsta periodu ir aplūkotas 5. iedaļā *Atbalsta periods*.

4.4.1. *Būtiskas modifikācijas, ko veikusi persona, kura nav sākotnējais ražotājs*

117. Saskaņā ar 21. un 22. pantu, ja tirgū jau laista produkta ar digitāliem elementiem būtisku modifikāciju veic fiziska vai juridiska persona, kas nav produkta ar digitāliem elementiem ražotājs, persona, kas veic būtisko modifikāciju un modificēto produktu ar digitāliem elementiem dara pieejamu tirgū, ir uzskatāma par modificētā produkta ar digitāliem elementiem ražotāju neatkarīgi no tā, vai minētā persona bija iesaistīta minētā produkta sākotnējā projektēšanā vai laišanā tirgū.

118. Regulas 22. pantā ir arī precizēts, ka uz personu, kas veic modifikāciju, 13. un 14. pantā noteiktie pienākumi attiecas tikai attiecībā uz to produkta ar digitāliem elementiem daļu, kuru ietekmē būtiskā modifikācija, ja minētā modifikācija neietekmē produkta ar digitāliem elementiem kiberdrošību kopumā.

119. Ja būtiska modifikācija ietekmē atbilstību pamatprasībām, bet negatīvi neietekmē produkta ar digitāliem elementiem kiberdrošību kopumā, personai, kas veic modifikāciju, 13. pants (arī pienākums nodrošināt atbilstību pamatprasībām un veikt atbilstības novērtēšanas procedūru) un 14. pants (ziņošanas pienākumi) attiecas tikai uz to produkta ar digitāliem elementiem daļu, kas ir būtiski modificēta ([16]). Turklāt sākotnējā ražotāja pienākumi saskaņā ar KNA joprojām attiecas uz sākotnējo tirgū laisto produktu ar digitāliem elementiem, nodrošinot ievainojamību novēršanas nepārtrauktību un neizmainīto daļu atbilstību.

120. Būtiskas modifikācijas gadījumu nevajadzētu jaukt ar integrācijas gadījumiem, kad persona samontē komponentus (arī attiecīgā gadījumā modificējot tos) jaunā produktā ar digitāliem elementiem, ko tā pati laiž tirgū. Šādos gadījumos integrētājs nemodificē produktu ar digitāliem elementiem, ko jau ir laidis tirgū cits ražotājs, bet gan laiž tirgū pats savu jaunu produktu ar digitāliem elementiem. Integrētājs KNA izpratnē ir šā jaunā produkta ar digitāliem elementiem ražotājs, un tam attiecībā uz produktu ar digitāliem elementiem kopumā ir pilnībā jāievēro regulas prasības. Ja ražotājs integrē komponentus, uz kuriem attiecas KNA, tas var izmantot komponentu ražotāju veiktās atbilstības nodrošināšanas darbības, lai atvieglotu savas atbilstības KNA nodrošināšanu.

51. piemērs: uzņēmums no trešo personu piegādātājiem iegādājas gatavus standarta mikrokontrolleru moduļus un savienotības komponentus, izstrādā īpašniekaparātprogrammatūru un sensoru komplektu un samontē tos savienotā lauksaimniecības uzraudzības produktā ar digitāliem elementiem, ko tas laiž tirgū ar savu nosaukumu. Lai gan uzņēmums ir modificējis pamatā esošos mikrokontrolleru moduļus un apvienojis tos ar citiem komponentiem, tas būtiski nemodificē produktu ar digitāliem elementiem, kas jau laists tirgū, bet gan laiž tirgū jaunu produktu ar digitāliem elementiem. Uzņēmums KNA vajadzībām ir lauksaimniecības uzraudzības ierīces ražotājs, un tam ir jāievēro regulas prasības attiecībā uz šo produktu kopumā.

([16]) Saskaņā ar zilās rokasgrāmatas 2.1. iedaļu "[n]av nepieciešams atkārtot testus un sagatavot jaunu dokumentāciju par aspektiem, kurus izmaiņas neietekmē. Pierādīt to, ka nav jāatjaunina visi tehniskās dokumentācijas elementi, ir tās fiziskās vai juridiskās personas pienākums, kura maina produktu vai ir likusi to mainīt. Fiziskā vai juridiskā persona, kas veic produkta izmaiņas vai liek tās veikt, ir atbildīga par izmainītā produkta atbilstību un sagatavo atbilstības deklarāciju, pat ja tā izmanto esošos testus un tehnisko dokumentāciju."

121. Ja būtiska modifikācija, ko veic persona, kura nav sākotnējais ražotājs, negatīvi ietekmē produkta ar digitāliem elementiem kiberdrošību kopumā, piemēram, tāpēc, ka modifikācija vairs nav vērsta uz konkrētu komponentu vai apakšsistēmu vai nav aprobežota ar to, modificētais produkts ar digitāliem elementiem, kas darīts pieejams tirgū, būtu jāuzskata par jaunu produktu ar digitāliem elementiem, uz kuru KNA attiecas kopumā. Šādos gadījumos ir mainījies minētā produkta vispārējais kiberdrošības riska profils, un modifikāciju nevar novērtēt, neņemot vērā produktu ar digitāliem elementiem kopumā. Uz personu, kas veic modifikāciju, attiecas 13. un 14. pantā noteiktie ražotāja pienākumi attiecībā uz modificēto produktu ar digitāliem elementiem kopumā.

4.4.2. *Būtiskas modifikācijas, ko veic sākotnējais ražotājs*

122. Ja būtisko modifikāciju veic sākotnējais ražotājs, arī programmatūras produktu ar digitāliem elementiem iteratīvās izstrādes kontekstā, minētais ražotājs joprojām ir ražotājs KNA vajadzībām. Tomēr būtiski modificētais produkts ar digitāliem elementiem ir uzskatāms par no jauna laistu tirgū.

123. Saskaņā ar zilās rokasgrāmatas 2.1. iedaļu sākotnējais ražotājs, kas laiž tirgū būtiski modificētu produktu ar digitāliem elementiem, attiecībā uz produkta ar digitāliem elementiem aspektiem, kurus būtiskā modifikācija neietekmē, var atkārtoti izmantot esošo dokumentāciju un testus. Īpaši tad, ja ražotājs laiž tirgū būtiski modificētas viena un tā paša produkta ar digitāliem elementiem versijas, atbilstības novērtēšanas procedūrā galvenā uzmanība būtu jāpievērš būtiski modificētajām produkta ar digitāliem elementiem daļām. Līdzīgi, ja atbilstības novērtēšanu veic trešā persona, atbilstības novērtēšanas struktūrai savā novērtējumā būtu jākoncentrējas uz būtiski modificētajām daļām. Attiecībā uz nemainītajām produkta ar digitāliem elementiem daļām tā var atkārtoti izmantot esošo dokumentāciju un testēšanas rezultātus.

124. Iepriekšējā apakšiedaļā izklāstītie samērīguma apsvērumi attiecas arī uz būtiskām modifikācijām, ko veic tāda produkta ar digitāliem elementiem sākotnējais ražotājs, kurš laists tirgū pirms 2027. gada 11. decembra. Šāda būtiska modifikācija, ko veicis sākotnējais ražotājs, pati par sevi neliek ražotājam nodrošināt visa produkta ar digitāliem elementiem, kas laists tirgū pirms minētā datuma, pilnīgu atbilstību KNA, ja vien modifikācija negatīvi neietekmē produkta ar digitāliem elementiem kiberdrošību kopumā. Ja modifikācija neietekmē produkta ar digitāliem elementiem kiberdrošību kopumā, sākotnējā ražotāja pienākumi attiecībā uz modifikāciju būtu jāattiecina tikai uz būtiski modificētajām daļām.

5. **ATBALSTA PERIODS**

125. KNA 13. panta 8. punktā ir paredzēts, ka ražotājiem jānosaka atbalsta periods, kurā produkta ar digitāliem elementiem, tostarp tā komponentu, ievainojamības tiek risinātas efektīvi un saskaņā ar I pielikuma II daļā noteiktajām kiberdrošības pamatprasībām. Atbalsta periods atspoguļo laikposmu, kurā sagaidāms, ka produkts ar digitāliem elementiem tiks izmantots (paredzamais lietošanas laiks), un tas būtu jānosaka, ņemot vērā 13. panta 8. punktā paredzētos kritērijus, it īpaši pamatotas lietotāju gaidas, produkta ar digitāliem elementiem iezīmes, tostarp tā paredzēto nolūku, kā arī attiecīgos Savienības tiesību aktus, kas nosaka produktu ar digitāliem elementiem darbmūžu ([17]). Kopumā šādi kritēriji ir jāņem vērā tā, lai, nosakot atbalsta periodu, nodrošinātu proporcionalitāti.

([17]) Saskaņā ar 13. panta 8. punktu papildu kritēriji, ko var ņemt vērā, ir citu ražotāju tirgū laistu produktu ar digitāliem elementiem, kuri nodrošina līdzīgu funkcionalitāti, atbalsta periodi, darbības vides pieejamība, no trešām personām iegūtu integrētu komponentu, kas nodrošina pamatfunkcijas, atbalsta periodi, kā arī attiecīgie KNA administratīvās sadarbības grupas (*ADCO*) un Komisijas sniegtie norādījumi.

126. Turklāt 13. panta 8. punktā ir noteikts, ka atbalsta periodam jābūt vismaz pieciem gadiem, izņemot gadījumus, kad paredzams, ka produkts ar digitāliem elementiem tiks lietots mazāk nekā piecus gadus, un tādā gadījumā atbalsta periods atbilst paredzamajam lietošanas laikam. Tāpēc minimālais atbalsta periods darbojas tikai kā aizsardzības pasākums, nodrošinot, ka ievainojamības tiek risinātas pietiekami ilgu laiku, vienlaikus ļaujot ražotājiem ņemt vērā produktus ar digitāliem elementiem ar patiesi īsāku paredzamo lietošanas laiku. 60. apsvērumā šajā sakarā ir sniegti papildu norādījumi, precizējot, ka, ja pamatoti paredzams, ka produkts ar digitāliem elementiem tiks izmantots ilgāk nekā piecus gadus, ražotājiem attiecīgi būtu jānodrošina garāki atbalsta periodi. Tāpēc piecu gadu atbalsta periods nav uzskatāms par noklusējuma periodu visiem produktiem ar digitāliem elementiem. Tā vietā ražotājam būtu jānosaka piemērots atbalsta periods, ņemot vērā 13. panta 8. punktā minētos kritērijus.

127. 13. panta 19. punktā ir noteikts, ka ražotājiem iegādes brīdī ir skaidri un saprotami jānorāda atbalsta perioda beigu datums (vismaz mēnesis un gads). Tajā arī noteikts, ka, ja tas ir tehniski iespējams, ņemot vērā produkta ar digitāliem elementiem iezīmes, ražotājiem pēc atbalsta perioda beigām jāizvieto attiecīgs paziņojums lietotājiem. Šā pienākuma mērķis ir nodrošināt lietotājiem pārredzamību attiecībā uz to, cik ilgi var gaidīt drošības atbalstu.

128. Attiecībā uz programmatūras produktiem ar digitāliem elementiem, kurus bieži izstrādā un izlaiž iteratīvi un kuru būtiski modificētas versijas laika gaitā var bieži laist tirgū, atbalsta periods ir jāsaprot, ņemot vērā šo izstrādes modeli. Katrai būtiski modificētai tirgū laista programmatūras produkta ar digitāliem elementiem versijai ir jābūt deklarētam atbalsta periodam, kas atbilst 13. panta 8. punktam. Tas ietver vismaz piecu gadu minimālo atbalsta periodu, ja vien nav pierādāms, ka attiecīgās versijas paredzamais lietošanas laiks ir īsāks, kā precizēts arī 60. apsvērumā. *5.1.* iedaļā *Būtiskas modifikācijas un atbalsta periods* ir arī precizēts, ka tad, ja būtiskā modifikācija neizraisa izmaiņas faktoros, kas sākotnēji noteica produkta ar digitāliem elementiem paredzamo lietošanas laiku, sākotnējais atbalsta periods nemainās (t. i., arī gadījumos, kad atlikušais atbalsta periods ir īsāks par pieciem gadiem).

129. Regulas 13. panta 10. punktā ir paredzēta elastība attiecībā uz programmatūras produktiem ar digitāliem elementiem, ļaujot ražotājiem, ievērojot konkrētus nosacījumus, nodrošināt atbilstību I pielikuma II daļas 2. punktā noteiktajai ievainojamību novēršanas prasībai (risināt ievainojamības un tās novērst) tikai attiecībā uz programmatūras produkta ar digitāliem elementiem versiju, kas pēdējā laista tirgū. Tas ir atļauts, ja iepriekš tirgū laistu versiju lietotājiem bez maksas ir pieejama pēdējā tirgū laistā versija un viņiem nerodas papildu izmaksas, pielāgojot aparatūras un programmatūras vidi, kurā tie izmanto produkta sākotnējo versiju.

130. Piemērojot 13. panta 10. punktu, jēdziens "papildu izmaksas" būtu jāinterpretē praktiski un samērīgi, ņemot vērā parasto un paredzamo praksi programmatūras uzturēšanā un darbībā. Tas neietver saprātīgas praktiskas pūles, kas parasti saistītas ar programmatūras atjauninājumu piemērošanu vai drošas darbības vides uzturēšanu, piemēram, personāla darba laiku, regulāru testēšanu, konfigurācijas pielāgojumus vai pamatā esošo programmatūras atkarību atjaunināšanu, kas nepieciešama saistībā ar aprites cikla beigas sasniegušiem komponentiem vai zināmām drošības ievainojamībām. Turpretī "papildu izmaksas" attiecas uz slogu, kas pārsniedz to, ko parasti var sagaidīt programmatūras atjauninājumu kontekstā, piemēram, jaunas aparatūras obligātu iegādi, infrastruktūras nomaiņu vai būtiskas izmaiņas darbības vidē.

131. Attiecībā uz pastāvīgi mainīgiem programmatūras produktiem ar digitāliem elementiem ražotāji var salīdzinoši īsos intervālos laist tirgū secīgas būtiski modificētas versijas un sagaidīt, ka lietotāji tās regulāri atjauninās. Šādos gadījumos katras būtiski modificētās versijas deklarētajam atbalsta periodam ir jāatbilst 13. panta 8. punktam brīdī, kad tā tiek laista tirgū. Citiem vārdiem sakot, ražotājam ir jādeklarē jauns atbalsta periods šai būtiski modificētajai versijai. Tomēr ražotāji var izmantot 13. panta 10. punktā paredzēto iespēju un pārtraukt risināt un novērst

ievainojamības agrākās versijās, tiklīdz lietotāji var bez maksas un bez iepriekš minētajām papildu izmaksām pāriet uz vēlāku versiju, pat ja tādējādi šo agrāko versiju faktiskais atbalsta periods kļūst īsāks ([18]). Uz ražotāju joprojām attiecas citas I pielikuma II daļā noteiktās ievainojamību novēršanas prasības, kā arī 14. pantā noteiktie ziņošanas pienākumi. Kā paskaidrots arī 40. apsvērumā, šīs prasības cita starpā ietver šādas prasības attiecībā uz visām turpmākajām būtiski modificētajām programmatūras produkta ar digitāliem elementiem versijām, kas laistas tirgū: i) uzturēt politiku koordinētai ievainojamību atklāšanai un ii) pasākumus, kas sekmē informācijas apmaiņu par iespējamām ievainojamībām ([19]).

52. piemērs: ražotājs laiž ES tirgū viedtālruņu modeli un deklarē X gadu atbalsta periodu no tirgū laišanas dienas, kura laikā tas nodrošinās drošības atjauninājumus, lai novērstu ievainojamības. Šajā laikposmā ražotājs izlaiž regulārus programmatūras atjauninājumus un būtiski modificētas operētājsistēmas versijas, ko lietotāji var instalēt bez maksas un bez nepieciešamības pēc jaunas aparatūras.

Ražotājs saskaņā ar 13. panta 10. punktu var risināt un novērst ievainojamības operētājsistēmas jaunākajā versijā, kas darīta pieejama minētajam viedtālruņa modelim, ar noteikumu, ka iepriekšējās versijas var atjaunināt bez maksas un bez papildu izmaksām. Atbalsta periodā uz ražotāju joprojām attiecas citas ievainojamību novēršanas prasības, piemēram, koordinētas ievainojamības atklāšanas un informācijas apmaiņas pasākumi.

53. piemērs: ražotājs laiž tirgū uzņēmuma programmatūras produktu ar digitāliem elementiem un ik pēc dažiem mēnešiem izlaiž būtiski modificētas versijas, kurās iekļauti drošības uzlabojumi, jaunas funkcijas un saderība ar atjauninātām operētājsistēmām un platformām. Katra versija tiek laista tirgū ar deklarētu atbalsta periodu saskaņā ar 13. panta 8. punktu. Ražotājs paredz, ka lietotāji parastās ekspluatācijas gaitā regulāri pāries uz jaunākām versijām, un nodrošina bezmaksas piekļuvi jaunākajai versijai. Jauninājumu ieviešanai var būt vajadzīgi saprātīgi praktiski centieni, piemēram, testēšana vai konfigurācijas pielāgojumi, bet nav vajadzīgas papildu izmaksas, piemēram, jaunas aparatūras iegāde vai būtiskas infrastruktūras izmaiņas. Šajā kontekstā ražotājs var izmantot 13. panta 10. punktā paredzēto iespēju un pārtraukt risināt un novērst ievainojamības agrākās versijās, tiklīdz lietotāji var pāriet uz jaunāko versiju, vienlaikus turpinot ievērot pārējās ievainojamību novēršanas prasības attiecībā uz visām turpmākajām būtiski modificētajām versijām.

5.1. **Būtiskas modifikācijas un atbalsta periods**

132. Kā izklāstīts 4.4. iedaļā *Būtiskas modifikācijas sekas*, ja produkta ar digitāliem elementiem modifikācija ir uzskatāma par būtisku modifikāciju un modificētais produkts ar digitāliem elementiem tiek darīts pieejams tirgū, KNA vajadzībām tas ir uzskatāms par jaunu produktu, un darbība, ar ko būtiski modificēto produktu ar digitāliem elementiem dara pieejamu tirgū, ir jauna laišana tirgū. Tāpēc ir lietderīgi precizēt, kā šī jaunā laišana tirgū ietekmē būtiski modificētā produkta ar digitāliem elementiem atbalsta periodu.

133. Būtiski modificēta produkta ar digitāliem elementiem atbalsta periods būtu jānosaka, ņemot vērā minētā produkta paredzamo lietošanas laiku un KNA 13. panta 8. punktā noteiktos kritērijus. Tāpēc būtiskas modifikācijas gadījumā produkts būtu atkārtoti jānovērtē atbilstoši minētajiem kritērijiem, taču tas automātiski nenozīmē atbalsta perioda sākšanu no jauna vai tā pagarināšanu. Svarīgs jautājums ir par to, vai būtiskā modifikācija ietekmē faktorus, kas sākotnēji noteica produkta paredzamo lietošanas laiku un līdz ar to sākotnējo atbalsta periodu.

([18]) Jāatgādina, ka 13. panta 19. punktā ražotājiem ir noteikts pienākums, ja tas ir tehniski iespējams, ņemot vērā produkta ar digitāliem elementiem būtību, parādīt lietotājiem paziņojumu, informējot viņus, ka produkta ar digitāliem elementiem atbalsta periods ir beidzies. Tāpēc, ja agrākās versijās tiek pārtraukta ievainojamību novēršana, paredzams, ka lietotāji, kuri nav pārgājuši uz jaunāko versiju, tiks informēti, ja tas būs tehniski iespējams.

([19]) Jāatzīmē, ka tad, ja lietotāji bez papildu izmaksām var pāriet uz programmatūras jaunāko versiju, ražotāji tomēr var izvēlēties turpināt risināt un novērst ievainojamības minētās programmatūras agrākajās versijās, tostarp par maksu vai saskaņā ar citiem komerciāliem nosacījumiem. KNA nav prasīts ražotājiem bez maksas nodrošināt drošības atjauninājumus šādām agrākām versijām.

134. Ja būtiskā modifikācija minētos faktorus neietekmē, 13. panta 8. punktā noteiktie kritēriji joprojām norāda to pašu paredzamo lietošanas laiku, kas sākotnēji noteikts, un modificētā produkta ar digitāliem elementiem atbalsta periodam būtu jāatbilst sākotnēji tirgū laistā produkta atlikušajam paredzamajam lietošanas laikam. Tā tas parasti būs gadījumos, kad paredzamo lietošanas laiku galvenokārt noteica faktori, kurus modifikācija nemaina, piemēram, aparatūras komponentu fiziskā ilgizturība, ja būtiskā modifikācija attiecas tikai uz programmatūras funkcionalitāti vai aizmugursistēmas pakalpojumiem.

54. piemērs: *ražotājs laiž tirgū robotizētu putekļsūcēju, kura paredzamais lietošanas laiks ir X gadi, ko nosaka, pamatojoties uz produkta ar digitāliem elementiem īpašībām, tostarp aparatūras komponentu fizisko ilgizturību un nodiluma īpašībām, un ņemot vērā pamatotas lietotāju gaidas attiecībā uz minētā produkta darbmūžu. Ražotājs nosaka X gadu atbalsta periodu. Pēc Y gadiem ražotājs izlaiž programmatūras atjauninājumu, kas kvalificējams kā būtiska modifikācija, pievienojot jaunus tīrīšanas veidus un navigācijas funkcijas. Programmatūras atjauninājums neietekmē aparatūras fizisko ilgizturību un nemaina pamatotas lietotāju gaidas attiecībā uz minētā produkta darbmūžu. Tāpēc 13. panta 8. punkta kritēriji joprojām norāda uz to pašu paredzamo lietošanas laiku. Modificētā produkta ar digitāliem elementiem atbalsta periods atbilst sākotnēji noteiktajam atlikušajam paredzamajam lietošanas laikam.*

55. piemērs: ražotājs laiž tirgū sarežģītu rūpniecisku iekārtu ar digitāliem elementiem, kurai ir mākoņa aizmugursistēma, kas ir attālinātas datu apstrādes risinājums. Paredzamais lietošanas laiks ir X gadi, ko nosaka, ņemot vērā pamatotas lietotāju gaidas un produkta ar digitāliem elementiem iezīmes, piemēram, iekārtas aparatūras fizisko ilgizturību un paredzamo nolietojumu. Atbalsta periods ir noteikts tā, lai tas atbilstu X gadu paredzamajam lietošanas laikam. Pēc Y gadiem ražotājs pārveido mākoņa aizmugursistēmas arhitektūru (attālinātas datu apstrādes risinājumu), ieviešot jaunas API *un datu plūsmas tādā veidā, kas ir uzskatāms par produkta ar digitāliem elementiem būtisku modifikāciju, bet nemaina minētā produkta būtību un neietekmē lietotāju gaidas. Tāpēc 13. panta 8. punkta kritēriji joprojām norāda uz to pašu paredzamo lietošanas laiku. Modificētā produkta ar digitāliem elementiem atbalsta periods atbilst sākotnēji noteiktajam atlikušajam paredzamajam lietošanas laikam.*

135. Ja būtiskā modifikācija ietekmē faktorus, kas sākotnēji noteica produkta ar digitāliem elementiem paredzamo lietošanas laiku, ražotājam būtu jāpārrēķina atbalsta periods, lai atspoguļotu jauno paredzamo lietošanas laiku, attiecīgi piemērojot 13. panta 8. punkta kritērijus. Tas var būt, piemēram, gadījums, kad tiek veiktas aparatūras modernizācijas modifikācijas, kas pagarina produkta ekspluatācijas laiku, vai kad produkta pamatprogrammatūra tiek būtiski pārprogrammēta vai pārrakstīta, tādējādi būtiski mainot tā paredzamo lietošanas laiku ([20]).

*56. piemērs: ražotājs laiž tirgū programmējamu loģisko kontrolleri (*PLC*) ar paredzamo lietošanas laiku X gadi, ko galvenokārt nosaka, pamatojoties uz produkta ar digitāliem elementiem būtību un pamatā esošās aparatūras ilgizturību. Ir attiecīgi noteikts atbalsta periods. Vairākus gadus pēc sākotnējās laišanas tirgū ražotājs veic būtisku modifikāciju, aizstājot* PLC *iegulto datošanas platformu, tostarp procesoru, atmiņu un izpildlaika vidi, ar jaunas paaudzes komponentiem, kas paredzēti ievērojami ilgākam ekspluatācijas laikam. Modifikācijas rezultātā mainās pamatotas lietotāju gaidas un produkta ar digitāliem elementiem iezīmes:* PLC *lietotājs tagad var pamatoti sagaidīt, ka* PLC *joprojām varēs tikt produktīvi izmantots arī pēc sākotnēji deklarētā paredzamā lietošanas laika beigām, jo to atbalstīs jaunā datošanas platforma. Tāpēc 13. panta 8. punkta kritēriji norāda uz ilgāku paredzamo lietošanas laiku, un ražotājs attiecīgi pārrēķina konkrētā* PLC *atbalsta periodu.*

6. **NOZĪMĪGI UN KRITISKI SVARĪGI PRODUKTI AR DIGITĀLIEM ELEMENTIEM**

136. KNA 7. panta 1. punktā ir noteikts, ka produktus ar digitāliem elementiem, kuriem ir regulas III pielikumā noteiktās produktu kategorijas pamatfunkcionalitāte, uzskata par "nozīmīgiem produktiem ar digitāliem elementiem". III pielikumā nozīmīgi produkti ar digitāliem elementiem ir sīkāk iedalīti I un II klasē. Līdzīgi 8. panta 1. punktā ir noteikts, ka produktus ar digitāliem elementiem, kuriem ir KNA IV pielikumā noteiktās produktu kategorijas pamatfunkcionalitāte, uzskata par "kritiski svarīgiem produktiem ar digitāliem elementiem" ([21]).

([20]) Jāatgādina, ka (un tas norādīts *4.1.* iedaļā *Fizisks remonts*) atjaunošanas, uzturēšanas vai remontēšanas darbības parasti neuzskata par būtiskām modifikācijām.

([21]) Komisijas Īstenošanas regulā (ES) 2025/2392 ir sniegts nozīmīgu un kritiski svarīgu produktu kategoriju tehniskais apraksts.

137. Produkta ar digitāliem elementiem klasificēšana par nozīmīgu vai kritiski svarīgu produktu vai, gluži pretēji, par "noklusējuma" kategorijai ([22]) piederošu produktu ir būtiska, nosakot atbilstības novērtēšanas procedūru, kas ražotājam saskaņā ar 32. pantu jāievēro pirms minētā produkta ar digitāliem elementiem laišanas tirgū. Proti, produkti ar digitāliem elementiem noklusējuma kategorijā vienmēr var izmantot iekšējās kontroles procedūru, kuras pamatā ir A modulis ("pašnovērtējums") ([23]). Nozīmīgiem I vai II klases produktiem ar digitāliem elementiem un kritiski svarīgiem produktiem ar digitāliem elementiem piemēro stingrākas atbilstības novērtēšanas procedūras. Tas neattiecas uz nozīmīgiem I vai II klases produktiem ar digitāliem elementiem, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra un ir laisti tirgū; attiecībā uz tiem saskaņā ar 32. panta 5. punktu ražotāji drīkst piemērot noklusējuma kategorijas procedūras.

138. Tāpēc pamatfunkcionalitātes jēdziens ir būtisks, lai ražotājs varētu noteikt piemērojamo atbilstības novērtēšanas režīmu. Tomēr KNA šis jēdziens nav skaidri definēts. Produkti ar digitāliem elementiem var pildīt virkni funkciju, no kurām dažas var būt palīgfunkcijas attiecībā pret produkta pamatfunkcionalitāti, un tām nevajadzētu ietekmēt produkta klasificēšanu noklusējuma kategorijā, nozīmīgu produktu I klasē, nozīmīgu produktu II klasē vai kritiski svarīgu produktu kategorijā. Tāpēc ir lietderīgi sniegt papildu norādījumus, lai palīdzētu ražotājiem pareizi veikt attiecīgās atbilstības novērtēšanas procedūras un tirgus uzraudzības iestādēm nodrošināt KNA saskaņotu izpildi visā ES.

6.1. **Pamatfunkcionalitāte**

139. Produkta ar digitāliem elementiem pamatfunkcionalitāti veido tā galvenās iezīmes un tehniskās spējas, bez kurām tas nespētu īstenot paredzēto nolūku. To var novērtēt, ņemot vērā minētā produkta īpašo kontekstu un lietošanas nosacījumus, cita starpā ņemot vērā informāciju, ko ražotājs sniedz lietošanas pamācībā, reklāmas vai pārdošanas materiālos un paziņojumos, kā arī tehniskajā dokumentācijā.

*57. piemērs: programmatūras produkts ar digitāliem elementiem nodrošina abstrakcijas slāni pār pamatā esošo aparatūru un pārvalda programmatūras komponentu izpildi. Tā galvenās funkcijas ietver aparatūras un perifērijas ierīču inicializēšanu, procesu un atmiņas pārvaldību, ievadizvades vadību, uzdevumu plānošanu, resursu piešķiršanu, kā arī sistēmas pakalpojumu un lietojumprogrammu saskarņu (*API*) nodrošināšanu, ar kuru starpniecību lietojumprogrammas mijiedarbojas ar ierīces aparatūras un programmatūras resursiem. Tehniskajā dokumentācijā norādīts, ka produkts ar digitāliem elementiem organizē datošanas resursus, nodrošina sistēmas konfigurāciju piemērošanu un nodrošina standartizētas saskarnes programmatūras moduļiem un savienotajām perifērijas ierīcēm. Ražotājs uzsver, ka šīs spējas ļauj platformai darboties kā centrālai programmatūras videi, kurā lietojumprogrammas var uzticami darboties. Produktam ar digitāliem elementiem ir operētājsistēmas pamatfunkcionalitāte, kā aprakstīts Īstenošanas regulas (ES) 2025/2392 I pielikuma 11. punktā.*

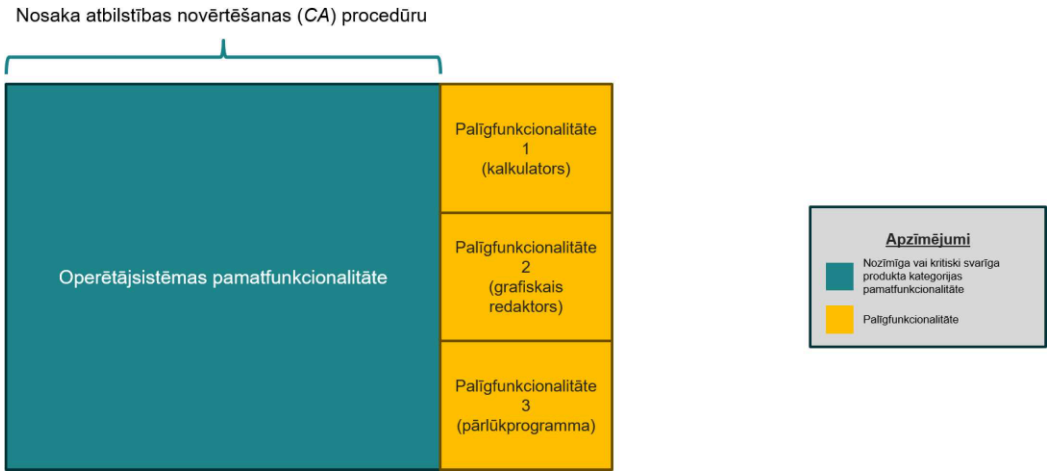
140. Produkta ar digitāliem elementiem funkcionalitāte reti kad aprobežojas tikai ar tā pamatfunkcionalitāti, jo produkti ar digitāliem elementiem bieži, ja ne vienmēr, veic papildu funkcijas, kas neveicina produkta pamatfunkcionalitāti. Tas var ietvert arī komponentus, kuriem pašiem ir cita nozīmīga vai kritiski svarīga produkta ar digitāliem elementiem funkcionalitāte. Tomēr tas, ka produkts ar digitāliem elementiem veic funkcijas, kas atšķiras no funkcijām, kuras sīki izklāstītas nozīmīgu vai kritiski svarīgu produktu ar digitāliem elementiem tehniskajos aprakstos, vai papildina tās, pats par sevi nenozīmē, ka produktam nevar būt viena no šādām pamatfunkcionalitātēm.

([22]) Apzīmējums "noklusējuma kategorija" KNA nav definēts. Termina lietojums šajā dokumentā attiecas uz produktiem ar digitāliem elementiem, kuriem nav KNA III vai IV pielikumā noteiktās produktu kategorijas pamatfunkcionalitātes un uz kuriem līdz ar to attiecas 32. panta 1. punktā noteiktais atbilstības novērtēšanas režīms.

([23]) Tomēr ražotājs vienmēr var izvēlēties piemērot stingrāku atbilstības novērtēšanas procedūru, kā noteikts 32. panta 1. punktā.

2. attēls

Ilustrācija, kurā attēlots tas, kā pamatfunkcionalitāte, nevis palīgfunkcionalitātes, nosaka piemērojamo atbilstības novērtēšanas procedūru



141. Produktam ar digitāliem elementiem var būt spēja pildīt nozīmīgu vai kritiski svarīgu produktu kategorijas funkcijas, tomēr tā pamatfunkcionalitāte var atšķirties no šādas produktu kategorijas pamatfunkcionalitātes. Šādos gadījumos minētais produkts ar digitāliem elementiem nebūtu kvalificējams kā nozīmīgs vai kritiski svarīgs produkts ar digitāliem elementiem. Kā skaidri noteikts KNA 7. panta 1. punktā attiecībā uz nozīmīgiem produktiem ar digitāliem elementiem (un piemērojot to pašu loģiku kritiski svarīgiem produktiem ar digitāliem elementiem), nozīmīga vai kritiski svarīga produkta ar digitāliem elementiem integrēšana pati par sevi nepadara produktu ar digitāliem elementiem par nozīmīgu vai kritiski svarīgu produktu ar digitāliem elementiem.

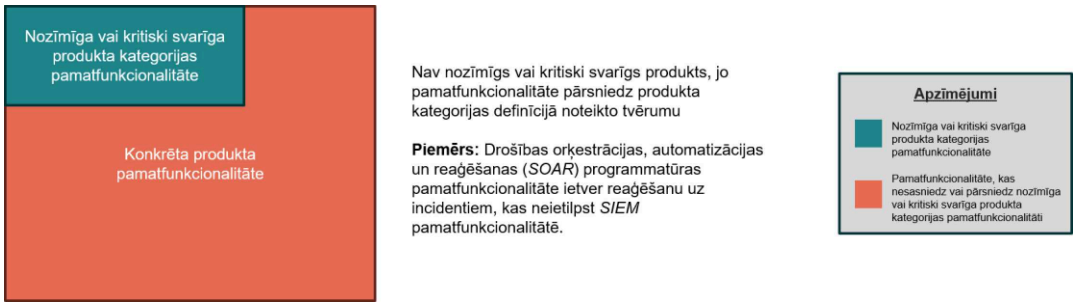
58. piemērs: viedtālrunī ir integrēta operētājsistēma, kas nodrošina Īstenošanas regulas (ES) 2025/2392 I pielikuma 11. punktā aprakstītās funkcijas. Lai gan operētājsistēma ļauj pārvaldīt aparatūras resursus un izpildīt lietojumprogrammas, viedtālrunim kopumā ir atšķirīga pamatfunkcionalitāte (piemēram, iespēja lietotājiem sazināties un piekļūt informācijai un pakalpojumiem). Operētājsistēmas integrācija vien nenozīmē, ka viedtālrunim ir operētājsistēmas pamatfunkcionalitāte.

142. Daži produkti ar digitāliem elementiem var būt līdzīgi nozīmīgu vai kritiski svarīgu produktu kategorijai vai piederēt pie tās pašas vispārīgās produktu saimes, tomēr to pamatfunkcionalitāte var būtiski pārsniegt vai būtiski atpalikt no minētās kategorijas pamatfunkcionalitātes. Tas neattiecas uz gadījumiem, kad produktam ar digitāliem elementiem ir papildu funkcijas, kas tikai papildina vai uzlabo pamatfunkcionalitāti, kura pati par sevi atbilst nozīmīgu vai kritiski svarīgu produktu kategorijas pamatfunkcionalitātei; šādos gadījumos produkts ar digitāliem elementiem saglabā minētās kategorijas pamatfunkcionalitāti un tiek attiecīgi klasificēts. Šā novērtējuma pamatā vajadzētu būt minētā produkta galvenajām iezīmēm un tehniskajām spējām, kas objektīvi izvērtētas, ņemot vērā tā paredzēto nolūku, nevis veidu, kādā produkts ar digitāliem elementiem tiek aprakstīts vai tirgots, ja minētais apraksts neatspoguļo produkta faktiskās tehniskās īpašības.

59. piemērs: drošības orķestrācijas, automatizācijas un reaģēšanas (SOAR) programmatūra bieži spēj pildīt produktu ar digitāliem elementiem kategorijas "drošības informācijas un notikumu pārvaldības (SIEM) sistēmas" funkcijas, proti, vākt datus no vairākiem avotiem, tos analizēt un korelēt un attēlot kā drošības vajadzībām praktiski izmantojamu informāciju. Tomēr šīs programmatūras pamatfunkcionalitāte būtiski pārsniedz SIEM pamatfunkcionalitāti, jo tās tehnisko spēju pamatelementi ietver arī tādus pakalpojumus kā reaģēšana uz incidentiem. Tāpēc parasti neuzskata, ka SOAR programmatūrai ir SIEM sistēmu pamatfunkcionalitāte.

3. attēls

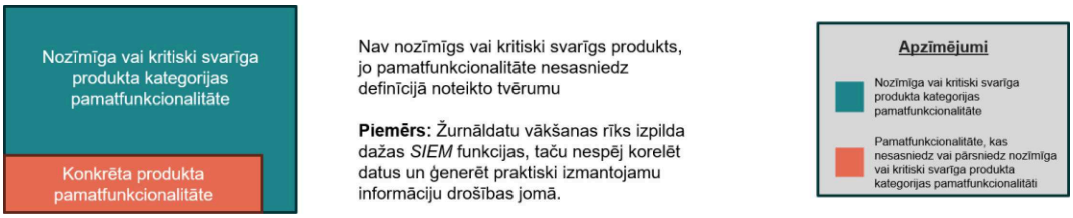
Tāda produkta ar digitāliem elementiem pamatfunkcionalitātes ilustrācija, kas būtiski pārsniedz nozīmīgu vai kritiski svarīgu produktu kategorijas definīciju



60. piemērs: daži žurnāldatu vākšanas un vizualizācijas rīki spēj uzņemt žurnāldatus un parādīt vienkāršus infopaneļus ar sistēmas notikumiem. Lai gan šādi rīki var atbalstīt drošības uzraudzību, to pamatfunkcionalitāte nesasniedz SIEM *sistēmu pamatfunkcionalitāti, jo tie neveic datu korelāciju un nesniedz praktiski izmantojamu informāciju drošības jomā. Tāpēc parasti neuzskata, ka šādiem rīkiem ir* SIEM *sistēmu pamatfunkcionalitāte.*

4. attēls

Tāda produkta ar digitāliem elementiem pamatfunkcionalitātes ilustrācija, kas būtiski neatbilst nozīmīgu vai kritiski svarīgu produktu kategorijas definīcijai

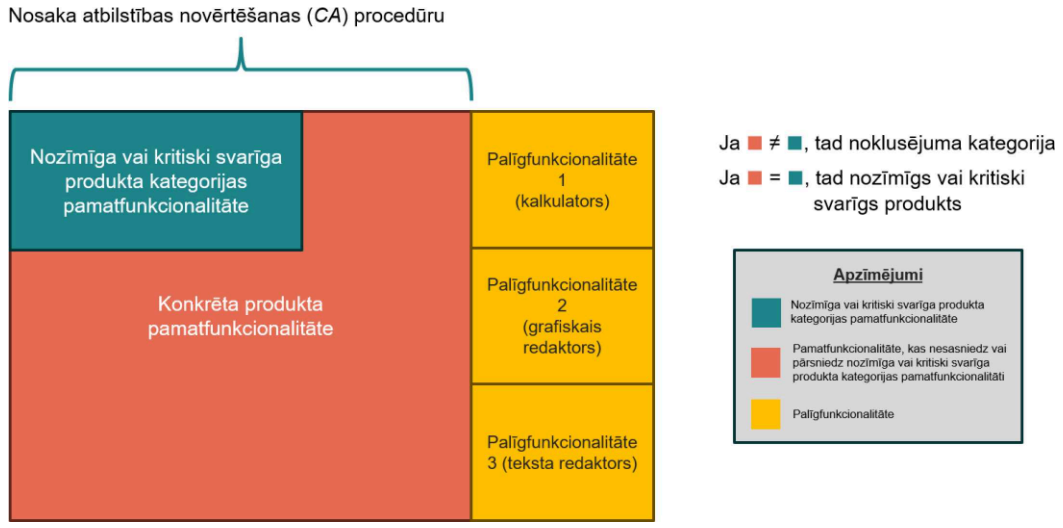


143. Ražotājs nedrīkst sagrozīt sava produkta ar digitāliem elementiem pamatfunkcionalitāti, lai izvairītos no atbilstības novērtēšanas režīma, kas piemērojams nozīmīgiem vai kritiski svarīgiem produktiem ar digitāliem elementiem, piemēram, pārmērīgi uzsverot vai mazinot noteiktu funkcionalitāšu nozīmi tā, ka produkts šķietami būtiski pārsniedz vai nesasniedz konkrēto pamatfunkcionalitāti. Tas attiecas, piemēram, uz gadījumiem, kad pastāv acīmredzamas neatbilstības starp reklāmas materiāliem, lietošanas pamācībām un tehnisko dokumentāciju.

144. Lai noteiktu piemērojamo atbilstības novērtēšanas režīmu, produktam ar digitāliem elementiem nevar būt vairāk par vienu pamatfunkcionalitāti. Saskaņā ar KNA VII pielikumu ražotājiem produkta tehniskajā dokumentācijā ir jāapraksta sava produkta ar digitāliem elementiem paredzētais nolūks un atbilstības novērtēšanas procedūra, ko tie ievērojuši. Tāpēc produkta pamatfunkcionalitāte būtu skaidri jāidentificē. Tas ļauj pareizi identificēt piemērojamo atbilstības novērtēšanas režīmu un ļauj tirgus uzraudzības iestādēm uzraudzīt un pārbaudīt, vai regula tiek piemērota pareizi.

5. attēls

Ilustrācija, kurā attēlots tas, kā konkrēta produkta ar digitāliem elementiem pamatfunkcionalitāte nosaka produkta klasi un līdz ar to piemērojamo atbilstības novērtēšanas procedūru



145. Daži produkti ar digitāliem elementiem tiek laisti tirgū kā atsevišķi produkti ar digitāliem elementiem, bet tos veido atsevišķi moduļi ar atsevišķām funkcijām. Ja ražotājs minētos moduļus dara pieejamus tirgū arī atsevišķi, piemēram, ja tos piedāvā atsevišķai iegādei, licencēšanai vai abonēšanai, minētie moduļi paši par sevi ir atsevišķi produkti ar digitāliem elementiem. Tādējādi tie ir jāklasificē, pamatojoties uz to attiecīgajām pamatfunkcionalitātēm (un tādējādi uz tiem attiecas atbilstošs atbilstības novērtēšanas režīms, pamatojoties uz katra moduļa pamatfunkcionalitāti). Tas neskar moduļus, ko piegādā tikai kā integrēta produkta ar digitāliem elementiem komponentus un nedara pieejamus atsevišķi; šādos gadījumos pamatfunkcionalitāti nosaka integrētā produkta ar digitāliem elementiem līmenī.

61. piemērs: ražotājs laiž tirgū vienotu drošības komplektu, kurā apvienoti vairāki moduļi, tai skaitā SIEM, *ielaušanās atklāšanas sistēma un analītikas modulis. Ražotājs šos moduļus piedāvā arī atsevišķai abonēšanai. Šajā scenārijā katrs modulis ir atsevišķs produkts ar digitāliem elementiem, un to klasificē, pamatojoties uz tā pamatfunkcionalitāti. Uz* SIEM *moduli attiecas nozīmīgu I klases produktu ar digitāliem elementiem atbilstības novērtēšanas režīms, jo tā pamatfunkcionalitāte ir "drošības informācijas un notikumu pārvaldības (*SIEM*) sistēmas". Uz ielaušanās atklāšanas sistēmu attiecas nozīmīgu II klases produktu ar digitāliem elementiem atbilstības novērtēšanas režīms, jo tās pamatfunkcionalitāte ir "ugunsmūri, ielaušanās atklāšanas un novēršanas sistēmas". Uz analītikas moduli attiecas "noklusējuma" produktu ar digitāliem elementiem atbilstības novērtēšanas režīms, jo tā pamatfunkcionalitāte nav nevienas nozīmīgu vai kritiski svarīgu produktu kategorijas pamatfunkcionalitāte.*

146. Par KNA 32. pantā noteikto pienākumu neizpildi var piemērot administratīvus naudas sodus saskaņā ar 64. panta 3. punktu.

6.2. Nozīmīgu un kritiski svarīgu produktu ar digitāliem elementiem atbilstības novērtēšana

147. Kad ražotājs ir noteicis sava produkta ar digitāliem elementiem pamatfunkcionalitāti, tam ir jāveic viena no piemērojamajām atbilstības novērtēšanas procedūrām. Ražotājam ir jānodrošina, ka produkts ar digitāliem elementiem kopumā atbilst pamatprasībām, attiecīgā gadījumā ņemot vērā tajā integrēto komponentu vai funkciju drošību.

148. Stingrāka atbilstības novērtēšanas procedūra ar trešās personas iesaisti (pamatojoties uz B+C moduli, H moduli vai kiberdrošības sertifikācijas shēmām) ir obligāta nozīmīgiem II klases produktiem ar digitāliem elementiem (izņemot tos, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra saskaņā ar 32. panta 5. punktu) un kritiski svarīgiem produktiem ar digitāliem elementiem ([24]). Turpretī nozīmīgiem I klases produktiem ar digitāliem elementiem (izņemot tos, kas kvalificējami kā brīvi pieejama atvērtā pirmkoda programmatūra saskaņā ar 32. panta 5. punktu) trešās personas atbilstības novērtēšanas procedūra jāveic tikai tad, ja ražotājs nav piemērojis vai tikai daļēji piemērojis attiecīgos saskaņotos standartus, uz kuriem atsauces ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī* (turpmāk – "saskaņotie standarti"), kopīgās specifikācijas vai Eiropas kiberdrošības sertifikācijas shēmas ar vismaz "būtisku" apliecinājuma līmeni ([25]).

149. Tāpēc, lai nozīmīgam I klases produktam ar digitāliem elementiem varētu piemērot iekšējās kontroles procedūru, i) jāpiemēro visas piemērojamās attiecīgā saskaņotā standarta prasības un ii) standarta darbības jomai jāaptver vismaz visi kiberdrošības riski, kas saistīti ar minētā produkta pamatfunkcionalitāti.

150. Produkta ar digitāliem elementiem tvērums var būt plašāks nekā attiecīgajā saskaņotajā standartā paredzētais tvērums, un šādas papildu funkcijas var radīt atšķirīgus vai papildu kiberdrošības riskus. Ražotājam vienmēr ir jāveic riska novērtējums saskaņā ar 13. panta 2. punktu un attiecīgi jāpārbauda, vai saskaņota standarta piemērošana aptver visus riskus, kas saistīti ar produktu ar digitāliem elementiem. Ja standarta piemērošana neaptver visus riskus, ražotājam ar citiem līdzekļiem būtu jānodrošina, ka tā produkts ar digitāliem elementiem atbilst pamatprasībām.

151. Tāpēc, ja nozīmīga I klases produkta ar digitāliem elementiem ražotājs ir piemērojis attiecīgu saskaņoto standartu, kas aptver riskus, kuri saistīti ar minētā produkta pamatfunkcionalitāti, tas var izvēlēties izmantot iekšējās kontroles procedūru, lai pierādītu sava produkta atbilstību. Atbilstības novērtēšanas darbību ietvaros ražotājam joprojām būs jāpierāda, ka ir risināti visi riski, kas attiecas uz tā produktu ar digitāliem elementiem. Tādējādi, ja pastāv atšķirība starp saskaņotā standarta aptvērumu un produkta ar digitāliem elementiem tvērumu kopumā, ražotājam joprojām ir jādokumentē, kādus papildu pasākumus tas ieviesis minēto risku risināšanai.

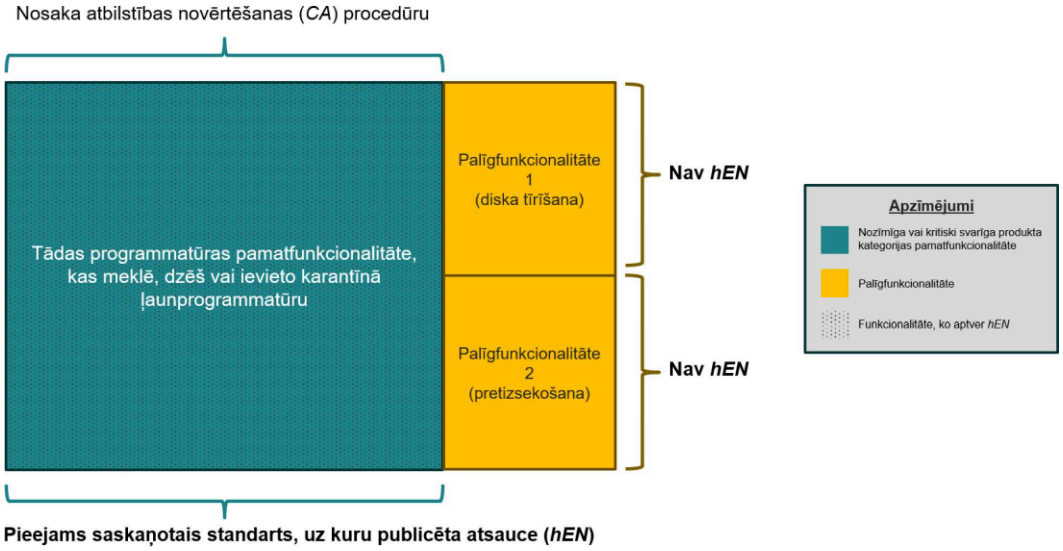
62. piemērs: pretvīrusu programmatūrai ir tādas programmatūras pamatfunkcionalitāte, kas meklē, dzēš vai ievieto karantīnā ļaunprogrammatūru, kā aprakstīts Īstenošanas regulas (ES) 2025/2392 I pielikuma 4. punktā. Šim produktam ar digitāliem elementiem ir arī papildu funkcijas, proti, diska tīrīšanas funkcija un pretizsekošanas funkcija, kas aizsargā lietotāju, kad tas pārlūko tīmekli. Ražotājs veic riska novērtējumu, kas aptver produktu ar digitāliem elementiem kopumā, tostarp pretvīrusu programmatūras pamatfunkcionalitāti, diska tīrīšanas funkciju un pretizsekošanas funkciju. Tas piemēro saskaņotu standartu, kas aptver riskus, kuri saistīti ar pretvīrusu pamatfunkcionalitāti, un papildu pasākumus, lai risinātu riskus, kas izriet no papildu funkcijām. Ražotājam ir atļauts atbilstības novērtēšanai izmantot iekšējās kontroles procedūru, kas aptver produktu ar digitāliem elementiem kopumā, tostarp diska tīrīšanas un pretizsekošanas funkcijas.

([24]) Tas attiecas arī uz gadījumiem, kad tiek izmantota Eiropas kiberdrošības sertifikācijas shēma, kuras apliecinājuma līmenis ir vismaz "būtisks", jo ir jāiesaista trešās personas sertifikācijas struktūra.

([25]) Īsuma labad pārējā šīs iedaļas daļa attiecas tikai uz saskaņotajiem standartiem, uz kuriem atsauces ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*. Tomēr tie paši norādījumi attiecas arī uz kopīgajām specifikācijām, kas pieņemtas saskaņā ar 27. panta 2. punktu, un uz Eiropas kiberdrošības sertifikācijas shēmām, ja Komisija tās noteikusi ar deleģētajiem aktiem saskaņā ar 27. panta 9. punktu.

6. attēls

Ilustrācija, kurā attēlots tas, kā tāda saskaņotā standarta izmantošana, uz kuru publicēta atsauce un kurš aptver tikai pamatfunkcionalitāti, nosaka piemērojamo atbilstības novērtēšanas procedūru



152. Tas attiecas arī uz gadījumiem, kad produktā ar digitāliem elementiem ir integrēta papildu funkcija, kas pati par sevi ir cita nozīmīga vai kritiski svarīga produkta ar digitāliem elementiem funkcija. Faktiski tas, vai produkts ar digitāliem elementiem ietilpst nozīmīgu vai kritiski svarīgu produktu kategorijā (un līdz ar to – kurš atbilstības novērtēšanas režīms ir piemērojams), ir atkarīgs no produkta ar digitāliem elementiem pamatfunkcionalitātes kopumā, nevis no integrēto komponentu funkcionalitātes atsevišķi. Piemēram, ja produktam ar digitāliem elementiem ir nozīmīga I klases produkta ar digitāliem elementiem pamatfunkcionalitāte, produktam kopumā piemēro nozīmīgiem I klases produktiem ar digitāliem elementiem piemērojamo atbilstības novērtēšanas režīmu, pat ja tajā ir integrēts komponents, kas pats par sevi ir kritiski svarīgs produkts ar digitāliem elementiem. Šādos gadījumos, ja ražotājs piemēro saskaņoto standartu, kas aptver ar minētā produkta pamatfunkcionalitāti saistītos riskus, ražotājam ir atļauts izmantot iekšējās kontroles procedūru.

63. piemērs: aparatūras produktam ar digitāliem elementiem ir maršrutētāja pamatfunkcionalitāte, kā aprakstīts Īstenošanas regulas (ES) 2025/2392 I pielikuma 12. punktā. Minētajam produktam ar digitāliem elementiem ir arī papildu funkcijas, tai skaitā ugunsmūra funkcionalitāte, jo tajā ir integrēts ugunsmūra komponents. Ražotājs veic riska novērtējumu, kas aptver produktu ar digitāliem elementiem kopumā, tostarp maršrutētāja pamatfunkcionalitāti un ugunsmūra funkcionalitāti. Tas piemēro saskaņotu standartu, kas aptver riskus, kuri saistīti ar maršrutētāja pamatfunkcionalitāti, un papildu pasākumus, lai risinātu riskus, kas izriet no papildu funkcijām. Piemēram, ražotājs var piemērot saskaņoto standartu ugunsmūriem, lai aptvertu riskus, kas saistīti ar ugunsmūra funkcionalitāti. Ražotājam ir atļauts atbilstības novērtēšanai izmantot iekšējās kontroles procedūru, kas aptver produktu ar digitāliem elementiem kopumā, tostarp ugunsmūra funkcionalitāti.

6.3. Ietekme uz pieņēmumu par atbilstību

153. KNA 27. panta 1. punktā ir noteikts, ka produktus ar digitāliem elementiem un ražotāja ieviestos procesus, kas atbilst tiem saskaņotajiem standartiem vai to daļām, uz kuriem atsauces ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, uzskata par atbilstošiem I pielikumā izklāstītajām KNA pamatprasībām, uz kurām attiecas minētie

standarti vai to daļas ([26]). Ar 27. panta 5. punktu tas pats pieņēmums par atbilstību tiek attiecināts arī uz produktiem ar digitāliem elementiem un ražotāja ieviestiem procesiem, kas atbilst kopīgajām specifikācijām, kuras Komisija pieņēmusi ar īstenošanas aktiem, un 27. panta 8. punktā ir noteikts pieņēmums par atbilstību attiecībā uz produktiem ar digitāliem elementiem un ražotāja ieviestiem procesiem, par kuriem ir izdots ES atbilstības apliecinājums vai sertifikāts saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu, kas pieņemta, ievērojot Regulu (ES) 2019/881, ja tas ir precizēts ar deleģētajiem aktiem saskaņā ar 27. panta 9. punktu ([27]).

154. Tāpēc, ja ražotājs ir piemērojis saskaņoto standartu, uz kuru atsauces ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, uz ražotāju attiecas pieņēmums par atbilstību attiecībā uz riskiem, ko aptver minētais standarts. Tas varētu attiekties, piemēram, uz gadījumiem, kad saskaņotais standarts, uz kuru ir publicēta atsauce, aptver visus riskus, kas saistīti ar produkta ar digitāliem elementiem pamatfunkcionalitāti, un nav papildu funkciju, kas rada kiberdrošības riskus. Piemēram, paredzams, ka saskaņotais maršrutētāju standarts aptvers vismaz riskus, kas saistīti ar šo produktu ar digitāliem elementiem pamatfunkcionalitāti. Ja šādam produktam nav nekādu papildu funkciju vai ja šīs papildu funkcijas nerada riskus, kas nav risināti ar standartu, uz produktu ar digitāliem elementiem var attiecināt pieņēmumu par atbilstību.

155. Gadījumos, kas aplūkoti 151. un 152. punktā, ražotājam ir atļauts izmantot iekšējās kontroles procedūru, jo saskaņotais standarts aptver riskus, kas saistīti ar produkta ar digitāliem elementiem pamatfunkcionalitāti. Tomēr minēto produktu ar digitāliem elementiem tvērums var būt plašāks par saskaņoto standartu tvērumu, un papildu funkcijas var radīt kiberdrošības riskus, uz kuriem šāds saskaņotais standarts neattiecas. Tāpēc uz minētajiem produktiem ar digitāliem elementiem var neattiekties pieņēmums par atbilstību attiecībā uz minētajām papildu funkcijām.

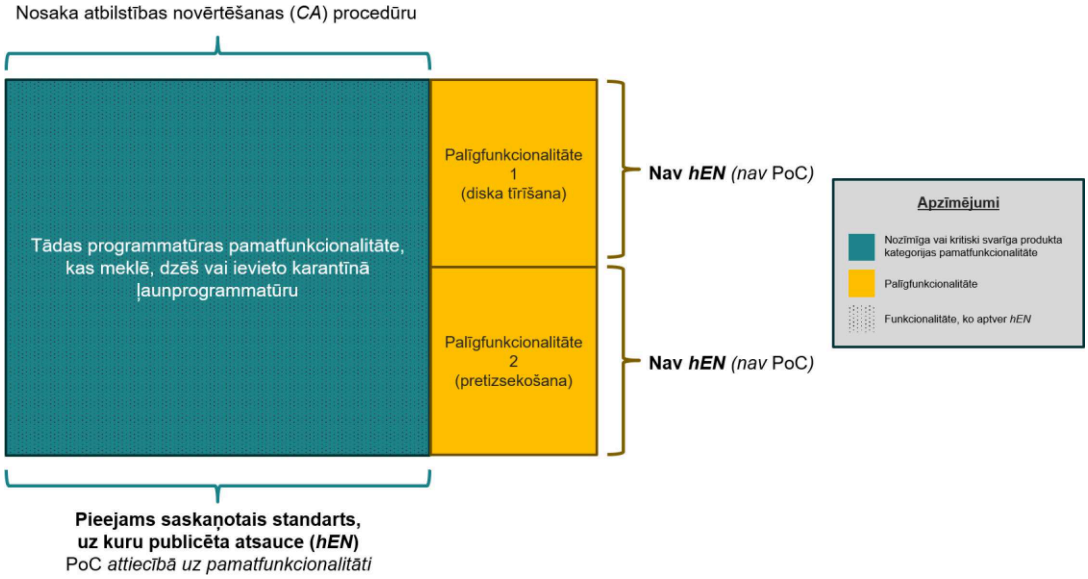
64. piemērs: pretvīrusu programmatūrai ir tādas programmatūras pamatfunkcionalitāte, kas meklē, dzēš vai ievieto karantīnā ļaunprogrammatūru, un ar šo pamatfunkcionalitāti saistītos riskus aptver saskaņotais standarts. Minētajam produktam ar digitāliem elementiem ir arī papildu funkcionalitātes, proti, diska tīrīšanas funkcija un pretizsekošanas funkcionalitāte, kas aizsargā lietotāju, pārlūkojot tīmekli; ar šīm funkcionalitātēm saistītos riskus saskaņotais standarts neaptver. Ja piemēro saskaņoto standartu, ražotājam atbilstības novērtēšanai ir atļauts izmantot iekšējās kontroles procedūru. Uz to attieksies pieņēmums par atbilstību attiecībā uz riskiem, kas saistīti ar minētā produkta pamatfunkcionalitāti, bet ne attiecībā uz riskiem, kas saistīti ar papildu funkcijām.

([26]) Kā skaidri norādīts zilās rokasgrāmatas 4.1.2.2. iedaļā, "[a]tbilstīgi saskaņošanas tiesību aktiem par riskiem (..) ražotāji vienmēr, arī izmantojot saskaņotos standartus, uz kuriem atsauces publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, ir pilnībā atbildīgi par visu ar produktu saistīto risku novērtēšanu, lai noteiktu, kuras pamatprasības (vai citas prasības) ir piemērojamas. Pēc minētā riska novērtēšanas ražotājs var izvēlēties piemērot saskaņotajos standartos, uz kuriem atsauces ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*, noteiktās tehniskās specifikācijas, lai īstenotu saskaņotajos standartos norādītos "riska samazināšanas pasākumus"".

([27]) Kā minēts iepriekš, īsuma labad pārējā šīs iedaļas daļa attiecas tikai uz saskaņotajiem standartiem, uz kuriem atsauces ir publicētas *Eiropas Savienības Oficiālajā Vēstnesī*. Tomēr tie paši norādījumi attiecas arī uz kopīgajām specifikācijām un Eiropas kiberdrošības sertifikācijas shēmām.

7. attēls

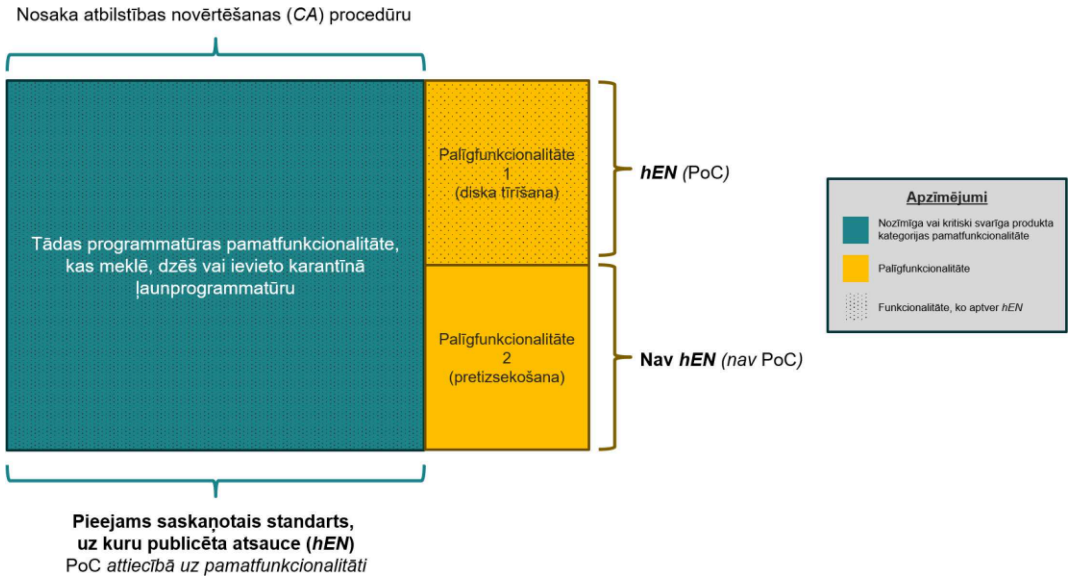
Saskaņotais standarts nodrošina pieņēmumu par atbilstību (PoC) attiecībā uz pamatfunkcionalitāti, jo tas aptver visus ar šo pamatfunkcionalitāti saistītos riskus, bet ne attiecībā uz palīgfunkcionalitātēm



65. piemērs: tajā pašā scenārijā kā iepriekšējā piemērā saskaņotais standarts tagad ir atjaunināts, lai aptvertu arī riskus, kas saistīti ar vienu no papildu funkcionalitātēm, proti, diska tīrīšanas funkciju, bet ne otru (t. i., pretizsekošanas funkcionalitāti). Ja piemēro saskaņoto standartu, ražotājam atbilstības novērtēšanai ir atļauts izmantot iekšējās kontroles procedūru. Uz to attieksies pieņēmums par atbilstību attiecībā uz riskiem, kas saistīti ar minētā produkta pamatfunkcionalitāti un diska tīrīšanas funkcionalitāti, bet ne attiecībā uz riskiem, kas saistīti ar pretizsekošanas funkcionalitāti.

8. attēls

Saskaņotais standarts nodrošina PoC attiecībā uz pamatfunkcionalitāti un 1. palīgfunkcionalitāti, jo tas aptver visus ar šīm divām funkcionalitātēm saistītos riskus, bet ne attiecībā uz 2. palīgfunkcionalitāti



7. **KIBERDROŠĪBAS RISKA NOVĒRTĒJUMS UN PRODUKTU AR DIGITĀLIEM ELEMENTIEM UN KOMPONENTU INTEGRĀCIJA**

7.1. **Par kiberdrošības risku izvērtēšanu un risināšanu**

156. KNA 13. panta 2. punktā paredzētajā kiberdrošības risku novērtējumā ir noteikts, ka ražotājiem ir jāapzina attiecīgie riski un jānovērtē to iespējamā ietekme uz produktu ar digitāliem elementiem. Ražotājiem arī jāīsteno atbilstoši pasākumi šo risku risināšanai saskaņā ar I pielikuma pamatprasībām.

157. Organizācijas riska pārvaldībā riskus parasti novērtē pēc pieņemamības kritērijiem, kas izriet no organizācijas iekšējiem mērķiem vai vēlmes uzņemties risku. Savukārt saskaņā ar KNA atlikušais kiberdrošības risks būtu jānovērtē, ņemot vērā prasību, ka tirgū laistais produkts ar digitāliem elementiem nodrošina atbilstošu kiberdrošības līmeni, pamatojoties uz riskiem, ņemot vērā tā paredzēto nolūku un pamatoti paredzamo lietojumu.

158. Tādējādi, nosakot, vai riski ir risināti, ražotāja iekšējai riska pielaidei, tirdzniecības stratēģijai vai vienkārši izmaksu apsvērumiem nav nozīmes. Šīs regulas 13. panta 2. un 3. punkta vajadzībām ražotājiem ir jāspēj noteikt, vai identificētie kiberdrošības riski ir pietiekami risināti, īstenojot I pielikuma I daļas pamatprasības, ņemot vērā paredzēto nolūku, pamatoti paredzamo lietojumu un lietošanas nosacījumus, tai skaitā attiecīgā gadījumā darbības vidi (piemēram, produkta ar digitāliem elementiem paredzētos lietotājus) un aizsargājamos aktīvus, ņemot vērā paredzamo produkta ar digitāliem elementiem lietošanas ilgumu.

159. Atlikušais kiberdrošības risks ir riska novērtēšanas un riska risināšanas neatņemams rezultāts. Ir atzīts, ka kiberdrošības riskus praksē nevar pilnībā novērst. Tomēr atlikušā riska esība nenozīmē, ka jebkādu risku var pieņemt pēc ražotāja ieskatiem. Produktu ar digitāliem elementiem var laist tirgū tikai tad, ja atlikušie riski pēc tam, kad ir veikti atbilstoši pasākumi, ir pietiekami risināti, īstenojot pamatprasības, ņemot vērā produkta ar digitāliem elementiem paredzēto nolūku un pamatoti paredzamo lietojumu.

160. Saskaņā ar 13. panta 3. punktu, ja tiek konstatēti kiberdrošības riski, ražotājiem tie ir jārisina, veicot atbilstīgus pasākumus, tostarp produkta līmenī. Atkarībā no apstākļiem tas var ietvert, piemēram, uzbrukuma laukuma samazināšanu, tehnisko aizsardzības pasākumu īstenošanu, funkcionalitātes ierobežošanu vai pielāgošanu vai produkta ar digitāliem elementiem paredzētā nolūka precīzāku definēšanu. Ražotāji var arī veikt pasākumus, lai veidotu pamatoti paredzamu produkta ar digitāliem elementiem lietojumu, piemēram, izmantojot riska komunikāciju, norādījumus lietotājam vai lietotāja saskarnes dizainu, lai sekmētu lietotāju uzvedības virzīšanu uz drošiem lietošanas paradumiem.

161. KNA neparedz kiberdrošības riska vai atbildības nodošanu lietotājiem vai trešām personām, lai kompensētu produkta projektējuma trūkumus vai pamatotu kiberdrošības risku nerisināšanu. Pienākums laist tirgū drošu produktu ar digitāliem elementiem un pierādīt atbilstību pamatprasībām paliek ražotājam.

162. Lietotājiem sniegto informāciju un norādījumus var izmantot, lai atbalstītu produkta ar digitāliem elementiem drošu ieviešanu un darbību, tostarp, ja ražotājs ir izvēlējies ierobežot minētā produkta paredzēto nolūku, attiecinot to tikai uz uzticamām vidēm, un lai informētu lietotājus par atlikušajiem riskiem veidā, kas ir piemērots produkta ar digitāliem elementiem raksturam un tā paredzētajiem lietotājiem.

66. piemērs: ražotājs izstrādā rūpniecisku sensoru izmantošanai uzticamā vidē. Lai sensors pareizi darbotos, ražotājs nēsteno pasākumus aizsardzībai pret fiziskiem uzbrukumiem pašam sensoram. Lai mazinātu riska novērtējumā identificētos saistītos riskus, ražotājs ierobežo sensora paredzēto nolūku, proti, to izmantot tikai uzticamās vidēs, kurās tiek novērsta neatļauta fiziska piekļuve produktam ar digitāliem elementiem. Informācija un instrukcijas lietotājiem sniedz skaidru informāciju par šiem sensora izmantošanas ierobežojumiem tādā veidā, kas atbilst produkta ar digitāliem elementiem būtībai un tā paredzētajiem lietotājiem.

67. piemērs: ražotājs izstrādā lietojumprogrammu profesionālai lietošanai pārvaldītos galddatoros un mobilajās ierīcēs. Lietojumprogramma apstrādā lokāli glabātus sensitīvus datus un lietotāju radītu saturu. Riska novērtēšanas laikā ražotājs identificē neatļautas piekļuves risku šādiem datiem, ja tie ierīcē tiek glabāti nešifrētā veidā. Tā vietā, lai pašā lietotnē projektētu un ieviestu savu šifrēšanas mehānismu, ražotājs izvēlas izmantot tās operētājsistēmas iebūvētās šifrēšanas un atslēgu pārvaldības funkcijas, kurā paredzēts izmantot lietotni, jo operētājsistēmā iebūvētie kriptogrāfijas pakalpojumi ir pietiekami attīstīti un tiek regulāri uzturēti.

163. Ja kiberdrošības risku novērtējumā ir identificēti riski, kurus nevar pienācīgi risināt ar atbilstošiem pasākumiem, lai nodrošinātu atbilstību KNA, var būt vajadzīgas izmaiņas produkta ar digitāliem elementiem projektējumā, funkcionalitātē vai paredzētajā nolūkā. Apsvērumi, kas saistīti tikai ar izmaksām vai komerciālo īstenojamību, nav pietiekams pamats, lai šādus riskus atstātu nerisinātus, ja tādējādi produkts ar digitāliem elementiem neatbilstu pamatprasībām.

7.2. **Produktus ar digitāliem elementiem projektē, izstrādā un ražo tā, lai tie nodrošinātu atbilstošu kiberdrošības līmeni, pamatojoties uz riskiem.**

164. KNA I pielikuma I daļas 1. punktā minētā kiberdrošības pamatprasība paredz, ka produktus ar digitāliem elementiem projektē, izstrādā un ražo tā, lai tie nodrošinātu atbilstošu kiberdrošības līmeni, pamatojoties uz riskiem.

165. Šīs pamatprasības mērķis ir risināt visus kiberdrošības riskus, kas identificēti kiberdrošības risku novērtējumā. Konkrētāk, tas ietver kiberdrošības riskus, kas citādi nav pienācīgi risināti, īstenojot I pielikuma I daļas pamatprasības, izņemot 1. punktu. Šī pamatprasība atšķiras no juridiskā pienākuma veikt kiberdrošības risku novērtējumu, kas jāveic saskaņā ar 13. panta 2. punktu.

166. Ja visi attiecīgie kiberdrošības riski, kas saistīti ar produktu ar digitāliem elementiem, tiek risināti, īstenojot atbilstīgus pasākumus, lai izpildītu piemērojamās pamatprasības, kas nav 1. punkts, I pielikuma I daļas 1. punktā minēto pamatprasību uzskata par izpildītu. Savukārt, ja kiberdrošības riska novērtējumā ir konstatēti papildu riski, kas ar šādiem pasākumiem nav pilnībā risināti, ražotājiem attiecībā uz produktu ar digitāliem elementiem ir jāīsteno atbilstoši pasākumi minēto risku risināšanai, lai nodrošinātu atbilstību I pielikuma I daļas 1. punktā minētajai pamatprasībai. Praksē paredzams, ka vairumā gadījumu atbilstība pārējām pamatprasībām nodrošinās atbilstību šai prasībai.

7.3. **Riska novērtējums un pienācīga pārbaude attiecībā uz ārējām atkarībām un integrētiem komponentiem**

167. KNA ražotājiem ir noteikti divi atšķirīgi, bet savstarpēji papildinoši pienākumi saistībā ar kiberdrošības riska pārvaldību. Pirmkārt, 13. panta 2. punktā ir noteikts, ka ražotājiem ir jāveic paša produkta ar digitāliem elementiem kiberdrošības riska novērtējums. Otrkārt, 13. panta 5. punktā ir noteikts pienākums veikt pienācīgu pārbaudi attiecībā uz integrētajiem komponentiem. Kopā šie divi pienākumi ir paredzēti, lai nodrošinātu, ka produkts ar digitāliem elementiem joprojām ir drošs, arī tad, ja tas ir atkarīgs no attālinātas datu apstrādes risinājumiem, attālinātiem pakalpojumiem vai trešo personu programmatūras vai aparatūras komponentiem.

168. Kiberdrošības risku novērtējums attiecas uz to attiecīgo risku identificēšanu un pārvaldību, kas var ietekmēt produktu ar digitāliem elementiem, tostarp riskiem, kuru izcelsme ir ārpus paša produkta, piemēram, ārējiem tīkliem, vides faktoriem vai citiem ārējiem aspektiem, kas var ietekmēt produktu ar digitāliem elementiem vai uz kuriem produkts balstās. Attiecībā uz šādiem ārējiem riskiem KNA nepieprasa ražotājiem kontrolēt vai pārvaldīt ārējo vidi. Ražotājiem drīzāk ir jāidentificē šādi riski un tie jāmazina, projektējot un izstrādājot pašu produktu ar digitāliem elementiem. Tas ietvers I pielikuma I daļā noteikto attiecīgo pamatprasību īstenošanu un vajadzības gadījumā informācijas un norādījumu sniegšanu lietotājiem par integrācijas vai ieviešanas riskiem.

169. Piemēram, ražotājs var identificēt risku, ka nepilnvarotas personas produkta darbības laikā var piekļūt aizmugursistēmām, kas nav daļa no paša produkta ar digitāliem elementiem, un mēģināt nosūtīt ļaunprātīgas komandas produktam ar digitāliem elementiem. Šādas aizmugursistēmas, ja tās nav projektējis un izstrādājis ražotājs vai tas nav darīts ražotāja atbildībā vai ja tās neatbalsta kādu no produkta ar digitāliem elementiem funkcijām, nav attālinātas datu apstrādes risinājumi un tāpēc neietilpst produkta ar digitāliem elementiem darbības jomā KNA vajadzībām. Tomēr KNA pieprasa ražotājam risināt risku, ko tie var radīt, izmantojot produkta līmeņa pasākumus, piemēram, pieprasot attālinātu komandu kriptogrāfisku autentifikāciju, verificējot konfigurācijas izmaiņu integritāti vai ģenerējot ar drošību saistītus žurnālus vai brīdinājumus, ja tiek konstatēta neparasta uzvedība. Tāpat, ja ražotājs konstatē risku, kas izriet no tā, ka šāds ārējs pakalpojums kļūst nepieejams, piemēram, elektroapgādes pārtraukumu vai infrastruktūras atteices dēļ, KNA var prasīt produkta līmeņa pasākumus šādu kiberdrošības risku mazināšanai, piemēram, nodrošinot, ka pārtraukums neizraisa produkta ar digitāliem elementiem nonākšanu nedrošā stāvoklī. Šādos gadījumos KNA reglamentē to, kā produkts ar digitāliem elementiem reaģē uz minētajiem ārējiem riskiem; tajā nav noteikti pienākumi attiecībā uz to, kā aizmugursistēmas infrastruktūra tiek organizēta, nodrošināta ar personālu vai ekspluatēta, kā arī šī infrastruktūra netiek uzskatīta par daļu no produkta ar digitāliem elementiem.

170. Pienācīga pārbaude attiecas uz elementiem, kas ir daļa no paša produkta ar digitāliem elementiem, it īpaši trešās personas nodrošinātiem integrētiem programmatūras vai aparatūras komponentiem. Ražotājiem ir jāveic atbilstoši pasākumi, lai nodrošinātu, ka šādi komponenti neapdraud produkta ar digitāliem elementiem atbilstību pamatprasībām. To var panākt, tikai nosakot, kas produktam ar digitāliem elementiem ir nepieciešams no tā komponentiem, lai sasniegtu tā kiberdrošības mērķus, un uz risku balstītā veidā verificējot, vai minētie komponenti atbilst produkta vajadzībām, kā norādīts arī 34. apsvērumā.

171. Saskaņā ar savu kiberdrošības riska novērtējumu ražotājam ir jānosaka prasības, kurām integrētajam komponentam būtu jāatbilst. Piemēram, ja produkts ar digitāliem elementiem balstās uz komponenta nodrošinātām kriptogrāfijas funkcijām, atjaunināšanas mehānismiem vai drošiem sakariem, ražotājam, veicot pienācīgu pārbaudi, ir jāidentificē minētās vajadzības un jāverificē, vai komponents atbilst šīm vajadzībām. Šim nolūkam pierādījumi var būt dokumentācija, kas iegūta no komponenta ražotāja, piemēram, tehniskās specifikācijas, drošības dokumentācija vai attiecīgā atbilstības vai apliecinājuma dokumentācija. Attiecīgā gadījumā ražotājs var arī veikt testus, lai verificētu, ka minētie komponenti pienācīgi pilda attiecīgās funkcijas. Lai gan pienācīga pārbaude ir atsevišķs juridisks pienākums, tā atbalsta un stiprina ražotāja spēju pierādīt atbilstību pamatprasībām attiecībā uz produktu ar digitāliem elementiem kopumā.

172. Novērtējot riskus produktam ar digitāliem elementiem kopumā, kiberdrošības riska novērtējumā jāņem vērā ārpus produkta esoši elementi, piemēram, vides elementi, ārējā infrastruktūra, citas sistēmas vai tīkli, un attiecīgā gadījumā tie jārisina, izmantojot produkta līmeņa pasākumus, lai nodrošinātu produkta ar digitāliem elementiem atbilstību pamatprasībām. Riska novērtējumā ir jāņem vērā arī komponenti, kas ir fiziski vai loģiski integrēti produktā ar digitāliem elementiem, bet iegūti no trešās personas. Tomēr atbilstības nodrošināšanas nolūkā ražotājam tie būtu jāuzskata par ārēji piegādātiem komponentiem, kuru īpašības pēc integrēšanas tiek verificētas, veicot pienācīgu pārbaudi, jo ražotājs, iespējams, nav tos pārprojektējis vai izstrādājis no jauna.

173. Tāda pati loģika attiecas uz komponentu izstrādi un integrāciju. Ja ražotājs pats izstrādā funkcijas, tam tieši jāīsteno pamatprasības. Ja ražotājs integrē citu personu izstrādātus komponentus, tam, veicot pienācīgu pārbaudi, jānodrošina, ka šos komponentus var izmantot tā, lai produkts ar digitāliem elementiem kopumā varētu atbilst prasībām. Abos gadījumos mērķis paliek viens un tas pats: ka tirgū laistais produkts ar digitāliem elementiem nodrošina atbilstošu kiberdrošības līmeni, kā tas prasīts KNA, ņemot vērā kiberdrošības risku novērtējumā identificētos riskus.

7.4. **Riska novērtējumu un atbilstības dokumentācijas atkārtota izmantošana produktu ar digitāliem elementiem saimēm**

174. Ražotāji var laist tirgū produktus ar digitāliem elementiem, kas ir līdzīgi, piemēram, vienas un tās pašas produktu saimes dažādus variantus, modeļus vai konfigurācijas. Ja šādiem produktiem ar digitāliem elementiem ir viena un tā pati arhitektūra, ar drošību saistīts dizains un paredzētais nolūks un tie ir pakļauti vieniem un tiem pašiem kiberdrošības riskiem, KNA neprasa ražotājiem riska novērtēšanas un atbilstības novērtēšanas vajadzībām katru variantu uzskatīt par pilnīgi atsevišķu produktu ar digitāliem elementiem.

175. Šādos gadījumos, ja visi attiecīgie varianti ir pienācīgi aptverti attiecīgo risku un pamatprasību ziņā, ražotāji var paļauties uz: i) vienotu kiberdrošības riska novērtējumu, kas veikts saskaņā ar KNA 13. panta 2. punktu, ii) vienotu tehniskās dokumentācijas kopumu un iii) vienotu atbilstības novērtēšanas procedūru. Tas arī ļauj izdot vienotu ES atbilstības deklarāciju produktu ar digitāliem elementiem grupai, ja vien tajā ir skaidri identificēti produkta varianti, uz kuriem tā attiecas.

176. Izšķirošais faktors ir tas, vai atšķirības starp variantiem attiecas uz kiberdrošību. Variācijām, kas neietekmē produkta ar digitāliem elementiem kiberdrošības īpašības, piemēram, krāsas, formfaktora, atmiņas lieluma vai citu ar drošību nesaistītu īpašību atšķirībām, nav vajadzīgi atsevišķi riska novērtējumi vai atbilstības novērtējumi. Savukārt dažos gadījumos varianti var atšķirties veidos, kas ietekmē pamatprasību īstenošanu, piemēram, izmantojot dažādas sakaru saskarnes, programmatūras komplektus, atjaunināšanas mehānismus vai attālinātu savienojamību. Šādos gadījumos minētās atšķirības ir jāatspoguļo riska novērtējumā un vajadzības gadījumā atbilstības novērtējumā un tehniskajā dokumentācijā.

177. Ražotāji joprojām ir atbildīgi par to, lai riska novērtējums un saistītā dokumentācija precīzi atspoguļotu tirgū laistos produktus ar digitāliem elementiem. Ja jauns variants rada jaunus kiberdrošības riskus vai maina veidu, kādā tiek īstenotas pamatprasības, esošais riska novērtējums un atbilstības dokumentācija ir attiecīgi jāatjaunina. Vienu atbilstības novērtējumu var izmantot tikai tiktāl, ciktāl produktiem ar digitāliem elementiem nav atšķirību attiecībā uz to kiberdrošības īpašībām.

8. **ATTĀLINĀTA DATU APSTRĀDE**

178. KNA 3. panta 1. punktā produkts ar digitāliem elementiem ir definēts kā "programmatūras vai aparatūras produkts un tā attālinātās datu apstrādes risinājumi, ieskaitot programmatūras vai aparatūras komponentus, kas tiek laisti tirgū atsevišķi". Ņemot to vērā, ražotājam ir jāņem vērā produkts ar digitāliem elementiem kopumā, tostarp tā attālinātās datu apstrādes risinājumi (*RDPS*). Piemēram, pierādot, ka produkts ar digitāliem elementiem atbilst I pielikumā noteiktajām pamatprasībām, ir jāņem vērā *RDPS*, sākot ar riska novērtējumu (13. panta 2. punkts). Tas pats attiecas uz aprites cikla pienākumiem, piemēram, ziņošanu par aktīvi izmantotām ievainojamībām un nopietniem incidentiem (14. pants).

179. Šo norādījumu mērķis ir sniegt ražotājiem papildu atbalstu, lai noteiktu, vai to produkts ar digitāliem elementiem ietver *RDPS* KNA izpratnē un kā šajā sakarā izpildīt atbilstības nodrošināšanas pienākumus. Pēc KNA noteikto definīciju un apsvērumu sākotnējas analīzes šajos norādījumos ir izklāstīti jautājumi, kas palīdz ražotājiem noskaidrot, vai to produkts ar digitāliem elementiem ietver *RDPS* (sk. *8.1.* iedaļu *Ko uzskata par attālinātas datu apstrādes risinājumu produktam ar digitāliem elementiem?*). Pēc tam ir izklāstītas *RDPS* tehniskās sekas un tas, kā novērtēt atbilstību KNA (sk. *8.2.* iedaļu *Attālinātas datu apstrādes risinājumu praktiskās un tehniskās sekas un paļaušanās uz trešo personu risinājumiem*).

180. KNA 3. panta 2. punktā jēdziens "attālināta datu apstrāde" ir definēts kā "tāda datu apstrāde no attāluma, kurai programmatūras projektēšanu un izstrādi ir veicis vai par to ir bijis atbildīgs ražotājs un kuras neesamība liegtu izpildīt kādu no produkta ar digitāliem elementiem funkcijām". Tādējādi *RDPS* ir attālinātas datu apstrādes programmatūras elementi ("elektroniskās informācijas sistēmas daļa, kura sastāv no datora koda", kā definēts 3. panta 4. punktā). Produkta ar digitāliem elementiem tvērumā nav paredzēts iekļaut aparatūru, uz kuru var balstīties attālināta datu apstrāde.

181. 11. un 12. apsvērumā ir sniegti papildu skaidrojumi par to, kā šis jēdziens būtu jāinterpretē. 11. apsvērumā ir precizēts, ka attālinātas datu apstrādes risinājumu aptveršanas mērķis ir nodrošināt, ka "ražotāji šādus produktus pilnībā pienācīgi aizsargā neatkarīgi no tā, vai datus apstrādā vai glabā lokāli lietotāja ierīcē, vai arī ražotājs tos apstrādā vai glabā attālināti". Tajā arī noteikts, ka "prasības attiecībā uz attālinātas datu apstrādes risinājumiem, kas ietilpst šīs regulas darbības jomā, neietver tehniskus, operatīvus vai organizatoriskus pasākumus, kuru mērķis ir pārvaldīt ražotāja tīkla un informācijas sistēmu drošības riskus kopumā".

182. Tāpēc no 11. apsvēruma izriet, ka KNA prasību nolūks nav aptvert visu organizācijas IT infrastruktūru, bet tikai programmatūras komponentus, kas ļauj īstenot datu apstrādes risinājumu. Piemēram, iekšējās sistēmas, kas saistītas ar paša ražotāja cilvēkresursiem, algu uzskaiti, klientu attiecību pārvaldību, nepārtrauktas integrācijas / nepārtrauktas piegādes (*CI/CD*) kanāliem un drošības atjauninājumu izplatīšanu perifērdatošanas vietās, nebūtu jāuzskata par *RDPS*. Tāpat sistēmas, kas saistītas ar auditiem un testēšanas darbībām, piemēram, ielaušanās testēšanu, proaktīvu draudu apzināšanu un "sarkanās komandas" testēšanu, neietilpst KNA aptvertā produkta ar digitāliem elementiem tvērumā. Ir svarīgi norādīt, ka, lai gan efektīvu un regulāru produkta ar digitāliem elementiem drošības testu un pārskatu veikšana ir KNA I pielikuma II daļas 3. punktā noteikta pamatprasība, tas nenozīmē, ka šādas darbības ir uzskatāmas par produkta ar digitāliem elementiem *RDPS*.

183. 12. apsvērumā galvenā uzmanība pievērsta mākoņpakalpojumiem un sīkāk izklāstīti apstākļi, kādos mākoņpakalpojumus varētu uzskatīt par *RDPS*. Apsvēruma beigās ir atgādināts, ka mākoņdatošanas pakalpojumi un mākoņdatošanas pakalpojumu modeļi ietilpst Direktīvas (ES) 2022/2555 (TID 2) ([28]) darbības jomā, kurā noteiktas kiberdrošības risku pārvaldības prasības mākoņdatošanas pakalpojumu sniedzējiem. Minētās prasības ir sīkāk precizētas Komisijas Īstenošanas regulā (ES) 2024/2690 ([29]).

8.1. **Ko uzskata par attālinātas datu apstrādes risinājumu produktam ar digitāliem elementiem?**

184. Tādējādi 3. panta 2. punktā noteiktā attālinātas datu apstrādes definīcija balstās uz trim elementiem: i) vai datu apstrāde notiek "no attāluma", ii) vai šādas datu apstrādes neveikšana liegtu izpildīt kādu no produkta ar digitāliem elementiem funkcijām un iii) vai programmatūras projektēšanu un izstrādi ir veicis vai par to ir bijis atbildīgs ražotājs. Nākamajās trīs apakšiedaļās katrs no šiem elementiem ir aplūkots sīkāk.

([28]) Eiropas Parlamenta un Padomes Direktīva (ES) 2022/2555 (2022. gada 14. decembris), ar ko paredz pasākumus nolūkā panākt vienādi augstu kiberdrošības līmeni visā Savienībā un ar ko groza Regulu (ES) Nr. 910/2014 un Direktīvu (ES) 2018/1972 un atceļ Direktīvu (ES) 2016/1148 (TID 2 direktīva) (OV L 333, 27.12.2022., 80. lpp., ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Komisijas Īstenošanas regula (ES) 2024/2690 (2024. gada 17. oktobris), kas attiecībā uz DNS pakalpojumu sniedzējiem, TLD nosaukumu reģistriem, mākoņdatošanas pakalpojumu sniedzējiem, datu centru pakalpojumu sniedzējiem, satura piegādes tīkla nodrošinātājiem, pārvaldītu pakalpojumu sniedzējiem, pārvaldītu drošības pakalpojumu sniedzējiem, tiešsaistes tirdzniecības vietu, tiešsaistes meklētājprogrammu un sociālās tīklošanās pakalpojumu platformu nodrošinātājiem un uzticamības pakalpojumu sniedzējiem nosaka Direktīvas (ES) 2022/2555 piemērošanas noteikumus, kuri attiecas uz kiberdrošības risku pārvaldības pasākumu tehniskajām un metodiskajām prasībām un precizē, kādos gadījumos incidentu uzskata par būtisku (OV L, 2024/2690, 18.10.2024., ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *Jēdziens "no attāluma"*

185. Jēdziens "no attāluma", kas minēts 3. panta 2. punktā, ir būtisks, bet ar to nepietiek, lai noteiktu, vai produkts ar digitāliem elementiem ietver *RDPS*. Turklāt, ņemot vērā dažādos risinājumus, uz kuriem varētu attiekties šis jēdziens, nav iespējams sniegt izsmeļošu "no attāluma" definīciju. Ražotājam ir jāizvērtē katrs gadījums atsevišķi.

186. KNA 11. apsvērumā ir minēti dati, ko "ražotājs (..) apstrādā vai glabā attālināti", nevis dati, ko apstrādā vai glabā "lokāli lietotāja ierīcē". Attālināta datu apstrāde parasti notiek ārpus produkta ar digitāliem elementiem lietotāja vides vai organizācijas darbības vides (profesionālam lietotājam). Tomēr tas neliedz apstrādi veikt arī ierīces tuvumā ("perifērijā"). Datu pārraide var notikt pa vadiem (piemēram, ar *Ethernet* kabeli) vai bezvadu režīmā (piemēram, izmantojot *Wi-Fi* vai *Bluetooth*). Mākoņdatošana, tai skaitā perifērdatošana, ir tipisks piemērs datu apstrādei, kas notiek "no attāluma". Piemēram, mākoņdatošanas funkcijas gadījumā, kurai lietotājs piekļūst no mobilās lietotnes, daļa datu apstrādes notiek mākonī ārpus lietotāja vides.

187. Ir svarīgi norādīt, ka *RDPS* ne vienmēr tiek ekspluatēti trešo personu mākoņdatošanas infrastruktūrā. Attālināta datu apstrāde, kas notiek vietējos serveros ražotāja telpās, arī var būt *RDPS*. Citiem vārdiem sakot, lokāli un privātā mākonī lietots risinājums tikpat lielā mērā var būt kvalificējams kā *RDPS* kā publiskā mākonī un ārpus uzņēmuma telpām lietots risinājums.

188. Divi izšķirošie un kumulatīvie jautājumi, kas nosaka, vai KNA datu apstrādi aptver kā attālinātas datu apstrādes risinājumu, ir izklāstīti tālāk *8.1.2.* un *8.2.* iedaļā. Ja atbilde uz abiem jautājumiem ir apstiprinoša, attālinātā datu apstrāde ir uzskatāma par *RDPS*.

8.1.2. *Vai šādas datu apstrādes neesība liegtu produktam ar digitāliem elementiem veikt kādu no savām funkcijām?*

189. Kā noteikts 3. panta 2. punktā iekļautajā "attālinātas datu apstrādes" definīcijā, lai datu apstrādi no attāluma varētu kvalificēt kā *RDPS*, tās neesībai būtu jāliedz izpildīt kādu no produkta ar digitāliem elementiem funkcijām. Šajā definīcijā lietotais jēdziens "funkcijas" neaprobežojas ar produkta ar digitāliem elementiem "pamatfunkcionalitāti" vai "paredzēto nolūku", jo KNA šādu ierobežojumu neparedz. KNA darbības jomā ietilpstošās funkcijas ir gan funkcijas, kas tieši atbilst produkta ar digitāliem elementiem paredzētajam nolūkam, kā to pieredzējuši lietotāji, gan funkcijas, kas atbalsta produkta vispārējo sniegumu.

190. Tādu funkciju piemēri, kurās var notikt attālināta datu apstrāde un kuras liegtu produktam ar digitāliem elementiem veikt kādu no savām funkcijām, būtu šādi: i) komandu nosūtīšana uz ierīci, ii) datņu sinhronizēšana, iii) lietotāja pievienošana, iv) konfigurēšana (produkta ar digitāliem elementiem personalizācija), v) atjauninājumu automatizēta izplatīšana, tostarp funkciju atjaunināšana un drošības ielāpu uzstādīšana, vi) identitātes un piekļuves pārvaldība.

191. Dažos gadījumos lietotājs var izmantot funkciju gan attālināti, gan manuāli (piemēram, ieslēdzot spuldzi ar lietotni vai manuāli). Šāda iespēja neizslēdz datu apstrādes, kas saistīta ar funkcijas attālinātu izpildi, kvalificēšanu par *RDPS*. Šīs funkcijas veikšana attālināti arī tiek uzskatīta par daļu no funkcijām, ko piedāvā produkts ar digitāliem elementiem.

192. Savukārt, ja konkrētas datu apstrādes neesība neliedz produktam ar digitāliem elementiem veikt kādu no savām funkcijām, šāda apstrāde netiek uzskatīta par *RDPS* KNA nozīmē. Tas ietver, piemēram, tādu telemetrijas datu attālinātu analīzi, kas savākti tikai statistikas vajadzībām vai turpmākai produktu izstrādei.

193. Tomēr pat tad, ja datu apstrāde neatbalsta produkta ar digitāliem elementiem funkciju, ražotājiem, veicot kiberdrošības riska novērtējumu, var būt jāapsver, vai šie attālinātie komponenti rada riskus produktam ar digitāliem elementiem (piemēram, ņemot vērā produkta darbības vidi), un attiecīgi jāmazina šādi riski (piemēram, veicot produkta līmeņa riska mazināšanas pasākumus).

194. Tīmekļvietnes ir īpašs gadījums, kam vajadzīgs papildu skaidrojums, kā paskaidrots arī *2.1.* iedaļā *Laišana tirgū*. Tīmekļvietnes neietilpst *RDPS* tvērumā, ja tās neatbalsta produkta ar digitāliem elementiem funkciju, kā paskaidrots KNA 11. apsvērumā. Nepietiek ar to, ka tīmekļvietnē ir ietverta informācija par produktu ar digitāliem elementiem, lai to uzskatītu par *RDPS* darbības jomā ietilpstošu, pat ja produkts novirza uz šādu tīmekļvietni. Piemēram, lietotāju novirzīšana uz ārēju tīmekļvietni, kurā tiek sniegta informācija un norādījumi lietotājiem, nav *RDPS*. Savukārt tīmekļvietne var ietilpt *RDPS* tvērumā, ja tā iespējo vai atbalsta produkta ar digitāliem elementiem funkciju. Piemēram, autentifikācijas portāls, kas izsniedz akreditācijas datus vai pilnvaras, kuras nepieciešamas produkta ar digitāliem elementiem darbībai, tiktu uzskatīts par *RDPS* (ar nosacījumu, ka ir izpildīti arī pārējie definīcijas kritēriji).

8.1.3. *Vai programmatūru ir projektējis un izstrādājis ražotājs vai tas ir darīts ražotāja atbildībā?*

195. KNA 3. panta 2. punktā sniegtajā "attālinātas datu apstrādes" definīcijā ir sīkāk precizēts, ka šādas attālinātas datu apstrādes programmatūras projektēšana un izstrāde ir jāveic ražotājam vai par to jābūt atbildīgam ražotājam. Attālināta datu apstrāde, ko pilnībā projektējis un izstrādājis pats ražotājs, dabiski būtu kvalificējama kā *RDPS*. Tas tā būtu arī tad, ja ražotājs risinājuma projektēšanā un izstrādē izmanto ārēju pakalpojumu sniedzēju (t. i., risinājums tiek izstrādāts "ražotāja atbildībā"). Frāze "par ko ir bijis atbildīgs ražotājs" attiecas uz attālinātas apstrādes risinājumiem, kas ir īpaši pielāgoti ražotājam. Tie ir gadījumi, kad ražotājs ne tikai licencē esošu produktu ar digitāliem elementiem vai pakalpojumu, ko pakalpojumu sniedzējs piedāvā saviem klientiem, vai nedaudz pārveidotas tā versijas. Frāze "par ko ir bijis atbildīgs ražotājs" nozīmē, ka programmatūru izstrādā tikai ražotājs vai tā tiek izstrādāta ražotāja vārdā, pamatojoties uz ražotāja sniegtajiem projektiem un specifikācijām.

196. *RDPS* izpratnē jēdziens "kas pārvalda risinājumu" nav izšķirošs faktors, jo KNA definīcija attiecas tikai uz *RDPS* projektēšanu un izstrādi. Tas atbilst KNA pieejai, saskaņā ar kuru prasības un pienākumi attiecas uz ražotājiem, nevis uz produkta ar digitāliem elementiem darbību. Ja ražotāji projektē un izstrādā risinājumus, kurus pēc tam ekspluatē trešā persona, tie joprojām ir atbildīgi par to tirgū laistā produkta ar digitāliem elementiem atbilstību KNA kiberdrošības pamatprasībām.

197. Ir jānošķir gadījumi, kad projektēšanu un izstrādi veic ražotāji (vai par to atbild ražotāji), un gadījumi, kad tiek izmantoti trešo personu risinājumi, kurus ražotāji nav projektējuši un izstrādājuši (vai par kuriem tie nav atbildīgi). Piemēram, ir lietderīgi ņemt vērā visizplatītākos mākoņpakalpojumu modeļus, kas nodrošina dažādas lietotāju kontroles pakāpes un kas ir minēti arī KNA 12. apsvērumā, proti, programmatūru kā pakalpojumu (*SaaS*), platformu kā pakalpojumu (*PaaS*) un infrastruktūru kā pakalpojumu (*IaaS*).

198. Trešās personas *IaaS* risinājuma gadījumā ražotājs nepārvalda un nekontrolē pamatā esošos fiziskos un virtuālos resursus (piemēram, pamatā esošo aparatūru un mākoņpakalpojumu sniedzēja virtuālo mašīnu pārraugu), bet spēj ieviest un izmantot jebkuru programmatūru pēc savas izvēles, izmantojot šādus resursus, piemēram, operētājsistēmas un lietojumprogrammas. Šādu programmatūru ir projektējis un izstrādājis ražotājs vai par tās izstrādi ir atbildīgs ražotājs, un tāpēc to var kvalificēt kā *RDPS* (ja tā atbilst pārējiem definīcijas elementiem).

199. Trešās personas *PaaS* risinājuma gadījumā ražotājs ievieš savu (radīto vai iegādāto) lietojumprogrammu, izmantojot programmēšanas valodas un izpildes vidi, ko nodrošina mākoņpakalpojumu sniedzējs, un integrē lietojumprogrammu savā produktā ar digitāliem elementiem. Ražotājs kontrolē lietojumprogrammu un, iespējams, konfigurācijas iestatījumus izpildes videi. Tādējādi lietojumprogrammu ir projektējis un izstrādājis ražotājs vai tā ir projektēta un izstrādāta ražotāja atbildībā, un tāpēc tā var būt kvalificējama kā *RDPS* (ja ir izpildīti pārējie definīcijas elementi).

200. Trešās personas *SaaS* risinājuma gadījumā *SaaS* pakalpojumu sniedzējs piedāvā ražotājam pilnībā izstrādātu lietojumprogrammu, kas integrējama ražotāja produktā ar digitāliem elementiem. Ražotājam ir ierobežotas iespējas pārvaldīt lietotājam specifiskas lietojumprogrammas konfigurācijas iestatījumus. Tāpēc ražotājs nav projektējis un izstrādājis lietotni, un ražotājs par to nav atbildīgs.

201. Tomēr, ja daži elementi nav kvalificējami kā *RDPS* (piemēram, virtuālo mašīnu pārraugs trešās personas *IaaS* infrastruktūras gadījumā, operētājsistēma trešās personas *PaaS* risinājuma gadījumā vai trešās personas *SaaS* lietojumprogramma), bet ir integrēti produktā ar digitāliem elementiem tādā veidā, kas ietekmē tā drošību, šādi risinājumi būtu jāuzskata par līdzīgiem trešo personu komponentiem. Ražotājam ir jāidentificē un jānovērtē riski, kas saistīti ar minēto elementu integrēšanu, un tie jārisina, īstenojot pamatprasības pašam produktam ar digitāliem elementiem. Attiecīgā gadījumā to var atbalstīt ar drošības funkcijām, ko mākoņpakalpojumu sniedzējs darījis pieejamas, izmantojot savu dalītās atbildības modeli, ja ražotājs izmanto vai konfigurē minētās funkcijas, lai risinātu identificētos riskus. Turklāt tiek sagaidīts, ka ražotājs pildīs pienākumu, kas ir līdzīgs 13. panta 5. punktā minētajam pienākumam veikt pienācīgu pārbaudi saistībā ar šo komponentu drošību, tādā veidā, kas ir samērīgs ar risku, ko attālinātais risinājums rada produkta ar digitāliem elementiem drošībai.

202. Tāpēc var izdarīt tālāk uzskaitītos secinājumus.

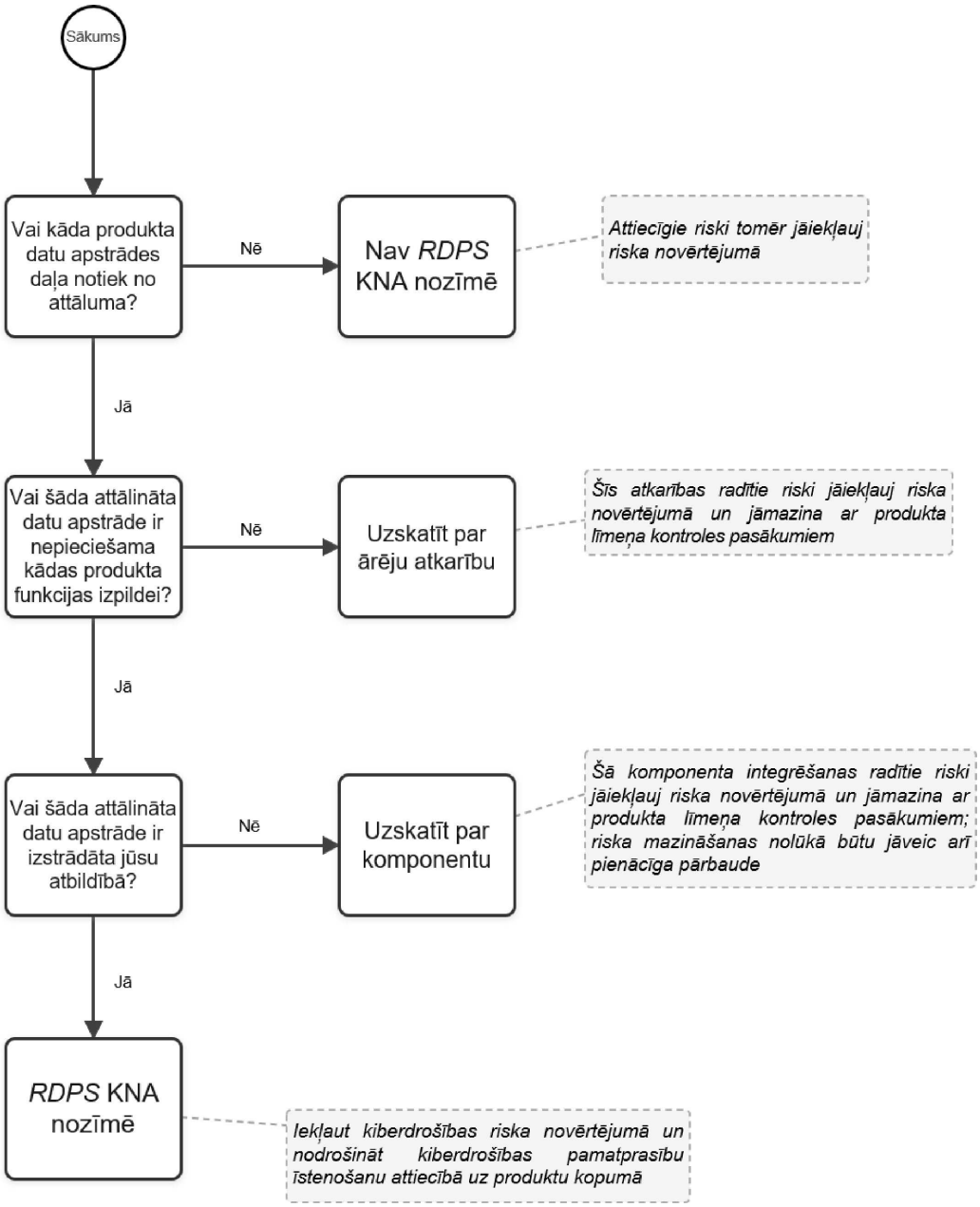
a) Lai datu apstrādi kvalificētu kā *RDPS*, atbildei uz abiem *8.1.2.* iedaļā *Vai šādas datu apstrādes neesība liegtu produktam ar digitāliem elementiem veikt kādu no savām funkcijām?* un *8.1.3.* iedaļā *Vai programmatūru ir projektējis un izstrādājis ražotājs vai tas ir darīts ražotāja atbildībā?* uzdotajiem jautājumiem ir jābūt apstiprinošai.

b) Ja atbilde uz *8.1.2.* iedaļā *Vai šādas datu apstrādes neesība liegtu produktam ar digitāliem elementiem veikt kādu no savām funkcijām?* uzdoto jautājumu ir noliedzoša, ražotājiem riska novērtējuma ietvaros būtu jānovērtē riski, kas izriet no šādas datu apstrādes.

c) Ja atbilde uz *8.1.2.* iedaļā *Vai šādas datu apstrādes neesība liegtu produktam ar digitāliem elementiem veikt kādu no savām funkcijām?* uzdoto jautājumu ir apstiprinoša, bet atbilde uz *8.1.3.* iedaļā *Vai programmatūru ir projektējis un izstrādājis ražotājs vai tas ir darīts ražotāja atbildībā?* uzdoto jautājumu ir noliedzoša, ražotājiem trešās personas risinājums būtu jāuzskata par komponentu. Riska novērtējuma ietvaros ražotājiem būtu jānovērtē riski, kas izriet no šāda risinājuma integrācijas, un tie attiecīgi jāmazina. Turklāt ražotājiem būtu jāveic pienācīga pārbaude.

9. attēls

Stilizēta blokshēma ar mērķi noteikt, vai produkts ar digitāliem elementiem ietver RDPS



8.2. **Attālinātas datu apstrādes risinājumu praktiskās un tehniskās sekas un paļaušanās uz trešo personu risinājumiem**

203. KNA pamatā ir uz risku balstīta pieeja, kas nostiprināta 13. panta 2. un 3. punktā, kā arī I pielikuma I daļas pirmajā pamatprasībā, saskaņā ar kuru "[p]roduktus ar digitāliem elementiem projektē, izstrādā un ražo tā, lai tie nodrošinātu atbilstošu kiberdrošības līmeni, pamatojoties uz riskiem". Līdz ar to, piemērojot KNA prasības *RDPS* un risinot riskus, kas izriet no trešo personu pakalpojumiem, kuri integrēti produktā ar digitāliem elementiem, būtu jāapsver uz risku balstīta pieeja.

204. Pirmkārt, ražotājiem tehniskajā dokumentācijā būtu i) jānorāda, ka to produktam ar digitāliem elementiem ir *RDPS* vai ka tas paļaujas uz trešo personu attālinātiem risinājumiem, un ii) jāapraksta šādi risinājumi. Ja viens un tas pats *RDPS* atbalsta vairākus produktus ar digitāliem elementiem, *RDPS* ir jādeklarē katra produkta tehniskajā dokumentācijā. Dokumentāciju par *RDPS*, kas apkalpo vairākus produktus ar digitāliem elementiem, var atkārtoti izmantot dažādu produktu atbilstības novērtēšanā.

205. Kā norādīts 11. apsvērumā, *RDPS*, kas ir daļa no produkta ar digitāliem elementiem un uz ko tāpēc attiecas produkta atbilstības novērtēšana, būtu jāattiecina tikai uz tiem programmatūras moduļiem, kas nodrošina produkta ar digitāliem elementiem funkcionalitāti, un uz saskarnēm, ko šie moduļi izmanto ar ārējiem pakalpojumiem. Citas aizmugursistēmas, kuras veic turpmāku apstrādi un ar kurām produktam ar digitāliem elementiem nav tiešas mijiedarbības, netiek uzskatītas par *RDPS*.

206. Tomēr šīs aizmugursistēmas joprojām ir ārējas atkarības, kas jānovērtē kiberdrošības riska novērtējuma ietvaros un kuru radītie riski jāmazina ar produkta līmeņa pasākumiem. Ražotāja veiktajā riska novērtējumā būtu jāņem vērā: i) ar *RDPS* saistītie riski, ii) riski, kas saistīti ar paļaušanos uz trešo personu attālinātiem risinājumiem (līdzīgi trešo personu komponentiem), un iii) riski, kas saistīti ar produkta vidi (piemēram, pamatā esošo aparatūru). Ražotājiem pašā produktā ar digitāliem elementiem būtu jāievieš drošības kontroles pasākumi, lai mazinātu šos riskus.

207. Turklāt atbilstības novērtēšanas un/vai ar trešo personu attālinātajiem pakalpojumiem saistīto pienācīgas pārbaudes pienākumu izpildes ietvaros ražotāja novērtējuma pamatošanai var atkārtoti izmantot cita starpā šādus apliecinājuma materiālus:

a) pierādījumus par pienākumu izpildi saskaņā ar Komisijas Īstenošanas regulu (ES) 2024/2690;

b) pierādījumus par Regulā (ES) 2022/2554 (*DORA*) noteikto pienākumu izpildi;

c) atbilstības apliecinājumu vai sertifikātu, kas iegūts saskaņā ar Eiropas kiberdrošības sertifikācijas shēmu (kas pieņemta saskaņā ar Regulu (ES) 2019/881 – Kiberdrošības aktu);

d) pierādījumus par atbilstību standartam ISO/IEC 27017:2015 vai ISO/IEC 27001:2022.

208. Visbeidzot, mijiedarbībā ar trešajām personām, kas sniedz attālinātus pakalpojumus, ražotājiem, pamatojoties uz riska novērtējumu, ir jāīsteno vispiemērotākie drošības pasākumi (attiecīgā gadījumā izmantojot arī pakalpojumu sniedzēja dalītās atbildības modeli). Šiem riska mazināšanas pasākumiem būtu jāietver ražotāju produktu ar digitāliem elementiem drošības kontroles pasākumi un pašu trešo personu pakalpojumu sniedzēju nodrošināto drošības pasākumu verifikācija (pienācīga pārbaude). Viens no līdzekļiem šādu risku mazināšanai ir drošības garantiju iekļaušana pakalpojumu līmeņa līgumos (*SLA*) ar trešo personu pakalpojumu sniedzējiem, tai skaitā apliecinājumi, ka pakalpojumu sniedzēji pienācīgi risina ievainojamības. Būtiskas izmaiņas risinājumos, ko nodrošina trešās personas, kas sniedz attālinātus pakalpojumus, nebūtu kvalificējamas kā produkta ar digitāliem elementiem būtiska modifikācija, jo šie elementi nav ražotāja atbildībā. Tomēr, pildot pienācīgas pārbaudes pienākumus un lai pienācīgi mazinātu riskus, ko rada trešo personu pakalpojumu sniedzēju izmantošana, ražotāji tiek mudināti nodrošināt, ka trešo personu mākoņdatošanas pakalpojumu sniedzēji viņus pienācīgi informē par izmaiņām, ko tie veic savos risinājumos. Pamatojoties uz šādu informāciju, ražotājiem var būt jāpārskata riska novērtējums. Atjauninātajā riska novērtējumā būtu jāapsver, vai trešo personu pakalpojumu sniedzēji joprojām sniedz pietiekamas kiberdrošības garantijas un vai produkta līmeņa drošības kontroles pasākumi joprojām ir atbilstoši. Dažos gadījumos ražotājiem var būt jāmaina šie kontroles pasākumi vai trešās personas pakalpojumu sniedzējs.

8.3. **Attālinātas datu apstrādes risinājumu lietojumgadījumi**

Lai ražotājiem sniegtu papildu praktiskus norādījumus, šajā iedaļā ir aplūkota virkne fiktīvu lietojumgadījumu, kuros aprakstīti tipiski produkti ar digitāliem elementiem, kas izmanto attālinātu datu apstrādi, un parādīts, vai šāda apstrāde ir kvalificējama kā attālinātas datu apstrādes risinājums KNA izpratnē.

8.3.1. *Mobilās bankas lietotne*

Finanšu vienība laiž tirgū mobilās bankas lietotni. Lietotnes aizmugursistēmas cita starpā nodrošina autentifikāciju, autorizāciju, kontu pārvaldību un maksājumus. Lai nodrošinātu lietotnes funkcionalitāti, finanšu vienība izmanto hibrīdstratēģiju, kurā apvienota iekšējā infrastruktūra un trešo personu attālinātie risinājumi. Tā ietver tālāk aprakstītos elementus.

Finanšu vienības izstrādāta pašuzturēta infrastruktūra

— Klients atver mobilās bankas lietotni un tiek autentificēts, izmantojot bankas saskarni – finanšu vienības izstrādātu pašuzturētu risinājumu, kas saņem lietotnes pieprasījumus un nosūta attiecīgās atbildes. Bankas saskarne verificē klienta identitāti, veicot vaicājumu kontu pārvaldības sistēmā, un piešķir piekļuvi lietotnei.

— Klients, izmantojot lietotni, uzsāk pārvedumu. Lietotne nosūta rīkojumu bankas saskarnei, kura iesniedz attiecīgu pieprasījumu virsgrāmatas sistēmai.

— Kontu pārvaldības sistēma un virsgrāmatas sistēma, kas abas ir pašuzturētas sistēmas, bet loģiski nodalītas no bankas saskarnes, reģistrē darījumu.

— Virsgrāmatas sistēma nosūta darījuma statusu bankas saskarnei, kura parāda rezultātu klientam.

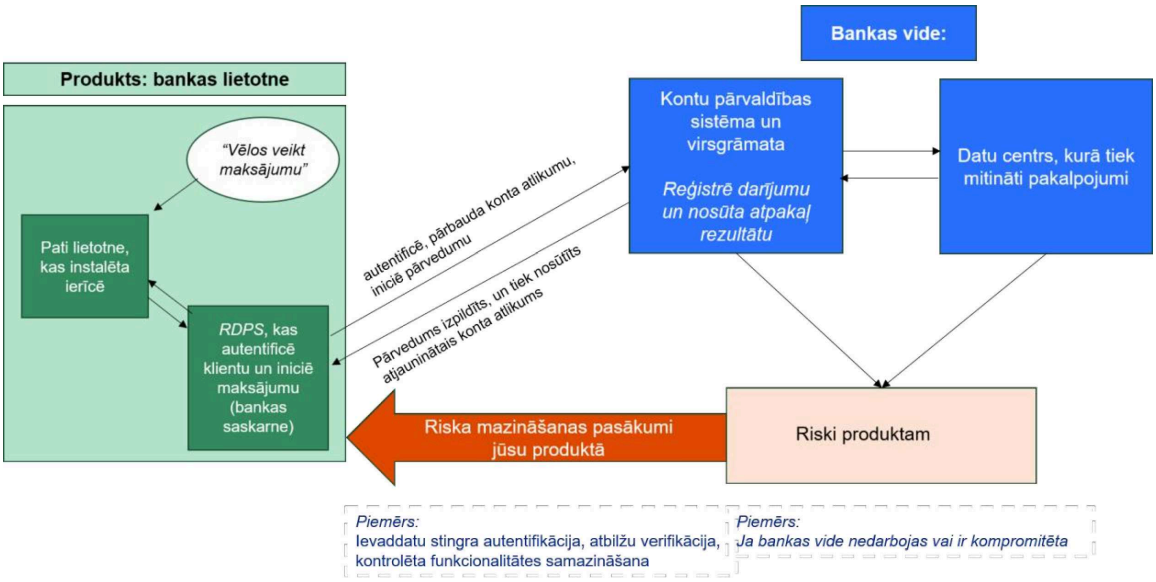
Sekas attiecībā uz RDPS

— Bankas saskarne ir nepieciešama, lai lietotne varētu pildīt savas funkcijas, proti, autentificēt klientu, iesniegt klienta rīkojumus, tostarp maksājumu un pārvedumu rīkojumus, un nosūtīt iegūto statusu. Bankas saskarne ir projektēta un izstrādāta ražotāja atbildībā. Tā kā atbilde uz abiem iepriekšējās iedaļās uzdotajiem jautājumiem ir apstiprinoša, bankas saskarne ir uzskatāma par *RDPS*. Tāpēc tā ir jāiekļauj kiberdrošības riska novērtējumā un kiberdrošības pamatprasību īstenošanā attiecībā uz produktu ar digitāliem elementiem kopumā. Rīkojuma turpmāko apstrādi pēc tā iesniegšanas, it īpaši darījuma reģistrēšanu kontu pārvaldības un virsgrāmatas sistēmās, norēķinus un tīrvērti, veic sistēmas, ar kurām lietotne tieši nemijiedarbojas, un tāpēc šāda apstrāde nav *RDPS*.

— Kontu pārvaldības sistēma un virsgrāmatas sistēma nav kvalificējamas kā bankas lietotnes *RDPS*. Lietotne ar tām tieši nemijiedarbojas (tā mijiedarbojas ar bankas saskarni, kura savukārt izmanto šīs sistēmas). Lai gan to pieejamība var būt nepieciešama funkcijas izpildei, KNA aptver tikai tās sistēmas daļas, kas tieši mijiedarbojas ar produktu ar digitāliem elementiem. Tāpēc KNA vajadzībām tās neietilpst *RDPS* definīcijā. Tomēr šīs sistēmas joprojām ir ārējas atkarības, kas var radīt būtiskus kiberdrošības riskus produktam ar digitāliem elementiem. Piemēram, virsgrāmatas sistēmas kompromitēšana varētu ļaut uzbrucējam ietekmēt darījumu rezultātus, kas pēc tam tiek parādīti lietotnē. Tāpēc ražotājam šie riski ir jāidentificē un jānovērtē kiberdrošības riska novērtējuma ietvaros un jāmazina ar produkta līmeņa pasākumiem, piemēram, stingru aizmugursistēmu saskarņu autentifikāciju, darījumu datu integritātes aizsardzību, drošiem sakaru kanāliem un lietotnes saņemto atbilžu verifikāciju.

10. attēls

Bankas lietotne, kas izmanto RDPS, – stilizēts attēlojums



Trešās personas SaaS *klientu atbalstam*

— Finanšu vienība savā lietotnē integrē klientu atbalsta tērzēšanas risinājumu, ko izstrādā un ekspluatē trešās personas pakalpojumu sniedzējs; pakalpojumu sniedzējs, kas ir trešā persona, ir uzrakstījis tērzēšanas servera kodu, izveidojis lietotāja saskarni un ekspluatē infrastruktūru, kurā ir izvietota tērzēšanas sistēma (t. i., *SaaS* modelis).

— Kad klients iesniedz atbalsta pieprasījumu, lietotne savieno klientu ar trešās personas pakalpojumu, lai izveidotu tērzēšanas sesiju un nodrošinātu ziņojumapmaiņu, nedodot trešajai personai piekļuvi bankas pamatsistēmām.

Sekas attiecībā uz RDPS

— Klientu atbalsta tērzēšanas risinājums ir nepieciešams, lai produkts ar digitāliem elementiem varētu pildīt kādu no savām funkcijām, taču finanšu vienība to nav projektējusi un izstrādājusi, un tas nav projektēts un izstrādāts tās atbildībā; tāpēc tas nav *RDPS*. Tomēr tas būtu jāuzskata par trešās personas komponentu. Šā trešās personas pakalpojuma izmantošana var radīt kiberdrošības riskus bankas lietotnei, piemēram, ja uzbrucējs izmantotu tērzēšanas kanālu, lai uzdotos par banku vai nogādātu lietotājiem ļaunprātīgu saturu. Finanšu vienībai šie riski ir jāņem vērā kiberdrošības riska novērtējumā un jāmazina ar produkta līmeņa pasākumiem, piemēram, tērzēšanas funkcijas nodalīšanu no bankas pamatsistēmas funkcijām, datu plūsmu kontroli un satura validēšanu. Pienācīga pārbaude būtu jāveic arī attiecībā uz *SaaS*.

8.3.2. *Viedais termostats*

Viedais termostats ļauj lietotājiem ar mobilās lietotnes palīdzību kontrolēt temperatūru savās mājās. Mobilā lietotne un viedais termostats izmanto attālinātu datu apstrādi, lai apmainītos ar datiem (piemēram, pieprasījumu paaugstināt temperatūru) un glabātu datus (piemēram, lietotāja preferences). Šīs funkcijas ir projektētas un izstrādātas ražotāja atbildībā, taču tās darbojas pamatā esošajā fiziskajā un virtuālajā infrastruktūrā, ko nodrošina trešā persona (trešās personas *IaaS*).

Tā kā bez šīs attālinātās datu apstrādes viedais termostats nevarētu nodrošināt savas viedās funkcijas, tās neesība liegtu produktam ar digitāliem elementiem pildīt vienu vai vairākas tā funkcijas. Turklāt programmatūra ir projektēta un izstrādāta viedā termostata ražotāja atbildībā. Tāpēc attālinātā datu apstrāde ir kvalificējama kā *RDPS* KNA izpratnē.

Lai nodrošinātu atbilstību KNA, viedā termostata ražotājam produkta ar digitāliem elementiem tehniskajā dokumentācijā ir jādokumentē *RDPS* un trešās personas *IaaS* izmantošana, tai skaitā jāsniedz informācija par līgumā paredzēto pakalpojumu. Ražotājam šie elementi ir jāņem vērā riska novērtējumā, kas ietver produkta ar digitāliem elementiem paredzēto nolūku un pamatoti paredzamo lietojumu. Ražotājs, pamatojoties uz *RDPS* radītajiem riskiem, īsteno KNA kiberdrošības pamatprasības. Attiecībā uz trešās personas *IaaS* ražotājam ir jānodrošina, ka trešās personas pakalpojumu sniedzēja nodrošinātie drošības pasākumi ir atbilstoši, un/vai jāveic attiecīgi pasākumi attiecībā uz infrastruktūru. Attiecībā uz pirmo no minētajiem aspektiem ražotājs, piemēram, varētu pieprasīt pierādījumus, ka ir izpildīti TID 2 pienākumi.

8.3.3. *E-lasītājs*

E-lasītāja programmatūras ražotājs izmanto trešās personas *SaaS* glabāšanas pakalpojumu, lai glabātu klientu iegādātās elektroniskās grāmatas un nodrošinātu klientiem piekļuvi viņu iegādātajām grāmatām. Šā glabāšanas pakalpojuma neesība liegtu produktam ar digitāliem elementiem pildīt kādu no tā funkcijām, taču trešās personas *SaaS* glabāšanas pakalpojumu nav izstrādājis ražotājs un tas nav izstrādāts ražotāja atbildībā; *SaaS* pakalpojumu sniedzējs to dara pieejamu klientiem jebkādiem lietojumgadījumiem.

SaaS glabāšanas pakalpojums neatbilst *RDPS* definīcijai. Tomēr e-lasītāja ražotājs sava produkta ar digitāliem elementiem darbībai izmanto šo ārējo pakalpojumu, tāpēc ar to saistītie riski ir jāņem vērā kiberdrošības riska novērtējumā. E-lasītāja ražotājam *SaaS* būtu jāuzskata par komponentu. Ražotājam ir jāīsteno atbilstoši produkta līmeņa drošības pasākumi, piemēram, droša autentifikācija, šifrēšana un sakaru ar glabāšanas pakalpojumu integritātes aizsardzība. Arī pienācīga pārbaude, izvēloties un integrējot *SaaS* pakalpojumu sniedzēju, palīdzēs ražotājam izpildīt tā pienākumus, lai produkts ar digitāliem elementiem kopumā varētu atbilst kiberdrošības pamatprasībām.

8.3.4. *Rūpniecības robots*

Rūpniecības robota uzdevums ir satvert detaļas. Robots ar kamerām savākto informāciju nosūta attālinātam pakalpojumam, ko projektējis un izstrādājis ražotājs. Šis pakalpojums darbojas pamatā esošajā fiziskajā un virtuālajā infrastruktūrā, ko nodrošina pakalpojumu sniedzējs, kas ir trešā persona (trešās personas *IaaS*). Mākoņpakalpojums, pamatojoties uz kameru datu plūsmām, aprēķina detaļas atrašanās vietu un nosūta robotam komandas detaļu satveršanai.

Šādas datu apstrādes neesība liegtu rūpniecības robotam satvert detaļas un tādējādi pildīt vienu no tā funkcijām. Turklāt programmatūru, kas darbojas uz šīs infrastruktūras pamata, ir projektējis un izstrādājis ražotājs. Ražotāja projektētā un izstrādātā programmatūra atbilst *RDPS* definīcijai.

Rūpniecības robota ražotājam produkta ar digitāliem elementiem tehniskajā dokumentācijā ir jādokumentē *RDPS* un trešās personas *IaaS* izmantošana (tai skaitā jāsniedz informācija par līgumā paredzēto pakalpojumu). Ražotājam šie elementi ir jāņem vērā arī riska novērtējumā, kas ietver produkta ar digitāliem elementiem paredzēto nolūku un pamatoti paredzamo lietojumu. Ražotājs, pamatojoties uz riskiem, īsteno KNA kiberdrošības pamatprasības attiecībā uz produktu ar digitāliem elementiem, tostarp tā *RDPS*. Arī pienācīga pārbaude, izvēloties *IaaS* pakalpojumu sniedzēju, palīdzēs ražotājam izpildīt tā pienākumus. Piemēram, ražotājs varētu pieprasīt pierādījumus, ka ir izpildīti TID 2 pienākumi.

8.3.5. *Mobilo sakaru tīkls*

Viedtālrunis izmanto 5G tīklu, lai lietotājiem nodrošinātu interneta savienojumu, tālruņa zvanus un ziņojumus (mobilā savienotība). Mobilo sakaru tīklu projektē un izstrādā telekomunikāciju operatori. Tīklu veido mazizmēra šūnas un mobilo sakaru torņi, kā arī cits tīkla aprīkojums.

Produktam ar digitāliem elementiem būtu jāspēj pareizi izveidot savienojumu ar tīklu; tā ir viena no tā funkcijām. Tomēr tam, vai šis tīkls darbojas, nav nozīmes, lai noteiktu, vai produkts ar digitāliem elementiem darbojas pareizi. Tīkls ir tikai sakaru kanāls, un tas nav nepieciešams, lai produkts ar digitāliem elementiem pildītu savu funkciju "pareizi izveidot savienojumu ar tīklu". Tāpat *Ethernet* kabelis, maršrutētājs vai *Wi-Fi* signāls netiek uzskatīts par datu apstrādi, kuras neesība liegtu produktam ar digitāliem elementiem pildīt kādu no tā funkcijām, bet gan par sakaru vai savienotības nodrošināšanas līdzekli.

Līdz ar to mobilo sakaru tīkls neatbilst *RDPS* definīcijai. Tīkls nebūtu jāuzskata par trešās personas komponentu, jo produktā ar digitāliem elementiem nav integrēta programmatūra; produkts vienkārši izmanto šo tīklu. Tādēļ ražotājam nav jāveic pienācīga pārbaude attiecībā uz tīkla nodrošinātāju.

9. **PAPILDU ELEMENTI**

9.1. **Ziņošanas pienākumi**

209. Saskaņā ar KNA 14. panta 1. un 3. punktu ražotājam par koordinatoru izraudzītajai *CSIRT* un *ENISA* vienlaikus jāpaziņo: i) par jebkuru aktīvi izmantotu ievainojamību, ko satur tā produkts ar digitāliem elementiem un par ko tam kļūst zināms, un ii) par jebkuru nopietnu incidentu, kas ietekmē produkta ar digitāliem elementiem drošību un par ko tam kļūst zināms.

210. Saskaņā ar 69. panta 3. punktu un 71. panta 2. punkta otro teikumu pienākumu ievērot 14. pantu no 2026. gada 11. septembra piemēro visiem produktiem ar digitāliem elementiem, kas ietilpst KNA darbības jomā, tostarp produktiem ar digitāliem elementiem, kuri laisti tirgū pirms 2027. gada 11. decembra. Turklāt atšķirībā no ievainojamību novēršanas pienākumiem, kas ir spēkā tikai produkta atbalsta periodā, ziņošanas pienākumus turpina piemērot arī pēc tam, kad produkts ar digitāliem elementiem vairs netiek atbalstīts. Ja produkts ar digitāliem elementiem ir laists tirgū pirms 2027. gada 11. decembra vai ja tā atbalsta periods ir beidzies, ražotājam nav jāpilda I pielikuma II daļā noteiktie ievainojamību novēršanas pienākumi.

211. Jāatgādina, ka pienākumu paziņot par šādiem notikumiem piemēro, tiklīdz ražotājs uzzina, ka ievainojamība tiek aktīvi izmantota vai ka ir noticis nopietns incidents, kura rezultātā ir apdraudēta tā produkta ar digitāliem elementiem drošība. Tāpēc norādījumiem par to, kad uzskatāms, ka ražotājs ir uzzinājis par attiecīgo notikumu, būtu jāpalīdz ražotājiem noteikt brīdi, no kura sāk skaitīt piemērojamos ziņošanas termiņus.

212. Uz ražotājiem saskaņā ar dažādiem ES tiesību aktiem var attiekties salīdzināmi ziņošanas pienākumi. Lai nodrošinātu konsekventu interpretāciju par to, kad uzskatāms, ka ražotājs ir uzzinājis par attiecīgo faktu, un atvieglotu ražotājiem minēto pienākumu izpildi, šie norādījumi ir saskaņoti ar Komisijas Īstenošanas regulas (ES) 2024/2690 31. apsvērumu un EDAK Pamatnostādņu 9/2022 par personas datu aizsardzības pārkāpumu paziņošanu saskaņā ar VDAR II iedaļas A punktu.

213. Dažos gadījumos ražotājs konstatēs aizdomīgu notikumu, savukārt citos trešā persona, piemēram, fiziska persona, klients, vienība, iestāde, mediju organizācija vai cits avots, vērsīs tā uzmanību uz iespējamu incidentu vai ievainojamību. Šādos gadījumos ražotājam aizdomīgais notikums būtu nekavējoties jānovērtē, lai noteiktu, vai tas ir aktīvi izmantota ievainojamība vai nopietns incidents, kas ietekmē produkta ar digitāliem elementiem drošību. Tāpēc uzskatāms, ka ražotājs ir uzzinājis par attiecīgo faktu, ja pēc šāda sākotnējā novērtējuma tam ir pamatota pārliecība, ka: i) tiek aktīvi izmantota kāda ievainojamība, ko satur tā produkts ar digitāliem elementiem, vai ii) ir noticis nopietns incidents, kura rezultātā ir apdraudēta tā produkta ar digitāliem elementiem drošība.

214. Tāpēc brīdis, kad var uzskatīt, ka ražotājs ir uzzinājis par attiecīgo faktu, būs atkarīgs no konkrētās aktīvi izmantotās ievainojamības vai nopietnā incidenta apstākļiem. Dažos gadījumos jau no paša sākuma būs samērā skaidrs, ka ievainojamība tiek aktīvi izmantota vai ka nopietns incidents ietekmē produkta ar digitāliem elementiem drošību. Citos gadījumos var būt vajadzīgs zināms laiks, lai noteiktu, vai produktu ar digitāliem elementiem ietekmē ievainojamība un vai šo ievainojamību izmanto ļaunprātīgs dalībnieks, vai arī incidents ietekmē produkta ar digitāliem elementiem drošību. Tomēr uzsvars būtu jāliek uz tūlītēju rīcību, veicot sākotnējo novērtējumu, lai noteiktu, vai šie nosacījumi patiešām ir izpildīti, it īpaši tad, ja ievainojamība var radīt būtisku risku, un, ja šie nosacījumi ir izpildīti, veikt korektīvus pasākumus un paziņot saskaņā ar KNA.

215. Turklāt ziņošanas kārtība paredz, ka ražotājiem savi paziņojumi jāatjaunina pakāpeniski – līdz ar iekšējās izmeklēšanas virzību un detalizētākas informācijas iegūšanu par incidentu vai aktīvi izmantoto ievainojamību. Konkrētāk, ražotājiem bez liekas kavēšanās un jebkurā gadījumā 24 stundu laikā pēc uzzināšanas jāiesniedz agrīnais brīdinājums, kurā ietverta ierobežota informācija. Pēc tam papildu informācija jāsniedz paziņojumā, kas jāiesniedz bez liekas kavēšanās un jebkurā gadījumā 72 stundu laikā pēc uzzināšanas (“72 stundu paziņojums”). Galīgais ziņojums par aktīvi izmantotām ievainojamībām jāiesniedz 14 dienu laikā pēc tam, kad ir pieejams korektīvs vai riska mazināšanas pasākums, savukārt par nopietniem incidentiem – viena mēneša laikā pēc 72 stundu paziņojuma.

216. Kā atgādināts arī *3.3.1.* iedaļā *Ilgstošs atbalsts un FOSS dzīvotspējas nodrošināšana*, atvērtā pirmkoda programmatūras pārziņiem saskaņā ar 24. panta 3. punktu arī jāziņo par aktīvi izmantotām ievainojamībām ([30]). Šo pienākumu piemēro, kad pārzinis uzzina par aktīvi izmantotu ievainojamību, nevis tikai tad, ja ievainojamība pastāv tādas *FOSS* koda bāzē, kuras pārzinis ir attiecīgā vienība. Praksē, tā kā *FOSS* komponenti parasti tiek integrēti citos produktos ar digitāliem elementiem lejasposmā, pārzinis par aktīvu izmantošanu, visticamāk, uzzinās no trešo personu ziņojumiem, kuros konstatēta citos produktos ar digitāliem elementiem integrētu *FOSS* komponentu ievainojamību aktīva izmantošana. Tas tā var būt, piemēram, ja produkta ar digitāliem elementiem ražotājs konstatē, ka tā produktā integrēta *FOSS* komponenta ievainojamība tiek aktīvi izmantota, un ziņo par to minētā komponenta pārzinim; vai ja lietotājs vai drošības pētnieks atrod pierādījumus, ka produktā ar digitāliem elementiem integrēta *FOSS* komponenta ievainojamība tiek aktīvi izmantota, un par šo aktīvo izmantošanu ziņo komponenta pārzinim.

217. Būtu jāprecizē arī tas, ka, tā kā pienākumu ziņot par aktīvi izmantotām ievainojamībām piemēro no brīža, kad ražotājs uzzina par aktīvu izmantošanu, ražotājam nav jāziņo par ievainojamībām, par kuru aktīvu izmantošanu tas bija uzzinājis jau pirms 2026. gada 11. septembra (datuma, no kura sāk piemērot ziņošanas pienākumu). Tādējādi KNA nav prasīts par šādām ievainojamībām ziņot atpakaļejošā kārtībā. Savukārt pienākumu piemēro, ja ražotājs zināja par ievainojamību pirms 2026. gada 11. septembra, taču tolaik nezināja, ka tā tiek aktīvi izmantota (vai nu tāpēc, ka aktīva izmantošana vēl nebija notikusi, vai arī tāpēc, ka ražotājs par to vēl nebija uzzinājis). Ja pēc 2026. gada 11. septembra ievainojamību sāk aktīvi izmantot vai ražotājs uzzina par tās aktīvu izmantošanu, šo ievainojamību uzskata par aktīvi izmantotu ievainojamību, uz kuru attiecas ziņošanas pienākums.

218. Tāpat ražotājam ir jāziņo tikai par aktīvi izmantotām ievainojamībām, ko satur tā produkts ar digitāliem elementiem. Ja produkts ar digitāliem elementiem satur aktīvi izmantotu ievainojamību, kuras izcelsme ir trešās personas komponentā, produkta ar digitāliem elementiem ražotājam ir jāpaziņo par šo aktīvi izmantoto ievainojamību. Tomēr, ja ražotājs zina, ka trešās personas komponents satur ievainojamību, bet šo ievainojamību vai nu i) nevar izmantot tā produktā ar digitāliem elementiem (piemēram, tāpēc, ka ievainojamais kods nav sasniedzams), vai arī ii) attiecīgajā produktā ar digitāliem elementiem tā nav izmantota, minētā ievainojamība nav kvalificējama kā aktīvi izmantota ievainojamība, ko satur tā produkts ar digitāliem elementiem, un tādēļ uz to neattiecas attiecīgā ražotāja obligātais ziņošanas pienākums. Minētais ražotājs tomēr var brīvprātīgi paziņot par šo ievainojamību saskaņā ar KNA 15. pantu. Tam arī jāievēro KNA I pielikuma II daļā noteiktās ievainojamību novēršanas prasības, kā arī saskaņā ar 13. panta 6. punktu jāziņo par ievainojamību personai vai vienībai, kas ražo vai uztur komponentu, kā sīkāk paskaidrots *9.2.1.* iedaļā *Ziņošana augšposmā un drošības labojumu kopīgošana*.

([30]) Ciktāl pārzinis ir iesaistīts produkta ar digitāliem elementiem izstrādē.

219. Kad ražotāji ir uzzinājuši par aktīvi izmantotu ievainojamību vai nopietnu incidentu, tiem saskaņā ar 14. panta 8. punktu arī jāinformē skartie lietotāji un attiecīgā gadījumā visi lietotāji. Ja tie to neizdara savlaicīgi, paziņojumu saņēmušās *CSIRT* var sniegt šādu informāciju lietotājiem, ja tas tiek uzskatīts par samērīgu un nepieciešamu, lai novērstu vai mazinātu minētās ievainojamības vai incidenta ietekmi.

220. Atbilstoši KNA uz risku balstītajai pieejai 14. panta 8. punktā noteiktais pienākums informēt lietotājus jāpiemēro samērīgi un atbilstoši riskiem. Konkrētāk, informācijas sniegšana par aktīvi izmantotu ievainojamību vai nopietnu incidentu nenozīmē, ka šī informācija ir jāpublisko vai jāizpaužnes elektīvi. Attiecīgā gadījumā un ņemot vērā produkta ar digitāliem elementiem raksturu, skartos lietotājus un ievainojamības vai incidenta iespējamo ietekmi, ražotāji var ierobežot detalizētas informācijas izpaušanu, to sniedzot tikai attiecīgajiem lietotājiem vai klientiem. Tas it īpaši attiecas uz produktiem ar digitāliem elementiem, kurus izmanto sensitīvās vai būtiski svarīgās vidēs, kur tehnisku detaļu publiska izpaušana pati par sevi varētu palielināt kiberdrošības riskus vai atvieglot ievainojamības turpmāku izmantošanu.

221. Kad ievainojamība ir pienācīgi novērsta vai tās radītais risks mazināts, var būt lietderīgi informāciju izpaust plašāk. Tā tas būtu, piemēram, ja informācijas izpaušana palīdz palielināt vispārējo informētību vai ļauj lietotājiem verificēt, ka viņu produkti ar digitāliem elementiem vairs nav skarti. Šādos gadījumos jebkādas plašākas informācijas izpaušanas detalizācijas līmenim un laikam arī turpmāk vajadzētu būt samērīgiem, ņemot vērā atlikušos ievainojamības izmantošanas riskus, produkta ar digitāliem elementiem būtību un attiecīgo lietotāju intereses. Turklāt I pielikuma II daļas 4. punktā ir noteikts, ka ražotājiem publiski jāatklāj informācija par novērstajām ievainojamībām, tiklīdz drošības atjauninājums ir darīts pieejams.

9.2. **Ievainojamību novēršana**

9.2.1. *Ziņošana augšposmā un drošības labojumu kopīgošana*

222. KNA 13. panta 6. punktā noteikts, ka ražotājiem par ievainojamībām integrētajos komponentos jāziņo personai vai vienībai, kas ražo vai uztur attiecīgo komponentu (“ziņošana augšposmā”).

223. Ražotājiem ir pienākums ziņot augšposmā tikai attiecībā uz to komponenta versiju, kuru tie integrē. Ja persona vai vienība, kas ražo vai uztur komponentu, ir ieviesusi drošības politikas, koordinētas informācijas par ievainojamībām izpaušanas procesus vai īpašus kanālus ziņošanai par ievainojamībām, ražotājiem būtu jāziņo saskaņā ar tiem, it īpaši tad, ja vēl nenovērstu ievainojamību priekšlaicīga izpaušana varētu palielināt kiberdrošības riskus. Turklāt, lai mazinātu slogu augšposma uzturētājiem, it īpaši atvērtā pirmkoda projektos, ražotājiem nav jāziņo augšposmā, ja tie var pārliecināties, ka persona vai vienība, kas ražo vai uztur komponentu, zina par ievainojamības esību. Ražotāji tiek mudināti veikt pamatotus pasākumus, lai izvairītos no dublējošu ziņojumu iesniegšanas, piemēram, pirms ziņošanas augšposmā pārbaudot publiski pieejamas ievainojamību datubāzes, konkrētā projekta drošības paziņojumus vai izveidotas problēmu uzskaites sistēmas.

224. Ražotājiem ir pienākums ziņot augšposmā tikai par tām ievainojamībām, kas pastāv pašā integrētajā komponentā, nevis par ievainojamībām, kuras rodas, komponentu integrējot ar citu ražotāja izstrādātu kodu vai integrējot citus komponentus. Tomēr var būt situācijas, kad komponenta integrēšana konkrētā produktā ar digitāliem elementiem atklāj noteiktu šā komponenta darbību, mijiedarbību vai drošībai būtiskas īpašības, kas, aplūkojot komponentu atsevišķi, nebija acīmredzamas vai viegli identificējamas. Šādos gadījumos ražotāji tiek mudināti paziņot šo informāciju personai vai vienībai, kas ražo vai uztur komponentu, lai veicinātu labu praksi ievainojamību risināšanā, sekmētu to efektīvu novēršanu un uzlabotu komponenta ekosistēmas vispārējo drošību.

225. Visbeidzot, ražotājiem nav jāziņo par ievainojamību augšposmā arī tad, ja komponentam vairs nav uzturētāja vai ja ražotājs jaunu versiju vai drošības labojumu saņemšanā vairs nepaļaujas uz sākotnējo uzturētāju. Tomēr šādos gadījumos ražotājs tiek mudināts informēt attiecīgā komponenta lietotājus, izmantojot pamatotus alternatīvus pasākumus, piemēram, esošos kopienas mehānismus (piemēram, adresātu sarakstus vai problēmu pieteikumus) vai publiskus ievainojamību ierakstus.

226. Turklāt saskaņā ar 13. panta 6. punktu ražotājiem, kas ir izstrādājuši programmatūras modifikāciju integrēta komponenta ievainojamības novēršanai, šī programmatūras modifikācija ("drošības labojums") ir jākopīgo ar personu vai vienību, kas ražo vai uztur komponentu ("kopīgošana augšposmā").

227. Ja ražotājiem saskaņā ar 13. panta 6. punktu ir jākopīgo drošības labojums, tas attiecīgā gadījumā būtu jāsniedz mašīnlasāmā formātā un tā, lai persona vai vienība, kas ražo vai uztur komponentu, to varētu viegli verificēt un attiecīgā gadījumā integrēt. Ja komponents ir brīvi pieejamas atvērtā pirmkoda programmatūras komponents, drošības labojums būtu jākopīgo veidā, kas ir saderīgs ar šā komponenta licenci, piemēram, saskaņā ar to pašu licenci vai licenci, kas ļauj uzturētājam izplatīt drošības labojumu saskaņā ar savu licenci. Ja attiecīgā komponenta uzturētājam ir norādījumi par drošības labojumu kopīgošanu, ražotājam šie norādījumi būtu jāievēro.

228. Tomēr KNA neprasa ražotājiem nodrošināt, lai persona vai vienība, kas ražo vai uztur komponentu, to drošības labojumus noteikti pieņemtu. Tiem arī nav jānodrošina, lai šie drošības labojumi noteikti tiktu integrēti komponenta koda repozitorijā, piemēram, ja uzturētājs problēmas novēršanai dod priekšroku citam risinājumam. Tāpat ražotājiem nav jāpieņem komponenta uzturētāja izstrādātais ierosinātais drošības labojums, un tie var dot priekšroku attiecīgā riska mazināšanai citos piemērotos veidos.

229. Dažos gadījumos persona vai vienība, kas ražo vai uztur komponentu, jau var būt sniegusi drošības labojumu ievainojamības novēršanai, taču ražotājs īsteno citu riska mazināšanas stratēģiju (piemēram, mainot citu konfigurāciju). Šādos gadījumos KNA neprasa ražotājam kopīgot augšposmā citas sistēmas daļas modifikāciju. Tomēr ražotājs tiek mudināts to darīt, ja tas var palīdzēt personai vai vienībai, kas uztur komponentu.

9.2.2. *Zināmās izmantojamās ievainojamības*

230. Viena no KNA I pielikuma I daļas kiberdrošības pamatprasībām paredz, ka, pamatojoties uz 13. panta 2. punktā minēto kiberdrošības riska novērtējumu, un attiecīgā gadījumā produkti ar digitāliem elementiem tiek darīti pieejami tirgū bez zināmām izmantojamām ievainojamībām.

231. KNA 3. panta 41. punktā "izmantojama ievainojamība" ir definēta kā "ievainojamība, ko pretinieki var efektīvi izmantot praktiskos ekspluatācijas apstākļos". Ne visas ievainojamības ir izmantojamas praktiskos ekspluatācijas apstākļos, un dažas ievainojamības var izmantot tikai teorētiskos apstākļos (piemēram, laboratorijā vai simulācijā) un/vai ne tādos apstākļos, kādi rastos produkta ar digitāliem elementiem darbības vidē.

232. KNA nosaka, ka ražotājiem ir jābūt atbilstošai politikai un procedūrām, lai apstrādātu un novērstu iespējamās ievainojamības, par kurām ziņots no iekšējiem vai ārējiem avotiem (13. panta 8. punkts). Tomēr KNA nav skaidri noteikts, kad izmantojama ievainojamība būtu uzskatāma par ražotājam zināmu, tādējādi izraisot pienākumu ievērot šo kiberdrošības pamatprasību laišanas tirgū brīdī.

233. Ievainojamība būtu jāuzskata par zināmu, ja tā ir iekļauta attiecīgajās publiski pieejamajās ievainojamību datubāzēs, piemēram, Eiropas ievainojamību datubāzē, kas izveidota saskaņā ar Direktīvas (ES) 2022/2555 12. panta 2. punktu, vai citās plaši atzītās ievainojamību datubāzēs.

234. Turklāt ievainojamība var būt zināma arī tad, ja ražotājs par to ir uzzinājis no nepubliskas informācijas, piemēram, drošības jomas pētnieka koordinētas informācijas izpaušanas ceļā vai ražotāja paša iekšējās testēšanas un analīzes rezultātā, tostarp, piemēram, izmantojot ar MI darbināmus pakalpojumus. Tāpat ievainojamība var būt uzskatāma par zināmu, ja par to publiski un plaši ziņots uzticamos mediju kanālos, tostarp specializētās kiberdrošības publikācijās vai vispārējos medijos.

235. Tomēr tas vien, ka par ievainojamību tiek ziņots vai tā tiek konstatēta, pats par sevi nenozīmē, ka tā ir izmantojama praksē vai attiecas uz konkrēto produktu ar digitāliem elementiem. Ražotājam būs jāizmeklē ievainojamība un jāapstiprina šīs informācijas patiesums un piemērojamība savam produktam ar digitāliem elementiem. Attiecīgi no pirmā ziņojuma par ievainojamību līdz tās apstiprināšanai var paiet ierobežots laikposms. Kā norādīts *9.1.* iedaļā *Ziņošanas pienākumi*, uzsvars būtu jāliek uz tūlītēju rīcību, lai veiktu izmeklēšanu un attiecīgi reaģētu.

236. Turklāt saskaņā ar 13. panta 1. punktu pienākumu ievērot I pielikuma I daļā noteiktās kiberdrošības pamatprasības ražotājiem piemēro brīdī, kad produkts tiek laists tirgū. Praksē jaunas potenciāli izmantojamas ievainojamības var tikt atklātas produkta ar digitāliem elementiem izstrādes aprites cikla pēdējos posmos, tai skaitā neilgi pirms tā nonākšanas izplatīšanas ķēdē (un līdz ar to – laišanas tirgū).

237. Tā kā pienākums laist tirgū produktus ar digitāliem elementiem bez zināmām izmantojamām ievainojamībām ir uz risku balstīts pienākums, ražotājam, pamatojoties uz kiberdrošības riska novērtējumu, jānosaka, vai produktu ar digitāliem elementiem var droši laist tirgū, ievērojot KNA. Ražotājs var arī secināt, ka jauna ievainojamība, kas var būt kļuvusi zināma, ir jānovērš, pirms produktu ar digitāliem elementiem var laist tirgū. Pieņemot šādu lēmumu, ražotājiem būtu jāņem vērā ievainojamības nopietnības pakāpe, izmantojamība un iespējamā ietekme, kā arī riski, kas pēc produkta ar digitāliem elementiem lietošanas sākšanas rodas pašam produktam. Tie var ņemt vērā arī riskus, ko rada produkta izlaides atlikšana līdz ievainojamības novēršanai, piemēram, tāpēc, ka jaunā versija novērš arī citas izmantojamas ievainojamības vai ir nepieciešama kritisku sistēmu nepārtrauktai darbībai. Jebkurā gadījumā pēc produkta ar digitāliem elementiem laišanas tirgū ražotājam joprojām ir pienākums nodrošināt, ka ievainojamības tiek risinātas efektīvi un saskaņā ar I pielikuma II daļā noteiktajām ievainojamību novēršanas prasībām.

9.2.3. *Efektīvi un regulāri testi un pārskati*

238. I pielikuma II daļas 3. punktā ir noteikts, ka ražotājiem visā atbalsta periodā jāveic efektīvi un regulāri produkta ar digitāliem elementiem drošības testi un pārskati. Regulāru testu veikšana neprasa mehāniski noteiktos intervālos atkārtot nemainīgu testēšanas kampaņu. Tas nozīmē regulāri pārskatīt, vai jauna informācija, piemēram, no jauna identificēti kiberdraudi vai jaunatklātas ievainojamības, prasa atjaunināt esošos testus, un pēc tam attiecīgi veikt testus.

239. Pārskatīšanas biežumam, dziļumam un saturam vajadzētu būt samērīgam ar produkta ar digitāliem elementiem kiberdrošības riska profilu, tā izmaiņām laika gaitā un kiberdraudu situāciju. Ja pārskatīšanā tiek konstatēta attiecīga jauna informācija, kas ietekmē testu kopumu, būtu jāizstrādā jauni vai modificēti testi un tie jāveic attiecībā uz produktu, lai nodrošinātu, ka neviena ievainojamība nepaliek nerisināta. Tas var ietvert esošo testu atkārtotu veikšanu, ja produkta ar digitāliem elementiem modifikācijas dēļ šāds testēšanas veids kļūst lietderīgs, piemēram, regresijas testēšanu.

240. Ja pārskatīšanā šāda jauna informācija netiek konstatēta, papildu testi nav jāizstrādā. Vienlaikus turpina piemērot citus ievainojamību novēršanas pienākumus, tostarp pienākumu atbilstoši radītajiem riskiem pievērsties ievainojamībām un tās novērst.

9.3. **Mijiedarbība ar citiem tiesību aktiem**

9.3.1. *Regula (ES) 2019/2144 un Regula (ES) Nr. 168/2013*

241. KNA 2. panta 2. punkta c) apakšpunktā ir noteikts, ka KNA nepiemēro produktiem ar digitāliem elementiem, uz kuriem attiecas Regula (ES) 2019/2144. Regulu (ES) 2019/2144 piemēro "M, N un O kategorijas transportlīdzekļiem, kā tie definēti Regulas (ES) 2018/858 4. pantā, un sistēmām, sastāvdaļām un atsevišķām tehniskajām vienībām, kas konstruētas un izgatavotas šādiem transportlīdzekļiem".

242. Tāpat produkti ar digitāliem elementiem, kas ietilpst Regulas (ES) Nr. 168/2013 darbības jomā, ar Komisijas Deleģēto regulu (ES) 2025/1535 ir izslēgti no KNA darbības jomas. Regula (ES) Nr. 168/2013 attiecas uz L kategorijas transportlīdzekļiem un "uz šādiem transportlīdzekļiem konstruētām un izgatavotām sistēmām, sastāvdaļām un atsevišķām tehniskām vienībām, kā arī detaļām un aprīkojumu" (2. panta 1. punkts).

243. Uz transportlīdzekļiem, kuriem piemēro minētās regulas, KNA neattiecas. Turklāt ir vajadzīgi papildu precizējumi par atbrīvojuma tvērumu attiecībā uz šādiem transportlīdzekļiem konstruētām un izgatavotām sistēmām, sastāvdaļām, atsevišķām tehniskām vienībām, detaļām un aprīkojumu (šajā iedaļā – "komponenti"), kas uzskatāmi par produktiem ar digitāliem elementiem KNA nozīmē.

244. Tiek uzskatīts, ka šādiem komponentiem KNA nav piemērojams, ja tie ir konstruēti un izgatavoti tikai integrēšanai transportlīdzekļos, uz kuriem attiecas Regula (ES) 2019/2144 un Regula (ES) Nr. 168/2013. Tas tā ir neatkarīgi no tā, vai attiecīgā komponenta ražotājs to pārdod tieši transportlīdzekļa ražotājam vai citam uzņēmējam automobiļu piegādes ķēdē, ja vien komponents ir skaidri paredzēts un piemērots tikai galīgai integrēšanai šādos transportlīdzekļos.

245. Savukārt KNA attiecas uz ražotāju, kas pārdod vispārīga lietojuma komponentus, kuri ir produkti ar digitāliem elementiem un kurus var integrēt dažādu veidu produktos, nevis tikai transportlīdzekļos, uz kuriem attiecas minētās regulas.

246. Novērtējums par to, vai komponents ir laists tirgū KNA izpratnē, jābalsta uz objektīvajiem nosacījumiem, saskaņā ar kuriem tas tiek darīts pieejams. Ja ražotājs komponentu, kas nav piemērots tikai galīgai integrēšanai šādos transportlīdzekļos, piedāvā izplatīšanas kanālos, kuri ir pieejami klientiem ārpus automobiļu piegādes ķēdes, piemēram, vispārējās mazumtirdzniecības vietās vai tiešsaistes pārdošanas kanālos, kuros pieņem plašas sabiedrības pasūtījumus, šis komponents ietilpst KNA darbības jomā neatkarīgi no jebkādiem apgalvojumiem par tā paredzēto izmantošanu. Šādos apstākļos komponentu nevar uzskatīt par konstruētu un izgatavotu tikai integrēšanai transportlīdzekļos, uz kuriem attiecas Regula (ES) 2019/2144 un Regula (ES) Nr. 168/2013, un ražotājam ir jāievēro KNA. Savukārt ierobežotu starpuzņēmumu izplatīšanas kanālu izmantošana tikai automobiļu piegādes ķēdē var liecināt, ka komponents ir konstruēts un izgatavots tikai šādai integrēšanai.

9.3.2. *ES tipa pārbaudes sertifikātu derīgums (69. panta 1. punkts)*

247. KNA 69. panta 1. punktā ir noteikts, ka "ES tipa pārbaudes sertifikāti un apstiprinājuma lēmumi, kas izdoti attiecībā uz kiberdrošības prasībām par produktiem ar digitāliem elementiem, uz kuriem attiecas Savienības saskaņošanas tiesību akti, kas nav šī regula, paliek spēkā līdz 2028. gada 11. jūnijam, ja vien to derīguma termiņš nav beidzies pirms minētās dienas vai ja šādos citos Savienības saskaņošanas tiesību aktos nav noteikts citādi, un tādā gadījumā tie paliek spēkā termiņā, kas norādīts minētajos Savienības tiesību aktos".

248. Šādu sertifikātu un apstiprinājuma lēmumu turpmākais derīgums būtu jāsaprot kā ierobežots tikai ar tiem kiberdrošības riskiem un attiecīgajām prasībām, ko aptver Savienības saskaņošanas tiesību akti, uz kuru pamata tie izdoti. Attiecībā uz minētajiem riskiem ražotājiem 69. panta 1. punktā minētajā derīguma laikposmā nav atkārtoti jānovērtē vai atkārtoti jāpierāda atbilstība tikai KNA vajadzībām attiecībā uz produktiem ar digitāliem elementiem, kurus tie plāno laist tirgū 2027. gada 11. decembrī vai pēc tam un līdz 2028. gada 11. jūnijam ([31]). Tas attiecas gan uz sertifikātiem un apstiprinājuma lēmumiem, kas izdoti gadījumos, kad piemērojamie Savienības saskaņošanas tiesību akti prasa ražotājam veikt atbilstības novērtēšanas procedūru ar paziņotās struktūras starpniecību, gan uz gadījumiem, kad ražotājs ir brīvprātīgi izvēlējies to darīt.

249. Tādējādi tas, ka saskaņā ar citiem Savienības saskaņošanas tiesību aktiem pastāv derīgs sertifikāts vai apstiprinājuma lēmums, neatbrīvo ražotājus no pienākuma veikt visaptverošu kiberdrošības riska novērtējumu saskaņā ar KNA (nedz arī no citiem KNA noteiktajiem pienākumiem). Tā vietā ražotāji savā atbilstības novērtēšanas procedūrā var izmantot esošos sertifikātus kā atbilstības pierādījumu tiktāl, ciktāl tie jau aptver attiecīgos kiberdrošības riskus. Ja sertifikāts vai apstiprinājuma lēmums saskaņā ar citiem Savienības saskaņošanas tiesību aktiem paliek spēkā pēc 2028. gada 11. jūnija, ražotājs KNA vajadzībām uz šādu sertifikātu vai lēmumu tomēr var paļauties tikai līdz 2028. gada 11. jūnijam.

250. Ja saskaņā ar 13. panta 2. punktu veiktajā kiberdrošības riska novērtējumā ir identificēti papildu riski, ko neaptver kiberdrošības prasības, uz kuru pamata izdots esošais sertifikāts vai apstiprinājuma lēmums, ražotāji joprojām ir atbildīgi par šo risku risināšanu saskaņā ar KNA. Šādos gadījumos atbilstības nodrošināšanai konstatētās nepilnības ir jānovērtē un jāmazina neatkarīgi no esošā sertifikāta vai apstiprinājuma lēmuma turpmāka derīguma.

251. To var ilustrēt ar gadījumu, kad uz produktu ar digitāliem elementiem attiecas kiberdrošības prasības, kas noteiktas Komisijas Deleģētajā regulā (ES) 2022/30, ar ko papildina Direktīvu 2014/53/ES (Radioiekārtu direktīvas (*RED*) deleģētais akts), un uz šo prasību pamata ir izdots ES tipa pārbaudes sertifikāts vai apstiprinājuma lēmums. Šādā gadījumā sertifikāts vai lēmums saskaņā ar 69. panta 1. punktu paliek spēkā attiecībā uz tiem kiberdrošības riskiem, kurus šis sertifikāts aptver un kuri ir saistīti ar Direktīvas 2014/53/ES (Radioiekārtu direktīva jeb "*RED*") kiberdrošības pamatprasībām.

252. Šādos gadījumos ražotājiem KNA vajadzībām nav atkārtoti jānovērtē vai atkārtoti jāpierāda atbilstība attiecībā uz riskiem, kurus jau aptver minētie sertifikāti, kamēr attiecīgais sertifikāts vai apstiprinājuma lēmums paliek spēkā, un jebkurā gadījumā ne ilgāk kā līdz 2028. gada 11. jūnijam. Tas ietver, piemēram, kiberdrošības riskus, kas saistīti ar tīkla vai tā darbības aizsardzību pret kaitējumu, lietotāja un abonenta personas datu un privātuma aizsardzību vai aizsardzību pret krāpšanu (ciktāl minētais sertifikāts šos riskus aptver) un kas ir saistīti ar *RED* kiberdrošības prasībām un atspoguļoti atbilstības novērtēšanā.

253. Tomēr, ja saskaņā ar KNA 13. panta 2. punktu veiktajā kiberdrošības riska novērtējumā ir identificēti papildu kiberdrošības riski, kurus šie sertifikāti neaptver, ražotāji joprojām ir atbildīgi par šo risku risināšanu saskaņā ar KNA. Tie var ietvert, piemēram, riskus, kas saistīti ar ievainojamību novēršanas procesiem, datu minimizēšanu un uzbrukuma laukuma samazināšanu, vai citus konkrētajam produktam raksturīgus kiberdrošības aspektus, kuri nav aplūkoti minētajos sertifikātos vai kurus jebkurā gadījumā neaptver *RED* kiberdrošības pamatprasības.

254. Tādējādi tas, ka saskaņā ar *RED* pastāv derīgs ES tipa pārbaudes sertifikāts vai apstiprinājuma lēmums attiecībā uz pamatprasībām, kas saistītas ar kiberdrošību, pats par sevi nepierāda pilnīgu atbilstību KNA. Tā vietā ražotāji minēto sertifikātu vai lēmumu var izmantot kā atbilstības pierādījumu attiecībā uz konkrētajiem riskiem, vienlaikus nodrošinot, ka visi atlikušie vai no jauna identificētie riski tiek novērtēti un mazināti saskaņā ar KNA.

([31]) Uz produktiem ar digitāliem elementiem, kas laisti tirgū pirms 2027. gada 11. decembra, attiecas Savienības tiesību akti, kuri bija piemērojami to laišanas tirgū brīdī, un, ja tie bija atbilstīgi, tos var pārdot un nodot ekspluatācijā, ja vien 2027. gada 11. decembrī vai pēc tam tajos netiek veiktas būtiskas modifikācijas. Jēdzienus "laist tirgū" un "darīt pieejamu tirgū" skatīt arī šā dokumenta *2.1.* iedaļā *Laišana tirgū*, kā arī zilās rokasgrāmatas 2. nodaļā.

255. Tāpat, ja uz produktu ar digitāliem elementiem attiecas ar kiberdrošību saistītās veselības un drošības pamatprasības, kas noteiktas Regulā (ES) 2023/1230 (Mašīnu regula), kuru pilnībā piemēro no 2027. gada 20. janvāra, un uz šo prasību pamata ir izdots ES tipa pārbaudes sertifikāts vai apstiprinājuma lēmums, minētais sertifikāts vai apstiprinājuma lēmums saskaņā ar KNA 69. panta 1. punktu paliek spēkā attiecībā uz kiberdrošības riskiem, kurus aptver Mašīnu regula.

256. Tas it īpaši attiecas uz kiberdrošības aspektiem, kas saistīti ar aizsardzību pret bojājumiem un vadības sistēmu drošumu un uzticamību, kā noteikts Mašīnu regulas III pielikuma 1.1.9. un 1.2.1. iedaļā. Attiecībā uz minētajiem riskiem ražotājiem KNA vajadzībām nav atkārtoti jānovērtē vai atkārtoti jāpierāda atbilstība, kamēr attiecīgais sertifikāts vai apstiprinājuma lēmums paliek spēkā, un jebkurā gadījumā ne ilgāk kā līdz 2028. gada 11. jūnijam. To piemēro, ja šie riski ir risināti atbilstības novērtēšanā saskaņā ar Mašīnu regulu.

257. Tāpat kā iepriekš minēto *RED* kiberdrošības pamatprasību gadījumā, ja saskaņā ar KNA 13. panta 2. punktu veiktajā kiberdrošības riska novērtējumā ir identificēti papildu kiberdrošības riski, kurus neaptver attiecīgais saskaņā ar Mašīnu regulu izdotais sertifikāts un uz kuriem attiecas minētās regulas ar kiberdrošību saistītās prasības, ražotāji joprojām ir atbildīgi par šo risku risināšanu saskaņā ar KNA.