REPUBLIKA E SHQIPËRISË

Kuvendi

P R O J E K T L I GJ

Nr._____/2026

PËR KËRKESAT E SIGURISË KIBERNETIKE PËR PRODUKTET ME ELEMENTË DIGJITALE DHE QËNDRUESHMËRINË KIBERNETIKE

Në mbështetje të neneve 78, 81, pika 1, dhe 83, pika 1, të Kushtetutës, me propozimin e Këshillit të Ministrave, Kuvendi i Republikës së Shqipërisë

V E N D O S I:

KREU I

DISPOZITA TË PËRGJITHSHME

Neni 1

Objekti

Ky ligj përcakton:

a) rregullat për vendosjen në treg të produkteve me elementë digjital, me qëllim garantimin e sigurisë kibernetike të këtyre produkteve;
b) kërkesat thelbësore të sigurisë kibernetike për projektimin, zhvillimin dhe prodhimin e produkteve me elementë digjital, si dhe detyrimet e operatorëve ekonomikë në lidhje me këto produkte sa i përket sigurisë kibernetike;
c) kërkesat thelbësore të sigurisë kibernetike për proceset e trajtimit të vulnerabiliteteve, të vendosura nga prodhuesit për garantimin e sigurisë kibernetike të produkteve me elementë digjital gjatë periudhës së parashikuar të përdorimit të tyre, si dhe detyrimet e operatorëve ekonomikë në lidhje me këto procese;
ç) rregullat për mbikëqyrjen e tregut, përfshirë monitorimin dhe zbatimin e kërkesave të përcaktuara në këtë nen.

Neni 2

Fusha e zbatimit

1. Ky ligj zbatohet për produktet me elementë digjital që bëhen të disponueshme në treg, të cilat kanë si qëllim përfshirjen e një lidhje të drejtpërdrejtë ose të tërthortë, logjike ose fizike, të të dhënave me një pajisje ose rrjet.

2. Ky ligj nuk zbatohet për produktet me elementë digjital që rregullohen nga legjislacioni në fuqi si vijon:
a) për pajisjet mjekësore sipas ligjit nr. 89/2014 "Për pajisjet mjekësore";
b) për pajisjet mjekësore dhe "*in vitro*"/ ligji nr. 89/2014 "Për pajisjet mjekësore";
c) për automjetet dhe rimorkiot e tyre, si dhe sistemet, përbërësit dhe njësitë teknike të veçanta të destinuara për automjete të tilla, sipas legjislacionit në fuqi për kërkesat e miratimit të tipit në lidhje me sigurinë e tyre të përgjithshme dhe mbrojtjen e pasagjerëve të automjetit dhe përdoruesve të rrugës në nevojë.
3. Ky ligj nuk zbatohet për produktet me elementë digjitale në fushën e aviacionit civil që i nënshtrohen rregullave për kërkesat thelbësore në fushën e aviacionit civil sipas legjislacionit në fuqi të miratuar në përputhje me praktikën e Bashkimit Evropian.
4. Ky ligj nuk zbatohet për pajisjet detare që i nënshtrohen rregullave të veçanta ligjore për kërkesat e sigurisë në det në përputhje me praktikën e Bashkimit Evropian dhe Konventave ndërkombëtare ku Shqipëria aderon.
5. Zbatimi i këtij ligji mund të kufizohet ose të përjashtohet, për produktet me elementë digjital që i nënshtrohen një legjislacioni tjetër përkatës në fuqi, që përcakton kërkesa të lidhura me të gjitha ose disa nga rreziqet e mbuluara nga kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I, të këtij ligji, kur:
a) një kufizim ose përjashtim i tillë është në përputhje me kuadrin e përgjithshëm rregullator që zbatohet për ato produkte; dhe
b) rregullat sektoriale arrijnë të njëjtin nivel ose një nivel më të lartë mbrojtjeje krahasuar me këtë ligj.
Rastet e kufizimit ose përjashtimit të zbatimit sipas kësaj pike, nëse është i nevojshëm, produktet, rregullat përkatëse, si dhe fushëveprimi i kufizimit sipas rastit, miratohen me Vendim të Këshillit të Ministrave.
6. Ky ligj nuk zbatohet për pjesët e këmbimit që bëhen të disponueshme në treg me qëllim zëvendësimin e komponentëve identikë në produktet me elementë digjital, të cilat prodhohen sipas të njëjtave specifikime si komponentët që synojnë të zëvendësojnë.
7. Ky ligj nuk zbatohet për produktet me elementë digjitale të zhvilluara ose të modifikuara ekskluzivisht për qëllime të sigurisë kombëtare, mbrojtjes, ose për produktet e projektuara posaçërisht për përpunimin e informacionit të klasifikuar.
8. Detyrimet e parashikuara në këtë ligj nuk përfshijnë dhënien e informacionit, kur zbulimi i tij është në kundërshtim me interesat thelbësore të sigurisë kombëtare, sigurisë publike ose mbrojtjes së Republikës së Shqipërisë.

Neni 3

Përkufizimet

Për qëllimet e këtij ligji, zbatohen përkufizimet e mëposhtme:

1. "Produkt me elementë digjital" është një produkt softuerik ose harduerik, si dhe zgjidhjet e tij të përpunimit të të dhënave në distancë, përfshirë komponentët softuerikë ose harduerikë që vendosen në treg veçmas.
2. "Përpunim i të dhënave në distancë" është përpunimi i të dhënave në distancë për të cilin softueri është projektuar dhe zhvilluar nga prodhuesi ose nën përgjegjësinë e tij, dhe mungesa e të cilit do të pengonte produktin me elementë digjitale të kryejë një nga funksionet e tij.
3. "Siguri kibernetike" ka të njëjtin kuptim si në ligjin nr. 25/2024 "Për sigurinë kibernetike".
4. "Softuer" është pjesa e një sistemi elektronik të informacionit që përbëhet nga kodi kompjuterik.

5. “Harduer” është një sistem fizik elektronik i informacionit ose pjesë të tij, i aftë për të përpunuar, ruajtur ose transmetuar të dhëna digjitale.
6. “Komponent” është softuer ose harduer i synuar për integrim në një sistem elektronik të informacionit.
7. “Sistem elektronik i informacionit” është një sistem, përfshirë pajisje elektrike ose elektronike, i aftë për të përpunuar, ruajtur ose transmetuar të dhëna digjitale.
8. “Lidhje logjike” është një paraqitje virtuale e lidhjes së të dhënave e realizuar përmes një ndërfaqeje softuerike.
9. “Lidhje fizike” është një lidhje midis sistemeve ose komponentëve elektronikë të informacionit, e realizuar përmes mjeteve fizike, përfshirë ndërfaqe elektrike, optike ose mekanike, tela ose valë radio.
10. “Lidhje indirekte” është një lidhje me një pajisje ose rrjet që nuk ndodh drejtpërdrejt, por realizohet përmes një sistemi më të madh të lidhur drejtpërdrejt me të.
11. “Pikë fundore” është çdo pajisje e lidhur me një rrjet që shërben si pikë hyrëse në atë rrjet.
12. “Operator ekonomik” është prodhuesi, përfaqësuesi i autorizuar, importuesi, shpërndarësi ose çdo person tjetër fizik apo juridik që ka detyrime në lidhje me prodhimin ose bërjen të disponueshme në treg të produkteve me elementë digjital, sipas përcaktimeve të këtij ligji.
13. “Prodhues” është çdo person fizik ose juridik që zhvillon, prodhon ose ka projektuar dhe prodhuar produkte me elementë digjital dhe i tregton ato nën emrin ose markën e tij, qoftë me pagesë, për qëllime fitimi ose pa pagesë.
14. “Mirëmbajtësi i softuerit me burim të hapur” është një person juridik, i ndryshëm nga prodhuesi, që synon të ofrojë mbështetje të qëndrueshme për zhvillimin e produkteve me elementë digjital me burim të hapur, të synuara për përdorim tregtar, dhe që siguron qëndrueshmërinë e tyre.
15. “Përfaqësues i autorizuar” është një person fizik ose juridik i themeluar në Republikën e Shqipërisë, i cili ka marrë një akt të shkruar përfaqësimi nga prodhuesi për të vepruar në emër të tij për detyra specifike.
16. “Importues” është një person fizik ose juridik i themeluar në Republikën e Shqipërisë, i cili vendos në treg një produkt me elementë digjital që mban emrin ose markën e një personi fizik ose juridik të themeluar jashtë tij.
17. “Shpërndarës” është çdo person fizik ose juridik në zinxhirin e furnizimit, përveç prodhuesit ose importuesit, që bën të disponueshëm një produkt në treg me elementë digjital pa ndikuar në karakteristikat e tij.
18. “Konsumator” është çdo person fizik që vepron për qëllime jashtë veprimtarisë tregtare, biznesit, zanatit ose profesionit të tij /ka të njëjtin kuptim sipas ligjit nr. 9902 datë 17.04.2008 “Për mbrojtjen e konsumatorëve” i ndryshuar.
19. “Ndërmarrje mikro, ndërmarrje e vogël dhe ndërmarrje e mesme” ka të njëjtin kuptim si në ligjin nr. 43/2022 “Për zhvillimin e ndërmarrjeve mikro, të vogla dhe mesme”.
20. “Periudhë e mbështetjes” është periudha gjatë së cilës një prodhuesi i kërkohet të sigurojë që vulnerabilitetet e një produkti me elementë digjital të trajtohen në mënyrë efektive dhe në përputhje me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksit I të këtij ligji.
21. “Vendosje në treg” është bërja e disponueshme për herë të parë e produktit me elementë digjitalë në treg.
22. “Bërje e disponueshme e produktit në treg” është çdo furnizim i produktit me elementë digjital në treg për shpërndarje, konsum ose përdorim të tij gjatë një veprimtarie tregtare, me ose pa pagesë.
23. “Qëllim i synuar” është përdorimi i synuar nga prodhuesi për një produkt me elementë digjital, duke përfshirë kontekstin specifik dhe kushtet e përdorimit, siç specifikohet në informacionin e dhënë nga prodhuesi në udhëzimet për përdorim, materialet promovuese ose të shitjes dhe deklaratat, si dhe në dokumentacionin teknik;

24. “Përdorim i parashikueshëm i arsyeshëm” është përdorimi që nuk është domosdoshmërisht qëllimi i synuar i ofruar nga prodhuesi në udhëzimet për përdorim, materialet dhe deklaratat promovuese ose të shitjes, si dhe në dokumentacionin teknik, por që mund të rezultojë nga sjellja njerëzore e parashikueshme në mënyrë të arsyeshme ose veprimet teknike ose ndërveprimet.
25. “Keqpërdorim i parashikueshëm i arsyeshëm” është përdorimi i një produkti me elementë digjital në një mënyrë që nuk është në përputhje me qëllimin e tij të synuar, por që mund të rezultojë nga sjellja e parashikueshme e arsyeshme njerëzore ose ndërveprimi me sisteme të tjera;
26. “ Autoritet notifikues” është autoriteti kombëtar përgjegjës për krijimin dhe kryerjen e procedurave të nevojshme për vlerësimin, caktimin dhe njoftimin e organeve të vlerësimit të konformitetit dhe për monitorimin e tyre.
27. “Vlerësim i konformitetit” është procesi i verifikimit nëse janë përmbushur kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I, të këtij ligji;
28. “Organ i vlerësimit të konformitetit” ka të njëjtin kuptim sipas ligjit nr. 116/2014 “Për akreditimin e organeve të vlerësimit të konformitetit në Republikën e Shqipërisë”, i ndryshuar.
29. “Organ i notifikuar” është organ i vlerësimit të konformitetit i caktuar sipas nenit 43, të këtij ligji dhe legjislacionit përkatës të harmonizuar të Republikës së Shqipërisë në fuqi.
30. “Ndryshim thelbësor” është një ndryshim i produktit me elementë digjitalë pas vendosjes së tij në treg, i cili ndikon në përputhshmërinë e produktit me elementë digjital me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I, të këtij ligji ose që rezulton në një ndryshim të qëllimit të synuar për të cilin është vlerësuar produkti me elementë digjital.
31. “Markimi CE” është markimi, me të cilën prodhuesi tregon se një produkt me elementë digjital dhe proceset e vendosura nga prodhuesi janë në përputhje me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I, të këtij ligji dhe legjislacionin tjetër përkatës në fuqi që parashikon vendosjen e tij.
32. “Legjislacion i harmonizuar” është legjislacioni i Bashkimit Evropian për mbikëqyrjen e tregut dhe konformitetin e produkteve dhe çdo legjislacion tjetër lidhur me tregtimin e produkteve për të cilat zbatohet ky legjislacion.
33. “Struktura përgjegjëse për mbikëqyrjen e tregut” është autoriteti përgjegjës për mbikëqyrjen e tregut siç përcaktohet në legjislacionin në fuqi për mbikëqyrjen e tregut.
34. “Standard ndërkombëtar” ka të njëjtin kuptim si në ligjin nr.9870/2008 “Për standardizimin”, i ndryshuar.
35. “Standard evropian” ka të njëjtin kuptim si në ligjin nr.9870/2008 “Për standardizimin”, i ndryshuar.
36. “Standard i harmonizuar” ka të njëjtin kuptim si në ligjin nr.9870/2008 “Për standardizimin”, i ndryshuar.
37. “Rrezik i sigurisë kibernetike” ka të njëjtin kuptim si në ligjin 25/2024 “Për sigurinë kibernetike”.
38. “Rrezik i rëndësishëm i sigurisë kibernetike” është një rrezik i sigurisë kibernetike i cili, bazuar në karakteristikat e tij teknike, mund të supozohet se ka një probabilitet të lartë për një incident që mund të çojë në një ndikim të rëndë negativ, duke përfshirë shkaktimin e humbjeve ose ndërprerjeve të konsiderueshme materiale ose jomateriale;
39. “Lista e komponentëve të softuerit” është një regjistrim zyrtar që përmban detaje dhe marrëdhëniet e zinxhirit të furnizimit të komponentëve të përfshirë në elementët e softuerit të një produkti me elementë digjital.
40. “Vulnerabilitet” ka të njëjtin kuptim si në ligjin nr. 25/2024 “Për sigurinë kibernetike”.
41. “Vulnerabilitet i shfrytëzueshëm” është një vulnerabilitet që ka potencialin për t'u përdorur në mënyrë efektive nga një aktor keqdashës në kushte praktike operacionale.
42. “Vulnerabilitet i shfrytëzuar aktivisht” është një vulnerabilitet për të cilin ka prova të besueshme se një aktor keqdashës e ka shfrytëzuar atë në një sistem pa lejen e pronarit të sistemit.
43. “Incident” ka të njëjtin kuptim si në ligjin nr. 25/2024 “Për sigurinë kibernetike”.

44. “Incident me ndikim në sigurinë e produktit me elementë digjitalë” është një incident që ndikon negativisht ose është i aftë të ndikojë negativisht në aftësinë e një produkti me elementë digjital për të mbrojtur disponueshmërinë, autenticitetin, integritetin ose konfidencialitetin e të dhënave ose funksioneve.
45. “Incident i shmangur” është një humbje e afërt që nënkupton një ngjarje që mund të kishte kompromentuar disponueshmërinë, autenticitetin, integritetin ose konfidencialitetin e të dhënave të ruajtura, të transmetuara ose të përpunuara ose të shërbimeve të ofruara nga, ose të arritshme nëpërmjet, rrjeteve dhe sistemeve të informacionit, por që u parandalua me sukses nga materializimi ose që nuk u materializua.
46. “Kërcënim kibernetik” ka të njëjtin kuptim si në ligjin nr. 25/2024 “Për sigurinë kibernetike”.
47. “Të dhëna personale” ka të njëjtin kuptim si në ligjin nr. 124/2024 “Për mbrojtjen e të dhënave personale”.
48. “Softuer i lirë dhe me burim të hapur” është softueri, kodi burim i të cilit shpërndahet në mënyrë të hapur dhe që vihet në dispozicion me një licencë të lirë dhe me burim të hapur që parashikon të gjitha të drejtat për ta bërë atë lirishttë aksesueshëm, të përdorshëm, të modifikueshëm dhe të rishpërndarshëm.
49. “Kthim i produktit” është çdo masë për kthimin mbrapsht të produktit, që është bërë i disponueshëm te përdoruesi fundor .
50. “Tërheqje” është çdo masë që synon parandalimin e bërjes së disponueshme në treg të një produkti në zinxhirin e furnizimit;
51. “CSIRT i caktuar si koordinator” është CSIRT Kombëtar sipas ligjit nr. 25/2024 “Për sigurinë kibernetike”.

Neni 4

Lëvizja e lirë

1. Produktet me elementë digjital bëhen të disponueshme në treg dhe vendosen në shërbim vetëm nëse janë në përputhje me kërkesat e këtij ligji.
2. Në panaire, ekspozita, demonstrime ose ngjarje të ngjashme, nuk pengohet prezantimi ose përdorimi i një produkti me elementë digjital që nuk është në përputhje me këtë ligj, duke përfshirë prototipet e tij, me kusht që produkti të paraqitet me një shenjë të dukshme që tregon qartë se nuk është në përputhje me këtë ligj dhe se produkti me elementë digjitalë, nuk do jetë i disponueshëm në treg derisa të përmbushë kërkesat përkatëse.
3. Bërja e disponueshme në treg e softuerit të papërfunduar, që nuk është në përputhje me këtë ligj, nuk do pengohet me kushtin që softueri vihet në dispozicion vetëm për një periudhë të kufizuar kohore të kërkuar per qëllime testimi, me një shenjë të dukshme që tregon qartë se nuk është në përputhje me këtë ligj dhe se nuk do të jetë i disponueshëm në treg për qëllime të tjera përveç testimit.
4. Pika 3 e këtij neni nuk zbatohet për komponentët e sigurisë të parashikuar në legjislacionin tjetër kombëtar, përveç këtij ligji.

Neni 5

Prokurimi ose përdorimi i produkteve me elementë digjitalë

1. Autoritetet publike mund të vendosin kërkesa shtesë të sigurisë kibernetike për prokurimin ose përdorimin e produkteve me elementë digjitalë për qëllime specifike, përfshirë rastet kur këto

produkte prokurohen ose përdoren për qëllime të sigurisë ose mbrojtjes kombëtare, me kusht që këto kërkesa të jenë në përputhje me detyrimet që rrjedhin nga legjislacioni përkatës dhe të jenë të nevojshme dhe proporcionale për arritjen e këtyre qëllimeve.
2. Pa paragjykuar legjislacionin për prokurimin publik, gjatë prokurimit të produkteve me elementë digjitale që bien në fushën e këtij ligji, autoritetet publike sigurojnë të merret parasysh përputhshmëria me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji, përfshirë dhe aftësinë e prodhuesve për të trajtuar në mënyrë efektive vulnerabilitetet.

Neni 6

Kërkesat për produktet me elementë digjitale

Produktet me elementë digjitalë bëhen të disponueshme në treg vetëm kur:

a) Plotësojnë kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij ligji, me kusht që të instalohen, mirëmbahen dhe përdoren siç duhet për qëllimin e tyre të synuar ose në kushte të parashikueshme në mënyrë të arsyeshme, dhe kur është e zbatueshme, të jenë instaluar përditësimet e nevojshme të sigurisë; dhe
b) Proceset e vendosura nga prodhuesi janë në përputhje me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksit I të këtij ligji.

Neni 7

Produkte të rëndësishme me elementë digjitalë

1. Produktet me elementë digjitalë që kanë funksionalitetin thelbësor të një kategorie produkti të përcaktuar në aneksin III të këtij ligji konsiderohen si produkte të rëndësishme me elementë digjitalë dhe i nënshtrohen procedurave të vlerësimit të konformitetit të përcaktuara në pikat 2 dhe 3 të nenit 32 të këtij ligji. Integrimi i një produkti me elementë digjitalë që ka funksionalitetin thelbësor të një kategorie produkti të përcaktuar në aneksin III të këtij ligji nuk e bën produktin në të cilin ai është integruar subjekt të procedurave të vlerësimit të konformitetit të përmendura në pikat 2 dhe 3 të nenit 32 të këtij ligji.
2. Kategoritë e produkteve me elementë digjital të përmendura në pikën 1 të këtij neni, të ndara në klasa I dhe II sipas aneksit III të këtij ligji, plotësojnë të paktën një nga kriteret e mëposhtme:

a) produkti me elementë digjitalë kryen kryesisht funksione kritike për sigurinë kibernetike të produkteve, rrjeteve ose shërbimeve të tjera, përfshirë sigurimin e autentifikimit dhe aksesit, parandalimin dhe zbulimin e ndërhyrjeve, sigurinë e pikave fundore ose mbrojtjen e rrjetit;
b) produkti me elementë digjitalë kryen një funksion që mbart një rrezik të konsiderueshëm për ndikime negative, për sa i përket intensitetit dhe aftësisë për të shkaktuar ndërprerje, kontroll ose dëme në një numër të madh produktesh të tjera ose në shëndetin ose sigurinë e përdoruesve, përmes manipulimit të drejtpërdrejtë, të tilla si një funksion qendror i sistemit duke përfshirë menaxhimin e rrjetit, kontrollin e konfigurimit, virtualizimin ose përpunimin e të dhënave personale.

3. Me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale, Këshilli i Ministrave inicion ndryshimet në aneksin III të këtij ligji, duke përfshirë në listë një kategori të re në secilën klasë të produkteve me elementë digjitalë dhe duke specifikuar përkufizimin e saj, duke zhvendosur një kategori produktesh nga një klasë në tjetrën ose duke tërhequr një kategori ekzistuese nga ajo listë. Gjatë vlerësimit të nevojës për këto ndryshime, merren në konsideratë funksionalitetet

e lidhura me sigurinë kibernetike, ose funksionin dhe nivelin e riskut të sigurisë kibernetike që paraqesin këto produkte, sipas kritereve të përcaktuara në pikën 2 të këtij neni.
4. Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale, sipas pikës 3 të këtij neni miraton, kur është e nevojshme, një periudhë kalimtare minimale prej 12 muajsh, veçanërisht në rastet kur një kategori e re e produkteve të rëndësishme me elementë digjital shtohet në klasën I ose II ose zhvendoset nga klasa I në klasën II në aneksin III të këtij ligji, përpara fillimit të zbatimit të procedurave përkatëse të vlerësimit të konformitetit të përmendura në pikat 2 dhe 3 të nenit 32 të këtij ligji, përveç rasteve kur justifikohet një periudhë më e shkurtër për shkak të urgjencës.
5. Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale, miraton përshkrimet teknike të kategorive të produkteve me elementë digjitalë të mbuluara nga klasat I dhe II të përcaktuara në aneksin III të këtij ligji, si dhe përshkrimi teknik i kategorive të produkteve me elementë digjital të përcaktuara në aneksin IV të këtij ligji.

Neni 8

Produkte kritike me elementë digjitale

1. Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale përcakton se cilat produkte me elementë digjital, që kanë funksionalitetin bërthamë të një kategorie produkti të përcaktuar në aneksin IV të këtij ligji, u kërkohet të marrin një certifikatë të sigurisë kibernetike në nivel sigurie të paktën "i konsiderueshëm", sipas skemës kombëtare të certifikimit të sigurisë kibernetike ose një skeme evropiane të certifikimit të sigurisë kibernetike, për të treguar konformitet me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji ose pjesë të tij, me kusht që një skemë e tillë certifikimi që mbulon atë kategori produktesh me elementë digjital të jetë miratuar dhe të jetë e disponueshme për prodhuesit.
Niveli i kërkuar i sigurisë përcaktohet në mënyrë proporcionale me nivelin e riskut të sigurisë kibernetike të lidhur me produktet me elementë digjitalë dhe merr në konsideratë qëllimin e tyre të synuar, përfshirë varësinë kritike të subjekteve kritike siç parashikohet në aneksin I të ligjit nr. 25/2024 "Për sigurinë kibernetike".
Para miratimit të vendimit, kryhet një vlerësim i ndikimit të mundshëm në treg dhe zhvillohen konsultime me palët e interesuara, përfshirë strukturat përkatëse të certifikimit të sigurisë kibernetike. Vlerësimi merr në konsideratë nivelin e gatishmërisë dhe kapacitetit të autoriteteve dhe tregut për zbatimin e skemës përkatëse të certifikimit.
2. Kur nuk është miratuar vendimi i parashikuar në pikën 1 të këtij neni, produktet me elementë digjital që kanë funksionalitetin bërthamë të një kategorie produkti të përcaktuar në aneksin IV të këtij ligji i nënshtrohen procedurave të vlerësimit të konformitetit të përcaktuara në pikën 3 të nenit 32 të këtij ligji.
3. Vendimi i Këshillit të Ministrave i përmendur në pikën 1 të këtij neni parashikon një periudhë kalimtare minimale prej 6 muajsh, përveç nëse justifikohet një periudhë më e shkurtër kalimtare për arsye të domosdoshme urgjence.
4. Me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale, Këshilli i Ministrave inicion ndryshimet në aneksin IV të këtij ligji, duke shtuar ose tërhequr kategori të produkteve kritike me elementë digjitalë në përputhje me praktikën përkatëse të Bashkimit Evropian. Gjatë përcaktimit të kategorive të tilla të produkteve kritike me elementë digjital dhe nivelit të kërkuar të sigurisë në përputhje me pikën 1 të këtij neni, merren në konsideratë kriteret e përcaktuara në pikën 2 të nenit 7 të këtij ligji dhe sigurohet që kategoritë e produkteve me elementë digjital plotësojnë të paktën një nga kriteret e mëposhtme:

a) ekziston një varësi kritike e subjekteve kritike, siç parashikohet në aneksin I të ligjit nr. 25/2024 “Për sigurinë kibernetike”, në kategorinë e produkteve me elementë digjitalë;
b) incidentet ose vulnerabilitetet e shfrytëzuara në lidhje me këto kategori produktesh me elementë digjitalë mund të çojnë në ndërprerje serioze të zinxhirëve kritikë të furnizimit në treg.

5. Para miratimit të akteve nënligjore të përmendura në këtë nen kryhet një vlerësim i llojit të përmendur në pikën 1 të këtij neni. Akti i përmendur në pikën 1 të këtij neni parashikon një periudhë kalimtare minimale prej 6 muajsh, përveç rasteve kur justifikohet një periudhë më e shkurtër për arsye të domosdoshme urgjence.

Neni 9

Konsultimi me palët e interesuara

1. Gjatë përgatitjes së masave për zbatimin e këtij ligji, autoritetet kompetente konsultohen dhe marrin në konsideratë pikëpamjet e palëve të interesuara, përfshirë autoritetet përkatëse publike, ndërmarrjet e sektorit privat, duke përfshirë mikrondërmarrjet dhe ndërmarrjet e vogla dhe të mesme, komunitetin e softuerit me burim të hapur, shoqatat e konsumatorëve, dhe komunitetin akademik. Në veçanti, konsultimi kryhet në mënyrë të strukturuar, kur është e përshtatshme, në rastet si vijon:
a) për përgatitjen e udhëzimeve të parashikuara në nenin 26 të këtij ligji;
b) për përgatitjen e përshkrimeve teknike të kategorive të produkteve të përcaktuara në aneksin III të këtij ligji, në përputhje me pikën 4 të nenit 7 të këtij ligji, duke vlerësuar nevojën për përditësime të mundshme të listës së kategorive të produkteve në përputhje me pikën 3 të nenit 7 dhe pikën 2 të nenit 8, të këtij ligji, ose për kryerjen e vlerësimit të ndikimit të mundshëm në treg të përmendur në pikën 1 të nenit 8 të këtij ligji;
c) për kryerjen e punës përgatitore për vlerësimin dhe rishikimin e këtij ligji.

2. Autoritetet kompetente organizojnë takime të rregullta konsultimi dhe informimi, të paktën një herë në vit, me qëllim mbledhjen e pikëpamjeve të palëve të interesuara të përmendura në pikën 1 të këtij neni lidhur me zbatimin e këtij ligji.

Neni 10

Rritja e aftësive në një mjedis digjital kibernetik

Për qëllimet e këtij ligji dhe në përgjigje të nevojave të profesionistëve që mbështesin zbatimin e tij, ministria përgjegjëse për ekonominë, mbikëqyrjen e tregut, akreditimin dhe formimin profesional, ministria përgjegjëse për arsimin, ministria përgjegjëse për administratën publike, ministria përgjegjëse për komunikimet elektronike dhe digjitale, dhe Autoriteti Kombëtar për Sigurinë Kibernetike, në bashkëpunim me institucionet përkatëse, promovojnë masa dhe strategji që synojnë:
a) zhvillimin e aftësive në fushën e sigurisë kibernetike dhe krijimin e mjeteve organizative dhe teknologjike për të siguruar disponueshmërinë e mjaftueshme të profesionistëve të kualifikuar, me qëllim mbështetjen e veprimtarisë së strukturave të mbikëqyrjes së tregut dhe organeve të vlerësimit të konformitetit;
b) forcimin e bashkëpunimit midis sektorit privat, operatorëve ekonomikë, duke përfshirë rikualifikimin dhe përmirësimin të aftësive të punonjësve të prodhuesve, konsumatorëve, ofruesve të trajnimeve dhe administratës publike, si dhe zgjerimin e mundësive për të rinjtë për t’u punësuar në sektorin e sigurisë kibernetike.

Neni 11

Siguria e përgjithshme e produktit

Pavarësisht nga sa parashikohet në dispozitat përkatëse të legjislacionit në fuqi për sigurinë e përgjithshme të produkteve, kërkesat dhe parimet e përgjithshme të atij legjislacioni, zbatohen për produktet me elementë digjitale, lidhur me rreziqet ose kategoritë e rreziqeve që nuk mbulohen nga ky ligj, kur këto produkte nuk i nënshtrohen kërkesave specifike të sigurisë të përcaktuara në legjislacionin specifik te harmonizuar, me praktiken e Bashkimit Evropian.

Neni 12

Sistemet e AI me rrezik të lartë

1. Pa paragjykuar kërkesat në lidhje me saktësinë dhe qëndrueshmërinë e përcaktuara në dispozitat përkatëse të legjislacionit në fuqi për inteligjencën artificiale, produktet me elementë digjitale që bien në fushën e këtij ligji dhe që klasifikohen si sisteme AI me rrezik të lartë, në përputhje me dispozitat përkatëse të legjislacionit në fuqi për inteligjencën artificiale, konsiderohen se kanë përmbushur kërkesat e sigurisë kibernetike të përcaktuara në dispozitat përkatëse të legjislacionit në fuqi për inteligjencën artificiale kur:
   a) plotësojnë kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij ligji;
   b) proceset e vendosura nga prodhuesi janë në përputhje me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksit I; dhe
   c) arritja e nivelit të kërkuar të mbrojtjes së sigurisë kibernetike sipas parashikimeve përkatëse të legjislacionit në fuqi për inteligjencën artificiale, demonstrohet në deklaratën e konformitetit në përputhje me standardet e Bashkimit Evropian të lëshuar në përputhje me këtë ligj.
2. Për produktet me elementë digjitale të përmendura në pikën 1 të këtij neni, zbatohet procedura përkatëse e vlerësimit të konformitetit e parashikuar në dispozitat përkatëse të legjislacionit në fuqi për inteligjencën artificiale. Për qëllime të këtij vlerësimi, organet e notifikuara që janë kompetente për vlerësimin e përputhshmërisë së sistemeve AI me rrezik të lartë sipas legjislacionit në fuqi për inteligjencën artificiale janë gjithashtu kompetente për të vlerësuar përputhshmërinë e këtyre sistemeve me kërkesat e këtij ligji, me kusht që përputhshmëria e tyre me kërkesat e nenit 39 të këtij ligji të jetë verifikuar në kuadër të procedurës së njoftimit sipas legjislacionit në fuqi për inteligjencën artificiale.
3. Në përjashtim të pikës 2, produktet e rëndësishme me elementë digjitale të listuara në aneksin III të këtij ligji, të cilat i nënshtrohen procedurave të vlerësimit të konformitetit të parashikuara në nenin 32, pika 2, shkronjat "a" dhe "b", dhe nenin 32, pika 3 të këtij ligji, si dhe produktet kritike me elementë digjitale të listuara në aneksin IV të këtij ligji, për të cilat kërkohet të marrin certifikatë evropiane të sigurisë kibernetike në përputhje me nenin 8, pika 1 të këtij ligji, ose në mungesë të saj i nënshtrohen procedurave të vlerësimit të konformitetit sipas nenit 32, pika 3 të këtij ligji, dhe që klasifikohen si sisteme AI me rrezik të lartë sipas përcaktimeve përkatëse të legjislacionit në fuqi për inteligjencën artificiale, i nënshtrohen procedurave të vlerësimit të konformitetit sipas përcaktimeve të këtij ligji për sa i përket kërkesave thelbësore të sigurisë kibernetike.
4. Prodhuesit e produkteve me elementë digjitale të përmendura në pikën 1 të këtij neni mund të marrin pjesë në sandbox-et rregullatore për inteligjencën artificiale të krijuara sipas legjislacionit shqiptar për inteligjencën artificiale. Pjesëmarrja në sandbox nuk përjashton përmbushjen e kërkesave të këtij ligji lidhur me sigurinë kibernetike dhe procedurat e vlerësimit të konformitetit.

KREU II

DETYRIMET E OPERATORËVE EKONOMIKË DHE DISPOZITAT NË LIDHJE ME SOFTWARE-IN E LIRË DHE ME BURIM TË HAPUR

Neni 13

Detyrimet e prodhuesve

1. Kur vendosin në treg një produkt me elementë digjitalë, prodhuesit sigurojnë që ai të jetë projektuar, zhvilluar dhe prodhuar në përputhje me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij ligji.
2. Për qëllime të përputhshmërisë me pikën 1 të këtij neni, prodhuesit ndërmarrin një vlerësim të risqeve të sigurisë kibernetike që lidhen me një produkt me elementë digjital dhe marrin në konsideratë rezultatin e këtij vlerësimi gjatë fazave të planifikimit, projektimit, zhvillimit, prodhimit, dorëzimit dhe mirëmbajtjes së produktit me elementë digjital me qëllim minimizimin e risqeve të sigurisë kibernetike, parandalimin e incidenteve dhe minimizimin e ndikimit të tyre, duke përfshirë shëndetin dhe sigurinë e përdoruesve.
3. Vlerësimi i riskut të sigurisë kibernetike dokumentohet dhe përditësohet sipas nevojës gjatë një periudhe mbështetjeje që përcaktohet në përputhje me pikën 8 të këtij neni. Ky vlerësim i riskut të sigurisë kibernetike përfshin të paktën një analizë të risqeve të sigurisë kibernetike bazuar në qëllimin e synuar dhe përdorimin e parashikueshëm në mënyrë të arsyeshme, si dhe kushtet e përdorimit të produktit me elementë digjital, të tilla si mjedisi operacional ose asetet që do të mbrohen duke marrë në konsideratë kohëzgjatjen e kohës që produkti pritet të jetë në përdorim. Vlerësimi i riskut të sigurisë kibernetike tregon nëse kërkesat e sigurisë të përcaktuara në pjesën I, pika 2, të aneksit I të këtij ligji janë të zbatueshme për produktin përkatës me elementë digjital dhe si zbatohen këto kërkesa duke u bazuar në vlerësimin e riskut të sigurisë kibernetike. Vlerësimi tregon gjithashtu se si prodhuesi duhet të zbatojë pjesën I, pika 1, të aneksit I të këtij ligji dhe kërkesat e trajtimit të vulnerabilitetit të përcaktuara në pjesën II të aneksit I të këtij ligji.
4. Kur vendos në treg një produkt me elementë digjital, prodhuesi përfshin vlerësimin e riskut të sigurisë kibernetike të përmendur në pikën 3 të këtij neni në dokumentacionin teknik të kërkuar në përputhje me nenin 31 dhe aneksin VII të këtij ligji. Për produktet me elementë digjital të përmendura në nenin 12 të këtij ligji, të cilat gjithashtu i nënshtrohen akteve të tjera ligjore në fuqi, vlerësimi i riskut të sigurisë kibernetike mund të jetë pjesë e vlerësimit të riskut të kërkuar nga ato akte ligjore. Kur disa kërkesa thelbësore të sigurisë kibernetike nuk janë të zbatueshme për produktin me elementë digjital, prodhuesi përfshin një justifikim të qartë për këtë qëllim në dokumentacionin teknik.
5. Për qëllime të përputhshmërisë me pikën 1 të këtij neni, prodhuesit ushtrojnë kujdesin e duhur kur integrojnë komponentët me burim nga palët e treta në mënyrë që ato komponentë të mos kompromentojnë sigurinë kibernetike të produktit me elementë digjital, duke përfshirë integrimin e komponentëve të softuerit të lirë dhe me burim të hapur që nuk janë bërë të disponueshme në treg gjatë një aktiviteti tregtar.
6. Prodhuesit, pas identifikimit të një vulnerabiliteti në një komponent, duke përfshirë një komponent me burim të hapur, i cili është i integruar në produkt me elementë digjital, raportojnë vulnerabilitetin tek personi ose subjekti që prodhon ose mirëmban komponentin si dhe adresojnë dhe korrigjojnë vulnerabilitetin në përputhje me kërkesat e trajtimit të vulnerabilitetit të përcaktuara në pjesën II të aneksit I të këtij ligji. Kur prodhuesit kanë zhvilluar një ndryshim softueri ose hardueri për të adresuar vulnerabilitetin në atë komponent, ata ndajnë kodin ose dokumentacionin përkatës me personin ose entitetin që prodhon ose mirëmban komponentin, kur është e përshtatshme, në një format të lexueshëm nga makina.

7. Prodhuesit dokumentojnë sistematikisht, në një mënyrë proporcionale me natyrën dhe rreziqet e sigurisë kibernetike, aspektet përkatëse të sigurisë kibernetike në lidhje me produktet me elementë digjital, duke përfshirë vulnerabilitetet për të cilat marrin dijeni dhe çdo informacion përkatës të ofruar nga palët e treta dhe, kur është e zbatueshme, përditësojnë vlerësimin e riskut të sigurisë kibernetike të produkteve.
8. Prodhuesit sigurojnë, kur vendosin një produkt me elementë digjital në treg dhe për periudhën e mbështetjes, që vulnerabilitetet e atij produkti, duke përfshirë komponentët e tij, trajtohen në mënyrë efektive dhe në përputhje me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksit I të këtij ligji.
Prodhuesit përcaktojnë periudhën e mbështetjes në mënyrë që të pasqyrojë kohëzgjatjen gjatë së cilës produkti pritet të jetë në përdorim, duke marrë në konsideratë, në veçanti, pritshmëritë e arsyeshme të përdoruesit, natyrën e produktit, duke përfshirë qëllimin e tij të synuar, si dhe legjislacionin përkatës në fuqi që përcakton jetëgjatësinë e produkteve me elementë digjital. Kur përcaktojnë periudhën e mbështetjes, prodhuesit mund të marrin në konsideratë gjithashtu periudhat e mbështetjes së produkteve me elementë digjital që ofrojnë funksionalitet të njëjtë të vendosur në treg nga prodhues të tjerë, disponueshmërinë e mjedisit operativ, periudhat e mbështetjes së komponentëve të integruar që ofrojnë funksione bërthamë me burim nga palët e treta, si dhe udhëzimet përkatëse të ofruara nga grupi i dedikuar i bashkëpunimit administrativ (adCO) të themeluar nga Komisioni Evropian. Çështjet që duhet të merren në konsideratë për të përcaktuar periudhën e mbështetjes konsiderohen në një mënyrë që siguron proporcionalitet.
Pa rënë ndesh me përcaktimet e kësaj pike, periudha e mbështetjes është të paktën pesë vjet. Kur produkti me elementë digjital pritet të jetë në përdorim për më pak se pesë vjet, periudha e mbështetjes korrespondon me kohën e pritshme të përdorimit.
Me vendim të Këshilli i Ministrave miratohet periudha minimale e mbështetjes për kategori specifike të produkteve, kur të dhënat e mbikëqyrjes së tregut sugjerojnë periudha mbështetëse të pamjaftueshme, sipas praktikave përkatëse të Bashkimit Evropian.

Prodhuesit përfshijnë informacionin që është marrë në konsideratë për të përcaktuar periudhën e mbështetjes së një produkti me elementë digjital në dokumentacionin teknik siç përcaktohet në aneksin VII të këtij ligji.
Prodhuesit kanë politika dhe procedura të përshtatshme, duke përfshirë politikat e zbulimit të koordinuar të vulnerabilitetit, sipas përcaktimeve në pikën 5 të pjesës II të aneksit I të këtij ligji, për të procesuar dhe korrigjuar vulnerabilitetet e mundshme në produktin me elementë digjital të raportuara nga burime të brendshme ose të jashtme.
9. Prodhuesit sigurojnë që çdo përditësim sigurie, siç përmendet në pikën 8, të pjesës II, të aneksit I të këtij ligji, i cili është vënë në dispozicion të përdoruesve gjatë periudhës së mbështetjes, të mbetet i disponueshëm pasi të jetë lëshuar për të paktën 10 vjet ose për pjesën e mbetur të periudhës së mbështetjes, nëse kjo e fundit është më e gjatë.
10. Kur një prodhues ka vendosur në treg versione të mëvonshme të ndryshuara në mënyrë thelbësore të një produkti softuerik, ai prodhues mund të sigurojë pajtueshmërinë me kërkesën thelbësore të sigurisë kibernetike të përcaktuar në pikën 2 të pjesës II, të aneksit I të këtij ligji, vetëm për versionin që ka nxjerrë së fundmi në treg, me kusht që përdoruesit e versioneve të hedhura më parë në treg të kenë akses në versionin më të fundit pa pagesë dhe të mos kenë kosto shtesë për të përshtatur mjedisin harduerik dhe softuerik në të cilin përdorin versionin origjinal të atij produkti.
11. Prodhuesit mund të mbajnë arkiva publike të softuerit duke rritur aksesin e përdoruesit në versionet historike. Në këto raste, përdoruesit të informohen qartë në një mënyrë lehtësisht të aksesueshme për rreziqet që lidhen me përdorimin e softuerit të pambështetur.
12. Para se të vendosin në treg një produkt me elementë digjitalë, prodhuesit hartojnë dokumentacionin teknik sipas përcaktimeve në nenin 31 të këtij ligji.

Ata kryejnë procedurat e zgjedhura të vlerësimit të konformitetit, të përmendura në nenin 32 të këtij ligji, ose sigurojnë që këto procedura të kryhen.
Kur përputhshmëria e produktit me elementë digjitalë me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit të I të këtij ligji dhe e proceseve të vendosura nga prodhuesi me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksit të I të këtij ligji është demonstruar nga ajo procedurë e vlerësimit të konformitetit, prodhuesit hartojnë deklaratën e konformitetit në përputhje me standardet e Bashkimit Evropian në përputhje me nenin 28 të këtij ligji dhe vendosin markimin CE në përputhje me nenin 30 të këtij ligji.
13. Prodhuesit mbajnë në dispozicion të strukturave përgjegjëse për mbikëqyrjen e tregut, dokumentacionin teknik dhe deklaratën e konformitetit në përputhje me standardet e Bashkimit Evropian për të paktën 10 vjet pasi produkti me elementë digjitalë të jetë vendosur në treg ose për periudhën e mbështetjes, nëse kjo e fundit është më e gjatë.
14. Prodhuesit sigurojnë që të ekzistojnë procedurat që produktet me elementë digjitalë që janë pjesë e një serie prodhimi të mbeten në përputhje me këtë ligj. Prodhuesit marrin në konsideratë në mënyrë të përshtatshme ndryshimet në procesin e zhvillimit dhe prodhimit ose në projektimin ose karakteristikat e produktit me elementë digjitalë dhe ndryshimet në standardet e harmonizuara, skemën e certifikimit të sigurisë kibernetike kombëtare dhe evropiane ose specifikimet e përbashkëta sipas përcaktimeve në nenin 27 të këtij ligji, ndaj të cilave deklarohet konformiteti i produktit me elementë digjitalë ose me aplikimin e të cilave verifikohet konformiteti i tij.
15. Prodhuesit sigurojnë që produktet e tyre me elementë digjitalë të kenë një tip, grup ose numër serial ose një elementë tjetër që lejon identifikimin e tyre, ose, kur kjo nuk është e mundur, që informacioni të jepet në paketimin e tyre ose në një dokument që shoqëron produktin me elementë digjitalë.
16. Prodhuesit paraqesin emrin, emrin tregtar të regjistruar ose markën tregtare të regjistruar të prodhuesit dhe adresën postare, adresën e emailit ose detaje të tjera digjitale të kontaktit, si dhe, kur është e zbatueshme, faqen e internetit ku mund të kontaktohet prodhuesi, në produktin me elementë digjitalë, në paketimin e tij ose në një dokument që shoqëron produktin me elementë digjitalë. Ky informacion përfshihet gjithashtu në informacionin dhe udhëzimet për përdoruesin sipas përcaktimeve në aneksin II të këtij ligji. Detajet e kontaktit janë në një gjuhë që mund të kuptohet lehtësisht nga përdoruesit dhe strukturat përgjegjëse për mbikëqyrjen e tregut.
17. Për qëllimet e këtij ligji, prodhuesit caktojnë një pikë të vetme kontakti për t'u mundësuar përdoruesve të komunikojnë drejtpërdrejt dhe shpejt me ta, duke përfshirë lehtësimin e raportimit të vulnerabiliteteve të produktit me elementë digjitalë.
Prodhuesit sigurojnë që pika e vetme e kontaktit të jetë lehtësisht e identifikueshme nga përdoruesit, si dhe përfshihet pika e vetme të kontaktit në informacionin dhe udhëzimet për përdoruesin, sipas përcaktimeve në aneksin II të këtij ligji.
Pika e vetme e kontaktit tu mundësojë përdoruesve të zgjedhin mjetet e tyre të preferuara të komunikimit dhe pa i kufizuar këto mjete vetëm në mjete të automatizuara.
18. Prodhuesit sigurojnë që produktet me elementë digjitalë të shoqërohen me informacionin dhe udhëzimet për përdoruesin sipas përcaktimeve në aneksin II të këtij ligji, në formë shkresore ose elektronike. Informacionet dhe udhëzimet të jepen në një gjuhë që mund të kuptohet lehtësisht nga përdoruesit dhe strukturat përgjegjëse për mbikëqyrjen e tregut. Informacionet dhe udhëzimet të jenë të qarta, të kuptueshme dhe të lexueshme gjithashtu të lejojnë instalimin, funksionimin dhe përdorimin e sigurt të produkteve me elementë digjitalë. Prodhuesit mbajnë informacionin dhe udhëzimet për përdoruesin sipas përcaktimeve në aneksin II të këtij ligji në dispozicion të përdoruesve dhe strukturave përgjegjëse për mbikëqyrjen e tregut për të paktën 10 vjet pasi produkti me elementë digjitalë të jetë vendosur në treg ose për periudhën e mbështetjes, cilado qoftë më e gjatë. Kur informacione dhe udhëzime të tilla jepen në internet, prodhuesit sigurojnë që ato të jenë të aksesueshme, lehtësisht të përdorshme dhe të disponueshme në internet për të paktën 10 vjet pasi

produkti me elementë digjitalë të jetë vendosur në treg ose për periudhën e mbështetjes, cilado qoftë më e gjatë.
19. Prodhuesit sigurojnë që data e përfundimit të periudhës së mbështetjes së përmendur në pikën 8 të këtij neni, duke përfshirë të paktën muajin dhe vitin, të specifikohet qartë dhe në mënyrë të kuptueshme në kohën e blerjes, në një mënyrë lehtësisht të aksesueshme dhe, kur është e aplikueshme, në produktin me elementë digjitalë, paketimin e tij ose me mjete digjitale.
Kur është teknikisht e mundur sipas llojit së produktit me elementë digjitalë, prodhuesit shfaqin një njoftim për përdoruesit që i informon ata se produkti i tyre me elementë digjitalë ka arritur fundin e periudhës së tij të mbështetjes.
20. Prodhuesit duhet të japin një kopje të deklaratës së konformitetit në përputhje me standardet e Bashkimit Evropian ose një deklaratë të thjeshtuar të konformitetit në përputhje me standardet e Bashkimit Evropian me produktin me elementë digjitalë. Kur jepet një deklaratë e thjeshtuar e konformitetit në përputhje me standardet e Bashkimit Evropian, ajo përmban adresën e saktë të internetit në të cilën aksesohet deklarata e plotë e konformitetit.
21. Nga momenti i bërjes së disponueshme e produktit në treg dhe për periudhën e mbështetjes, prodhuesit që e dinë ose kanë arsye të besojnë se produkti me elementëë digjitalë ose proceset e vendosura nga prodhuesi nuk janë në konformitet me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji, marrin menjëherë masat korrigjuese të nevojshme që produkti me elementëë digjitalë ose proceset e prodhuesit të jenë në konformitet me këtë ligj, ose të tërhiqet ose të kthehet produkti, sipas rastit.
22. Prodhuesit, me kërkesë të arsyetuar nga struktura përgjegjës për mbikëqyrjen e tregut, i japin autoritetit, të gjithë informacionin dhe dokumentacionin, në formë shkresore ose elektronike në një gjuhë lehtësisht të kuptueshme, të nevojshme për të demonstruar konformitetin e produktit me elementë digjitalë dhe të proceseve të vendosura nga prodhuesi me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji. Prodhuesit bashkëpunojnë me autoritetin përgjegjës për mbikëqyrjen e tregu , me kërkesë të tij, për çdo masë të marrë për të eliminuar rrisqet e sigurisë kibernetike të paraqitura nga produkti me elementë digjitalë që ata kanë vendosur në treg.
23. Një prodhues që ndërpret operacionet e tij dhe, si rezultat, nuk është në gjendje të jetë në përputhje me këtë ligj, informon, përpara se ndërprerja e operacioneve të hyjë në fuqi, strukturat përgjegjëse të mbikëqyrjes së tregut si dhe, me çdo mjet të disponueshëm dhe për aq sa është e mundur, përdoruesit e produkteve përkatëse me elementë digjitalë të vendosura në treg, për ndërprerjen e afërt të operacioneve.
24. Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale miraton formatet dhe elementët e listës së komponentëve të softuerit të materialeve të referuara në pikën 1, të pjesës II, të aneksit I të këtij ligji, në përputhje me praktikat përkatëse të Bashkimit Evropian.

Neni 14

Detyrimet e prodhuesve për raportim

1. Një prodhues njofton njëkohësisht për çdo vulnerabilitet të shfrytëzuar në mënyrë aktive që përmban produkti me elementë digjitalë, për të cilin vihet në dijeni, CSIRT-in Kombëtar, sipas përcaktimeve në pikën 7 të këtij neni, si dhe ENISA-n me anëtarësimin në Bashkimin Evropian. Prodhuesi njofton vulnerabilitetin e shfrytëzuar në mënyrë aktive përmes platformës së vetme të raportimit sipas nenit 16 të këtij ligji, me anëtarësimin në Bashkimin Evropian.
2. Për qëllimet e njoftimit të përmendur në pikën 1 të këtij neni, prodhuesi paraqet:
   a) një njoftim paralajmërues të hershëm për një vulnerabilitet të shfrytëzuar në mënyrë aktive, menjëherë dhe pa vonesë, në çdo rast, brenda 24 orëve nga marrja në dijeni e prodhuesit, duke

treguar, kur është e aplikueshme, me anëtarësimin në BE edhe shtetet anëtare në territorin e të cilave prodhuesi është i vetëdijshëm se produkti i tij me elementë digjitalë është vënë në dispozicion;

b) nëse informacioni përkatës nuk është dhënë tashmë, një njoftim për vulnerabilitetin, menjëherë dhe pa vonesë dhe, në çdo rast, brenda 72 orëve nga marrja e dijenisë së prodhuesit për vulnerabilitetin e shfrytëzuar në mënyrë aktive, i cili ofron informacion të përgjithshëm, sipas disponueshmërisë, për produktin me elementë digjitalë në fjalë, natyrën e përgjithshme të shfrytëzimit dhe vulnerabilitetin në fjalë, si dhe për çdo masë korrigjuese ose zbutëse të marrë dhe masat korrigjuese ose zbutëse që përdoruesit mund të ndërmarrin, dhe që gjithashtu duhet të tregojë, kur është e aplikueshme, se sa sensitiv prodhuesi e konsideron informacionin e njoftuar;

c) nëse informacioni përkatës nuk është dhënë tashmë, një raport përfundimtar, jo më vonë se 14 ditë pasi një masë korrigjuese ose lehtësuese është vënë në dispozicion, duke përfshirë të paktën sa vijon:

i. një përshkrim të vulnerabilitetit, duke përfshirë ashpërsinë dhe ndikimin e tij;

ii. kur është e disponueshme, informacion në lidhje me çdo aktor keqdashës që ka shfrytëzuar ose po shfrytëzon vulnerabilitetin;

iii. detaje rreth përditësimit të sigurisë ose masave të tjera korrigjuese që janë vënë në dispozicion për të korrigjuar vulnerabilitetin.

3. Një prodhues njofton çdo incident të rëndë që ka ndikim në sigurinë e produktit me elementë digjitalë, për të cilin merr dijeni, njëkohësisht CSIRT-in kombëtar, në përputhje me pikën 7 të këtij neni dhe me anëtarësimin në BE ENISA-n. Prodhuesi njofton incidentin përmes platformës së vetme të raportimit të krijuar në përputhje me nenin 16 të këtij ligji me anëtarësimin në BE.

4. Për qëllimet e njoftimit të përmendur në pikën 3 të këtij neni, prodhuesi paraqet:

a) një njoftim paralajmërues të hershëm për një incident të rëndë që ka ndikim në sigurinë e produktit me elementë digjitalë, menjëherë dhe pa vonesë dhe, në çdo rast, brenda 24 orëve nga marrja dijeni e prodhuesit, duke përfshirë të paktën nëse incidenti dyshohet se është shkaktuar nga veprime të paligjshme ose keqdashëse, i cili gjithashtu tregon, kur është e aplikueshme, shtetet anëtare në territorin e të cilave prodhuesi është i vetëdijshëm se produkti i tij me elementë digjitalë është vënë në dispozicion;

b) nëse informacioni përkatës nuk është dhënë tashmë, një njoftim për incidentin, menjëherë dhe pa vonesë dhe, në çdo rast, brenda 72 orëve nga marrja në dijeni e incidentit nga prodhuesi, i cili siguron informacion të përgjithshëm, kur është i disponueshëm, për natyrën e incidentit, një vlerësim fillestar të incidentit, si dhe çdo masë korrigjuese ose lehtësuese të marrë dhe masat korrigjuese ose zbutëse që përdoruesit mund të marrin, dhe që gjithashtu tregon, kur është e aplikueshme, se sa sensitiv prodhuesi e konsideron informacionin e njoftuar;

c) nëse informacioni përkatës nuk është dhënë tashmë, një raport përfundimtar, brenda një muaji pas dorëzimit të njoftimit të incidentit sipas shkronjës “b”, duke përfshirë të paktën sa vijon:

i. një përshkrim të detajuar të incidentit, duke përfshirë ashpërsinë dhe ndikimin e tij;

ii. llojin e kërcënimit ose shkakun rrënjësor që ka të ngjarë të ketë shkaktuar incidentin;

iii. masat e aplikuara dhe të vazhdueshme zbutëse.

5. Për qëllimet e pikës 3 të këtij neni, një incident që ka ndikim në sigurinë e produktit me elementë digjitalë konsiderohet i rëndë kur:

a) ndikon negativisht ose është i aftë të ndikojë negativisht në aftësinë e një produkti me elementë digjitalë për të mbrojtur disponueshmërinë, autenticitetin, integritetin ose konfidencialitetin e funksioneve ose të dhënave të rëndësishme ose sensitive; ose

b) ka çuar ose është në gjendje të çojë në futjen ose ekzekutimin e kodit keqdashës në një produkt me elementë digjitalë ose në rrjetet dhe sistemet e informacionit të një përdoruesi të produktit me elementë digjitalë.

6. Kur është e nevojshme, CSIRT-i kombëtar me marrjen e njoftimit mund t'u kërkojë prodhuesve të japin një raport të ndërmjetëm mbi përditësimet përkatëse të statusit në lidhje me vulnerabilitetin e shfrytëzuar në mënyrë aktive ose incidentin e rëndë që ka ndikim në sigurinë e produktit me elementë digjitalë.
7. Me anëtarësimin në BE, njoftimet e përmendura në pikat 1 dhe 3 të këtij neni dërgohen përmes platformës së vetme të raportimit të përmendur në nenin 16 të këtij ligji.
8. Pasi të bëhet me dije për një vulnerabilitet të shfrytëzuar në mënyrë aktive ose një incident të rëndë që ka ndikim në sigurinë e produktit me elementë digjitalë, prodhuesi informon përdoruesit e prekur të produktit me elementë digjitalë dhe, kur është e përshtatshme, të gjithë përdoruesit, për atë vulnerabilitet ose incident dhe, kur është e nevojshme, për çdo masë zbutëse dhe korrigjuese të rrezikut që përdoruesit mund të përdorin për të zbutur ndikimin e atij vulnerabiliteti ose incidenti, aty ku është e përshtatshme në një format të strukturuar, të lexueshëm elektronikisht dhe lehtësisht të përpunueshëm në mënyrë automatike. Kur prodhuesi nuk informon përdoruesit e produktit me elementë digjitalë në kohën e duhur, CSIRT-ti kombëtar mund t'i japi një informacion të tillë përdoruesve, kur kjo konsiderohet proporcionale dhe e nevojshme për parandalimin ose zbutjen e ndikimit të vulnerabilitetit ose incidentit.
9. Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale miraton formatin dhe procedurat e njoftimeve të përmendura në këtë nen sipas praktikës përkatëse të Bashkimit Evropian.

Neni 15

Raportimi vullnetar

1. Prodhuesit, si dhe persona të tjerë fizikë ose juridikë, mund të njoftojnë çdo vulnerabilitet që një produkt me elementë digjitalë përmban, si dhe kërcënime kibernetike që mund të ndikojnë në profilin e rrezikut të një produkti me elementë digjitalë, në baza vullnetare, tek CSIRT- i kombëtar.
2. Prodhuesit, si dhe persona të tjerë fizikë ose juridikë, mund të njoftojnë çdo incident që ka ndikim në sigurinë e produktit me elementë digjitalë, si dhe incidentet e parandaluara, në baza vullnetare, tek CSIRT-i kombëtar.
3. Me anëtarësimin në BE, CSIRT-i kombëtar përpunon njoftimet e përmendura në pikat 1 dhe 2 të këtij neni në përputhje me procedurën e përcaktuar në nenin 16 të këtij ligji.
CSIRT-i kombëtar mund t'i japë përparësi përpunimit të njoftimeve të detyrueshme ndaj njoftimeve vullnetare.
4. Kur një person fizik ose juridik, i ndryshëm nga prodhuesi, njofton një vulnerabilitet të shfrytëzuar në mënyrë aktive ose një incident të rëndë që ka ndikim në sigurinë e një produkti me elementë digjitalë në përputhje me pikat 1 ose 2 të këtij neni, CSIRT-i kombëtar informon prodhuesin menjëherë.
5. CSIRT-i kombëtar, siguron konfidencialitetin dhe mbrojtjen e duhur të informacionit të dhënë nga një person fizik ose juridik njoftues. Pa paragjykuar parandalimin, hetimin, zbulimin dhe ndjekjen penale të veprave penale, raportimi vullnetar nuk rezulton në vendosjen e detyrimeve shtesë ndaj personit fizik ose juridik njoftues, të cilave nuk do t'u ishte nënshtruar nëse nuk do të kishte bërë njoftimin.

Neni 16

Krijimi i platformës së vetme të raportimit

1. Me anëtarësimin në Bashkimin Evropian, njoftimet e përmendura në pikat 1 dhe 3 të nenit 14 dhe pikat 1 dhe 2 të nenit 15 të këtij ligji, me qëllim thjeshtimin e detyrimit të raportimit të prodhuesve, bëhen në platformën e vetme të raportimit të krijuar nga ENISA.

2. Me anëtarësimin në Bashkimin Evropian, pas marrjes së një njoftimi, CSIRT i caktuar si koordinator që fillimisht merr njoftimin, shpërndan pa vonesë njoftimin përmes platformës së vetme të raportimit tek CSIRT-të e caktuara si koordinatorë në territorin e të cilave prodhuesi ka treguar se produkti me elementë digjitalë është bërë i disponueshëm.
Në rrethana të jashtëzakonshme dhe, në veçanti, me kërkesë të prodhuesit dhe duke marrë në konsideratë nivelin e së informacionit të njoftuar siç tregohet nga prodhuesi sipas shkronjës "a" të pikës 2 të nenit 14, të këtij ligji, shpërndarja e njoftimit mund të vonohet në bazë të arsyeve të justifikuara të lidhura me sigurinë kibernetike për një periudhë kohore të nevojshme, duke përfshirë rastin kur një vulnerabilitet i nënshtrohet një procedure të koordinuar të zbulimit të vulnerabilitetit sipas përcaktimeve në legjislacionin në fuqi për sigurinë kibernetike. Me anëtarësimin në Bashkimin Evropian, kur CSIRT-i vendos të mos e përcjellë një njoftim, informon menjëherë ENISA-in për vendimin dhe jep një arsyetim për mosndarjen e njoftimit, si dhe një tregues se kur do ta shpërndajë njoftimin në përputhje me procedurën e përcaktuar në këtë pikë.

Në rrethana veçanërisht të jashtëzakonshme, kur prodhuesi tregon në njoftimin e përmendur në shkronjën b të pikës 2 të nenit 14 të këtij ligji, se:

a) vulnerabiliteti i njoftuar është shfrytëzuar në mënyrë aktive nga një aktor keqdashës dhe, sipas informacionit të disponueshëm, nuk është shfrytëzuar në asnjë shtet tjetër përveç atij të CSIRT-it të caktuar si koordinator të cilit prodhuesi i ka njoftuar vulnerabilitetin;

b) çdo shpërndarje e menjëhershme e vulnerabilitetit së njoftuar ka gjasa të çojë në dhënien e informacionit, zbulimi i të cilit do të ishte në kundërshtim me interesat thelbësore të atij shteti; ose

c) vulnerabiliteti i njoftuar paraqet një rrezik të afërt të lartë të sigurisë kibernetike që rrjedh nga përhapja e mëtejshme;

vetëm informacioni se është bërë një njoftim nga prodhuesi, informacioni i përgjithshëm për produktin, informacioni mbi natyrën e përgjithshme të shfrytëzimit dhe informacioni që janë ngritur çështje të lidhura me sigurinë duhet të vihen në dispozicion njëkohësisht për ENISA-n derisa njoftimi i plotë të shpërndahet në CSIRT-et përkatëse dhe ENISA.

3. Pas marrjes së një njoftimi për një vulnerabilitet të shfrytëzuar në mënyrë aktive në një produkt me elementë digjitalë ose për një incident të rëndë që ka ndikim në sigurinë e një produkti me elementë digjitalë, CSIRT-i kombëtar u ofron strukturave të mbikëqyrjes së tregut informacionin e njoftuar të nevojshëmpër autoritetet e mbikëqyrjes së tregut për të përmbushur detyrimet e tyre sipas këtij ligji.

4. Kur CSIRT-i kombëtar është vënë në dijeni të një vulnerabiliteti të shfrytëzuar në mënyrë aktive si pjesë e një procedure të koordinuar të zbulimit të vulnerabilitetit, sipas legjislacionit në fuqi për sigurinë kibernetike, me anëtarësimin në BE, CSIRT-i kombëtar pas marrjes së njoftimit mund të vonojë shpërndarjen e njoftimit përkatës nëpërmjet platformës së vetme të raportimit, bazuar në arsye të justifikuara të lidhura me sigurinë kibernetike, për një periudhë që nuk është më e gjatë sesa periudha e nevojshme dhe deri në dhënien e pëlqimit për zbulimin nga palët e përfshira në procedurën e koordinuar të zbulimit të vulnerabilitetit. Kjo kërkesë nuk pengon prodhuesit të njoftojnë vullnetarisht një vulnerabilitet në përputhje me procedurën e përcaktuar në këtë nen.

Neni 17
Dispozita të tjera në lidhje me raportimin

1. Kur ndërgjegjësimi i publikut është i nevojshëm për të parandaluar ose zbutur një incident të rëndë që ka ndikim në sigurinë e produktit me elementë digjitalë ose për të trajtuar një incident të vazhdueshëm, ose nëse nga ana tjetër zbulimi i incidentit është në interes publik, CSIRT-i kombëtar pas konsultimit me prodhuesin përkatës mund të informojë publikun për incidentin ose tí kërkojë prodhuesit informimin e publikut.
2. Autoriteti, në bazë të njoftimeve të marra në përputhje me pikat 1 dhe 3 të nenin 14 dhe pikat 1 dhe 2 të nenin 15 të këtij ligji, përgatit një raport teknik çdo 24 muaj mbi tendencat në zhvillim në lidhje me risqet e sigurisë kibernetike në produktet me elementë digjitalë, dhe me anëtarësimin në Bashkimin Evropian, ia paraqet atë Grupit të Bashkëpunimit të Bashkimit Evropian.
3. Akti i njoftimit në përputhje me pikat 1 dhe 3 të nenit 14 ose pikat 1 dhe 2 të nenit 15 të këtij ligji nuk i bën personin fizik ose juridik njoftues subjekte të përgjegjësisë së shtuar.
4. Pasi të jetë i disponueshëm një përditësim sigurie ose një formë tjetër e masës korrigjuese ose zbutëse, Autoriteti, në marrëveshje me prodhuesin e produktit në fjalë me elementë digjitalë, duhet të shtojë vulnerabilitetin e njohur publikisht, të njoftuar në përputhje me pikën 1 të nenit 14 ose pikën 1 të nenit 15 të këtij ligji, në në regjistrin e vulnerabiliteteve të krijuar në përputhje me pikën 5 të nenit 14 të ligjit nr. 25/2024 "Për sigurinë kibernetike".
5. CSIRT-i kombëtar ofron mbështetje në lidhje me detyrimet e raportimit sipas nenit 14 të këtij ligji për prodhuesit dhe, në veçanti, për prodhuesit që kualifikohen si mikrondërmarrje ose si ndërmarrje të vogla dhe të mesme.

Neni 18

Përfaqësuesit e autorizuar

1. Një prodhues, me një akt të shkruar përfaqësimi, mund të caktojë një përfaqësues të autorizuar.
2. Detyrimet e përcaktuara në pikat 1 deri në 11 të nenit 13, paragrafi i parë i pikës 12 të nenit 13 dhe të pikës 14 të nenit 13 nuk janë pjesë e objektit të aktit të përfaqësimit të përfaqësuesit të autorizuar.
3. Një përfaqësues i autorizuar kryen detyrat e specifikuara në aktin e përfaqësimit të marrë nga prodhuesi. Përfaqësuesi i autorizuar u jep një kopje të aktit të përfaqësimit strukturave përgjegjëse të mbikëqyrjes së tregut, sipas kërkesës. Aktit i përfaqësimit i lejon përfaqësuesit të autorizuar të bëjë të paktën sa vijon:
   a) të mbajë deklaratën e konformitetit në përputhje me standardet e Bashkimit Evropian të përmendur në nenin 28 të këtij ligji dhe dokumentacionin teknik të përmendur në nenin 31 të këtij ligji në dispozicion të strukturave të mbikëqyrjes së tregut për të paktën 10 vjet pasi produkti me elementë digjitalë të jetë vendosur në treg ose për periudhën e mbështetjes, nëse kjo e fundit është më e gjatë;
   b) pas një kërkese të arsyetuar nga një strukturë përgjegjëse për mbikëqyrjen e tregut, t'i sigurojë autoritetit të gjithë informacionin dhe dokumentacionin e nevojshëm për të demonstruar konformitetin e produktit me elementë digjitalë;
   c) të bashkëpunojë me strukturat përgjegjëse për mbikëqyrjen e tregut, me kërkesë të tyre, për çdo veprim të ndërmarrë për të eliminuar risqet e paraqitura nga një produkt me elementë digjitalë të mbuluar nga akti i përfaqësimit i përfaqësuesit të autorizuar.

Neni 19

Detyrimet e importuesve

1. Importuesit vendosin në treg vetëm produkte me elementë digjitalë që përputhen me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij ligji dhe kur proceset e vendosura nga prodhuesi përputhen me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në Pjesën II të aneksit I të këtij ligji.
2. Para se të vendosin një produkt me elementë digjitalë në treg, importuesit sigurojnë që:
   a) procedurat e duhura të vlerësimit të konformitetit të përmendura në nenin 32 të këtij ligji janë kryer nga prodhuesi;
   b) prodhuesi ka hartuar dokumentacionin teknik;
   c) produkti me elementë digjitale mban markimin CE të përmendur në nenin 30 të këtij ligji dhe shoqërohet me deklaratën e konformitetit në përputhje me standardet e Bashkimit Evropian të përmendur në pikën 20 të nenit 13 të këtij ligji dhe informacionin dhe udhëzimet për përdoruesin të përcaktuata në aneksin II të këtij ligji në një gjuhë lehtësisht të kuptueshme nga përdoruesit dhe strukturat përgjegjëse për mbikëqyrjen e tregut;
   ç) prodhuesi ka përmbushur kërkesat e përcaktuara në pikat 15,16 dhe 19 të nenit 13 të këtij ligji.

Për qëllimet e kësaj pike, importuesit janë në gjendje të sigurojnë dokumentet e nevojshme që vërtetojnë përmbushjen e kërkesave të përcaktuara në këtë nen.

3. Kur një importues konsideron ose ka arsye të besojë se një produkt me elementë digjitalë ose proceset e vendosura nga prodhuesi nuk janë në konformitet me këtë ligj, importuesi nuk e vendos produktin në treg derisa ai produkt ose proceset e vendosura nga prodhuesi të kenë arritur konformitetin me këtë ligj. Për më tepër, kur produkti me elementë digjitalë paraqet një rrezik të konsiderueshëm të sigurisë kibernetike, importuesi informon prodhuesin dhe strukturat përgjegjëse për mbikëqyrjen e tregut për këtë qëllim.

Kur një importues ka arsye të besojë se një produkt me elementë digjitalë mund të paraqesë një rrezik të rëndësishëm të sigurisë kibernetike duke konsideruar faktorët e riskut jo-teknikë, importuesi informon strukturat përgjegjëse të mbikëqyrjes së tregut për këtë qëllim. Pas marrjes së informacionit të tillë, strukturat përgjegjëse për mbikëqyrjen e tregut ndjekin procedurat e përmendura në pikën 2 të nenit 51 të këtij ligji.

4. Importuesit tregojnë emrin e tyre, emrin e regjistruar tregtar ose markën tregtare të regjistruar, adresën postare, adresën e emailit ose kontaktet e tjera digjitale, si dhe, kur është e aplikueshme, faqen e internetit në të cilën mund të kontaktohen për produktin me elementë digjitalë ose në paketimin e tij ose në një dokument që shoqëron produktin me elementë digjitalë. Detajet e kontaktit të jenë në një gjuhë lehtësisht të kuptueshme nga përdoruesit dhe strukturat përgjegjëse për mbikëqyrjen e tregut.
5. Importuesit që kanë dijeni ose kanë arsye të besojnë se një produkt me elementëë digjitalë që ata kanë vendosur në treg nuk është në konformitet me këtë ligj, marrin menjëherë masat korrigjuese të nevojshme për të siguruar që produkti me elementë digjitalë të arrijë konformitetin me këtë ligj, ose që produkti të tërhiqet ose të kthehet, nëse është e përshtatshme.

Pasi marrin dijeni për një vulnerabilitet në produkt me elementë digjitalë, importuesit duhet të informojnë prodhuesin menjëherë për atë vulnerabilitet. Për më tepër, kur produkti me elementë digjitalë paraqet një rrezik të rëndësishëm të sigurisë kibernetike, importuesit informojnë menjëherë strukturat përgjegjëse për mbikëqyrjen e tregut në të cilat e kanë bërë të disponueshëm në treg produktin me elementë digjitalë për këtë qëllim, duke dhënë detaje, në veçanti, për moskonformitetin dhe për çdo masë korrigjuese të marrë.

6. Importuesit, për të paktën 10 vjet pasi produkti me elementë digjitale është vendosur në treg ose për periudhën e mbështetjes, nëse kjo e fundit është më e gjatë, duhet të mbajnë një kopje të deklaratës së konformitetit në përputhje me standardet e Bashkimit Evropian në dispozicion të strukturave përgjegjëse për mbikëqyrjen e tregut dhe të sigurojnë që dokumentacioni teknik të mund t'u vihet në dispozicion autoriteteve, sipas kërkesës.
7. Importuesit, pas një kërkese të arsyetuar nga struktura përgjegjëse për mbikëqyrjen e tregut, i japin të gjithë informacionin dhe dokumentacionin, në formë letre ose elektronike, të nevojshëme për të demonstruar konformitetin e produktit me elementë digjitalë me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij ligji, si dhe të proceseve të vendosura nga prodhuesi me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksit I të këtij ligji në një gjuhë që mund të jetë lehtësisht e kuptuar nga strukturat. Ata bashkëpunojnë me strukturat, me kërkesë të tij, për çdo masë të marrë për të eliminuar risqet e sigurisë kibernetike të paraqitura nga një produkt me elementë digjitalë, të cilin ata e kanë vendosur në treg.
8. Kur importuesi i një produkti me elementë digjitalë merr dijeni se prodhuesi i atij produkti ka ndërprerë operacionet e tij dhe, si rezultat, nuk është në gjendje të përmbushë detyrimet e përcaktuara në këtë ligj, importuesi informon strukturat përgjegjëse të mbikëqyrjes së tregut për këtë situatë, si dhe, me çdo mjet në dispozicion dhe për aq sa është e mundur, përdoruesit e produkteve me elementë digjitalë të vendosura në treg.

Neni 20

Detyrimet e shpërndarësve

1. Kur bëjnë të disponueshëm në treg një produkt me elementë digjitalë, shpërndarësit duhet të veprojnë me kujdesin e duhur në lidhje me kërkesat e përcaktuara në këtë ligj.
2. Para se të bëjnë të disponueshëm një produkt në treg me elementë digjitalë, shpërndarësit duhet të verifikojnë se:
   a) produkti me elementë digjitalë mban markën CE;
   b) prodhuesi dhe importuesi kanë përmbushur detyrimet e përcaktuara në pikat 15, 16, 18, 19 dhe 20 të nenit 13 dhe në pikën 4 të nenit 19 të këtij ligji dhe i kanë mundësuar të gjitha dokumentet e nevojshme shpërndarësit.
3. Kur një shpërndarës konsideron ose ka arsye të besojë, në bazë të informacionit që zotëron, se një produkt me elementë digjitalë ose proceset e vendosura nga prodhuesi nuk janë në konformitet me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji, shpërndarësi e bën të disponueshëm në treg produktin me elementë digjitalë derisa produkti ose proceset e vendosura nga prodhuesi të kenë arritur konformitetin me këtë ligj. Për më tepër, kur produkti me elementë digjitalë paraqet një rrezik të konsiderueshëm të sigurisë kibernetike, shpërndarësi informon, menjëherë, prodhuesin dhe strukturat përgjegjëse për mbikëqyrjen e tregut për këtë qëllim.
4. Shpërndarësit që kanë dijeni ose kanë arsye të besojnë, në bazë të informacionit që zotërojnë, se një produkt me elementë digjitalë që ata e kanë bërë të disponueshëm në treg, ose proceset e vendosura nga prodhuesi i tij nuk janë në konformitet me këtë ligj, sigurohen që janë marrë masat korrigjuese të nevojshme për ta sjellë atë produkt me elementë digjitalë ose proceset e vendosura nga prodhuesi i tij në konformitet, ose për ta tërhequr ose për ta kthyer produktin, nëse është e përshtatshme.
Me marrjen dijeni për një vulnerabilitet në produktin me elementë digjitalë, shpërndarësit informojnë me njëherë prodhuesin për vulnerabilitin. Për më tepër, kur produkti me elementë digjitalë paraqet një rrezik të konsiderueshëm të sigurisë kibernetike, shpërndarësit informojnë menjëherë strukturat

përgjegjëse për mbikëqyrjen e tregut, duke dhënë detaje, në veçanti, për mospërputhjen dhe për çdo masë korrigjuese të marrë.
5. Shpërndarësit, pas një kërkese të arsyetuar nga një strukturë përgjegjës për mbikëqyrjen e tregut, japin të gjithë informacionin dhe dokumentacionin, në formë shkresore ose elektronike, të nevojshëm për të demonstruar konformitetin e produktit me elementë digjitalë dhe proceset e vendosura nga prodhuesi i tij me këtë ligj në një gjuhë që mund të kuptohet lehtësisht nga strukturat. Ata bashkëpunojnë me strukturat, me kërkesë të tij, për çdo masë të marrë për të eliminuar risqet e sigurisë kibernetike të paraqitura nga një produkt me elementë digjitalë të cilin ata e kanë bërë të disponueshëm në treg.
6. Kur shpërndarësi i një produkti me elementëë digjitalë merr dijeni, në bazë të informacionit në posedim të tij, se prodhuesi i atij produkti ka ndërprerë operacionet e tij dhe, si rezultat, nuk është në gjendje të përmbushë detyrimet e përcaktuara në këtë ligj, shpërndarësi informon me njëherë strukturat përgjegjëse të mbikëqyrjes së tregut për këtë situatë, si dhe, me çdo mjet në dispozicion dhe për aq sa është e mundur, përdoruesit e produkteve me elementë digjitalë të vendosura në treg.

Neni 21

Rastet në të cilat detyrimet e prodhuesve zbatohen për importuesit dhe shpërndarësit

Një importues ose shpërndarës konsiderohet si prodhues për qëllimet e këtij ligji dhe është subjekt i zbatimit të neneve 13 dhe 14, kur ai importues ose shpërndarës vendos një produkt me elementë digjitalë në treg nën emrin ose markën e tij tregtare ose kryen një modifikim thelbësor të një produkti me elementë digjitalë tashmë të vendosur në treg.

Neni 22

Raste të tjera në të cilat zbatohen detyrimet e prodhuesve

1. Një person fizik ose juridik, përveç prodhuesit, importuesit ose shpërndarësit, që kryen një modifikim thelbësor të një produkti me elementë digjitalë dhe e bën atë produkt të disponueshëm në treg, konsiderohet prodhues për qëllimet e këtij ligji.
2. Personi i përmendur në pikën 1 të këtij neni i nënshtrohet detyrimeve të përcaktuara në nenet 13 dhe 14 të këtij ligji për pjesën e produktit me elementë digjitalë që preket nga modifikimi thelbësor ose, nëse modifikimi thelbësor ka ndikim në sigurinë kibernetike të produktit me elementë digjitalë në tërësi, për të gjithë produktin.

Neni 23

Identifikimi i operatorëve ekonomikë

1. Operatorët ekonomikë, sipas kërkesës, u japin strukturave përgjegjëse për mbikëqyrjen e tregut informacionin e mëposhtëm:
   a) emrin dhe adresën e çdo operatori ekonomik që i ka furnizuar me një produkt me elementë digjitalë;
   b) kur është e disponueshme, emrin dhe adresën e çdo operatori ekonomik të cilin e kanë furnizuar me një produkt me elementë digjitalë.

2. Operatorët ekonomikë duhet të jenë në gjendje të paraqesin informacionin e përmendur në pikën 1 të këtij neni për 10 vjet pasi të jenë furnizuar me produktin me elementë digjitalë dhe për 10 vjet pasi të kenë furnizuar produkte me elementë digjitalë.

Neni 24

Detyrimet e mirëmbajtësve të softuerit me burim të hapur

1. Mirëmbajtësit e softuerit me burim të hapur vendosin dhe dokumentojnë në një mënyrë të verifikueshme një politikë të sigurisë kibernetike për të nxitur zhvillimin e një produkti të sigurt me elementë digjitalë, si dhe një trajtim efektiv të vulnerabiliteteve nga zhvilluesit e atij produkti. Kjo politikë gjithashtu nxit raportimin vullnetar të vulnerabiliteteve siç përcaktohet në nenin 15 nga zhvilluesit e atij produkti dhe merr parasysh natyrën specifike të mirëmbajtësit të softuerit me burim të hapur dhe marrëveshjet ligjore dhe organizative të cilave ai i nënshtrohet. Kjo politikë, në veçanti, përfshin aspekte që lidhen me dokumentimin, adresimin dhe korrigjimin e vulnerabiliteteve dhe promovon ndarjen e informacionit në lidhje me vulnerabilitetet e zbuluara brenda komunitetit me burim të hapur.
2. Mirëmbajtësit e softuerit me burim të hapur bashkëpunojnë me strukturat përgjegjëse për mbikëqyrjen e tregut, me kërkesën e tyre, me qëllim zbutjen e risqeve të sigurisë kibernetike të paraqitura nga një produkt me elementë digjitalë që kualifikohen si softuer i lirë dhe me burim të hapur. Pas një kërkese të arsyetuar nga një strukturë përgjegjëse e mbikëqyrjes së tregut, mirëmbajtësit e softuerit me burim të hapur i japin strukturës, në një gjuhë që mund të kuptohet lehtësisht nga struktura, dokumentacionin e përmendur në pikën 1të këtij neni, në formë shkresore ose elektronike.
3. Detyrimet e përcaktuara në pikën 1 të nenit 14 zbatohen për mirëmbajtësit e softuerit me burim të hapur në masën që ata janë të përfshirë në zhvillimin e produkteve me elementë digjitalë. Detyrimet e përcaktuara në pikat 3 dhe 8 të nenit 14 zbatohen për mirëmbajtësit e softuerit me burim të hapur në masën që incidentet e rënda që kanë ndikim në sigurinë e produkteve me elementë digjitalë ndikojnë në sistemet e rrjetit dhe informacionit të ofruara nga mirëmbajtësit e softuerit me burim të hapur për zhvillimin e produkteve të tilla.

Neni 25
Vërtetimi i sigurisë së softuerit të lirë dhe me burim të hapur

Për të lehtësuar përmbushjen e detyrimit të kujdesit të duhur të përcaktuar në pikën 5 të neni 13, veçanërisht në lidhje me prodhuesit që integrojnë komponentë të softuerit të lirë dhe me burim të hapur në produktet e tyre me elementë digjitalë, Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale miraton programe vullnetare të vërtetimit të sigurisë. Këto programe vullnetare të vërtetimit të sigurisë u mundësojnë zhvilluesve ose përdoruesve të produkteve me elementë digjitalë që kualifikohen si softuer i lirë dhe me burim të hapur, si dhe palë të treta të tjera, të vlerësojnë konformitetin e këtyre produkteve me të gjitha ose me një pjesë të kërkesave thelbësore të sigurisë kibernetike ose detyrimeve të tjera të përcaktuara në këtë ligj.

Neni 26

Udhëzimet

1. Për të lehtësuar dhe për të siguruar konsistencën e zbatimit të ligjit, ministri përgjegjës për ekonominë dhe ministri përgjegjës për digjitalizimin, duke konsideruar edhe sugjerimet e autoritetit përgjegjës për sigurinë kibernetike dhe autoritetit përgjegjës për qeverisjen elektronike, miratojnë udhëzime të përbashkëta për të ndihmuar operatorët ekonomikë në zbatimin e këtij ligji, me fokus të veçantë në lehtësimin e pajtueshmërisë nga mikrondërmarrjet dhe ndërmarrjet e vogla dhe të mesme.
2. Për qëllim të ofrimit të këtyre udhëzimeve sipas pikës 1 të këtij neni, ministri përgjegjës trajton të paktën aspektet e mëposhtme:
   a) fushëveprimin e këtij ligji, me fokus të veçantë në zgjidhjet e përpunimit të të dhënave në distancë dhe softuerin e lirë dhe me burim të hapur;
   b) aplikimin e periudhave të mbështetjes në lidhje me kategori të veçanta produktesh me elementë digjitalë;
   c) udhëzimet e synuara për prodhuesit që i nënshtrohen këtij ligji dhe që janë gjithashtu subjekt i legjislacionit tjetër përkatës në fuqi;
   ç) koncepti i modifikimit thelbësor.
3. Gjatë përgatitjes së udhëzimeve sipas këtij neni, ministri përgjegjës konsultohet me palët përkatëse të interesit.

KREU III

KONFORMITETI I PRODUKTIT ME ELEMENTË DIGJITALE

Neni 27

Prezumimi i konformitetit

1. Produktet me elementë digjitalë dhe proceset e vendosura nga prodhuesi që janë në konformitet me standardet e harmonizuara ose pjesë të tyre, referencat e të cilave janë botuar në Fletoren Zyrtare, prezumohen të jenë në konformitet me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji, të mbuluara nga ato standarde ose pjesë të tyre.
Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale miraton lista me standardet e harmonizuara, në përputhje me standardet përkatëse Evropiane të harmonizuara, për kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji.
2. Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale miraton specifikime të përbashkëta që mbulojnë kërkesat teknike që ofrojnë një mjet për të përmbushur kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I për produktet me elementë digjitalë që bien në fushën e këtijj ligji, në përputhje me praktikën përkatëse të Komisionit Evropian.
3. Produktet me elementë digjitalë dhe proceset e vendosura nga prodhuesi që janë në konformitet me specifikimet e përbashkëta të përcaktuara nga aktet të përmendura në pikën 2 të këtij neni, ose pjesë të tyre, prezumohen të jenë në konformitet me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të mbuluara nga ato specifikime të përbashkëta ose pjesë të tyre.
4. Produktet me elementë dhe procese digjitale të vendosura nga prodhuesi për të cilat është lëshuar një deklaratë konformiteti në përputhje me standardet e Bashkimit Evropian ose certifikatë sipas skemës të certifikimit të sigurisë kibernetike të miratuar në zbatim të legjislacionit në fuqi për

sigurinë kibernetike si dhe një skeme evropiane të certifikimit të sigurisë kibernetike prezumohen të jenë në konformitet me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji për aq sa deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian ose certifikata e sigurisë kibernetike, ose pjesë të tyre, mbulojnë ato kërkesa.
5. Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale , specifikon skemat e certifikimit të sigurisë kibernetike të miratuara që mund të përdoren për të treguar konformitetin e produkteve me elementë digjitalë me kërkesat thelbësore të sigurisë kibernetike ose pjesët e tyre siç përcaktohet në aneksin I të këtijj ligji. Lëshimi i një certifikate të sigurisë kibernetike të lëshuar sipas këtyre skemave, në të paktën në nivelin e sigurisë 'të konsiderueshëm', eliminon detyrimin e një prodhuesi për të kryer një vlerësim të konformitetit të palëve të treta për kërkesat përkatëse, siç përcaktohet në shkronjat “a” dhe “b” të pikës 2 të nenit 32,dhe shkronjat “a” dhe “b” të pikës 3 të nenit 32 të këtij ligji.

Neni 28

Deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian

1. Deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian hartohet nga prodhuesit në përputhje me pikën 12 të nenit 13 të këtij ligji dhe deklaron se është treguar përmbushja e kërkesave thelbësore të sigurisë kibernetike të zbatueshme të përcaktuara në aneksin I të këtij ligji.
2. Deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian ka strukturën e modelit të përcaktuar në aneksin V dhe përmban elementët e specifikuar në procedurat përkatëse të vlerësimit të konformitetit të përcaktuara në aneksin VIII të këtij ligji. Deklarata përditësohet sipas rastit dhe vihet në dispozicion në gjuhën shqipe Deklarata e thjeshtuar e konformitetit në përputhje me standardet e Bashkimit Evropian e përmendur në pikën 20 të nenit 13 të këtij ligji ka strukturën model të përcaktuar në aneksin VI të këtij ligji. Ai vihet në dispozicion në gjuhën shqipe.
3. Kur një produkt me elementë digjitale është subjekt i një ose më shumë akteve ligjore që kërkojnë një deklaratë të konformitetit në përputhje me standardet e Bashkimit Evropian, hartohet një deklaratë e konformitetit e vetme në zbatim të të gjitha këtyre akteve ligjore. Deklarata përmban listën e akteve ligjore në fjalë, duke përfshirë referencat e publikimit të tyre.
4. Përmes hartimit të deklaratës të konformitetit në përputhje me standardet e Bashkimit Evropian, prodhuesi merr përgjegjësinë për konformitetin e produktit me elementë digjitale.
5. Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale miraton elementë shtesë në përmbajtjen minimale të deklaratës ë konformitetit në përputhje me standardet e Bashkimit Evropian, përcaktuar në aneksin V të këtij ligji, për të marrë në konsideratë zhvillimet teknologjike në përputhje me praktikën përkatëse të Bashkimit Evropian.

Neni 29

Parimet e përgjithshme të markimit CE

Markimi CE i nënshtrohet parimeve të përgjithshme të përcaktuara sipas legjislacionit në fuqi për akreditimin lidhur me reklamimin e produkteve.

Neni 30

Rregullat dhe kushtet për vendosjen e markimit CE

1. Markimi CE vendoset në mënyrë të dukshme, të lexueshme dhe të përhershme në produkt me elementë digjitalë. Kur kjo nuk është e mundur ose nuk garantohet për shkak të natyrës së produktit me elementë digjitalë, ajo vendoset në paketim dhe në deklaratën e konformitetit në përputhje me standardet e Bashkimit Evropian përmendur në nenin 28 të këtij ligji që shoqëron produktin me elementë digjitalë. Për produktet me elementë digjitalë që janë në formën e softuerit, markimi CE vendoset ose në deklaratën konformitetit në përputhje me standardet e Bashkimit Evropian përmendur në nenin 28 të këtij ligji ose në faqen e internetit që shoqëron produktin softuerik. Në rastin e fundit, seksioni përkatës i faqes së internetit të jetë lehtësisht dhe drejtpërdrejt i aksesueshëm për konsumatorët.
2. Për shkak të natyrës së produktit me elementë digjitalë, lartësia e markimit CE e vendosur në produkt me elementë digjitalë mund të jetë më e ulët se 5 mm, me kusht që të mbetet e dukshme dhe e lexueshme.
3. Markimi CE vendoset përpara se produkti me elementë digjitalë të vendoset në treg. Ai mund të pasohet nga një ikonë (piktogram) ose ndonjë shenjë tjetër që tregon një rrezik ose përdorim të veçantë të sigurisë kibernetike të përcaktuar në aktet nënligjore të përmendura në pikën 6 të këtij neni.
4. Markimi CE pasohet nga numri i identifikimit të organit të notifikuar, kur ai organ është i përfshirë në procedurën e vlerësimit të konformitetit bazuar në sigurimin e plotë të cilësisë (bazuar në modulin H të aneksit VIII të këtij ligji) të përmendur në nenin 32 të këtij ligji.
Numri i identifikimit të organit të notifikuar vendoset nga vetë organi ose, sipas udhëzimeve të tij, nga prodhuesi ose përfaqësuesi i autorizuar i prodhuesit.
5. Vendosja e markimit CE në produkte me elementë digjital bazohet në mekanizmat ekzistues për të siguruar zbatimin e saktë të regjimit që rregullon markimin CE dhe ndërmerren veprimet e duhura në rast të përdorimit jo të duhur të asaj marke. Kur produkti me elementë digjitale i nënshtrohet legjislacionit tjetër, përveç këtij ligji, i cili parashikon gjithashtu vendosjen e markimit CE, markimi CE tregon se produkti gjithashtu përmbush kërkesat e përcaktuara në legjislacionin tjetër përkatës në fuqi.
6. Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale miraton specifikime teknike për etiketat, ikonat (piktogramet) ose çdo markë tjetër që lidhet me sigurinë e produkteve me elementë digjitale, periudhat e mbështetjes së tyre dhe mekanizmat për të promovuar përdorimin e tyre dhe për të rritur ndërgjegjësimin e publikut për sigurinë e produkteve me elementë digjitale.

Neni 31

Dokumentacioni teknik

1. Dokumentacioni teknik përmban të gjitha të dhënat përkatëse ose detajet e mjeteve të përdorura nga prodhuesi për të siguruar që produkti me elementë digjitalë dhe proceset e vendosura nga prodhuesi të jenë në përputhje me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji. Dokumentacioni teknik përmban të paktën elementët e përcaktuar në aneksin VII të këtij ligji.

2. Dokumentacioni teknik hartohet përpara se produkti me elementë digjitalë të vendoset në treg dhe përditësohet vazhdimisht, kur është e përshtatshme, të paktën gjatë periudhës së mbështetjes.
3. Për produktet me elementë digjitale të përmendura në nenin 12 të këtij ligji, të cilat janë gjithashtu subjekt i akteve ligjore të tjera në fuqi që parashikojnë dokumentacion teknik, hartohet një grup i vetëm dokumentacioni teknik që përmban informacionin e përmendur në aneksin VII të këtij ligji dhe informacionin e kërkuar nga këto akte ligjore.
4. Dokumentacioni teknik dhe korrespondenca në lidhje me çdo procedurë të vlerësimit të konformitetit hartohen në një gjuhë shqipe.
5. Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale miraton elementët shtesë për tu përfshirë në dokumentacionin teknik të përcaktuar në aneksin VII të këtij ligji duke marrë në konsideratë zhvillimet teknologjike, si dhe zhvillimet e hasura në procesin e zbatimit të këtij ligji. Për këtë qëllim, Këshillit i Ministrave siguron që barra administrative për mikrondërmarrjet dhe ndërmarrjet e vogla dhe të mesme të jetë proporcionale.

Neni 32

Procedurat e vlerësimit të konformitetit për produktet me elementë digjitale

1. Prodhuesi kryen vlerësimin e konformitetit të produktit me elementë digjitalë dhe proceseve të vendosura nga prodhuesi për të përcaktuar nëse plotësohen kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji. Prodhuesi tregon konformitet me kërkesat thelbësore të sigurisë kibernetike duke përdorur një nga procedurat e mëposhtme:
   a) procedurën e kontrollit të brendshëm (bazuar në modulin A) të përcaktuar në aneksin VIII të këtij ligji;
   b) procedurën e ekzaminimit të tipit të BE-së (bazuar në modulin B) të përcaktuar në aneksin VIII të këtij ligji të ndjekur nga konformiteti me llojin e BE-së bazuar në kontrollin e brendshëm të prodhimit (bazuar në modulin C) të përcaktuar në aneksin VIII të këtij ligji;
   c) vlerësimin e konformitetit bazuar në sigurimin e plotë të cilësisë (bazuar në modulin H) të përcaktuar në aneksin VIII të këtij ligji; ose
   ç) aty ku është e disponueshme dhe e aplikueshme, një skemë e certifikimit të sigurisë kibernetike në përputhje me pikën 9 të nenit 27 të këtij ligji.
2. Kur në vlerësimin e përputhshmërisë së një produkti të rëndësishëm me elementë digjitalë që bie në klasën I siç përcaktohet në aneksin III të këtij ligji dhe proceset e vendosura nga prodhuesi i tij me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji, prodhuesi nuk ka aplikuar ose ka aplikuar vetëm pjesërisht standarde të harmonizuara, specifikime të përbashkëta ose skema të certifikimit të sigurisë kibernetike në nivel sigurie të paktën "të konsiderueshëm" siç përmendet në neni 27 të këtij ligji, ose kur standarde të tilla të harmonizuara, specifikime të përbashkëta ose skema të certifikimit të sigurisë kibernetike nuk ekzistojnë, produkti me elementë digjitalë dhe proceset e vendosura nga prodhuesi vlerësohen në lidhje me ato kërkesa thelbësore të sigurisë kibernetike sipas njërës nga procedurat e mëposhtme:
   a) procedurës së ekzaminimit të tipit të BE-së (bazuar në modulin B) të përcaktuar në aneksin VIII të këtij ligji e ndjekur nga konformiteti me llojin e BE-së bazuar në kontrollin e brendshëm të prodhimit (bazuar në modulin C) të përcaktuar në aneksin VIII të këtij ligji;
   b) një vlerësim i konformitetit bazuar në sigurimin e plotë të cilësisë (bazuar në modulin H) të përcaktuar në aneksin VIII të këtij ligji.
3. Kur produkti është një produkt i rëndësishëm me elementë digjitalë që bie në klasën II siç përcaktohet në aneksin III të këtij ligji, prodhuesi tregon konformitet me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji duke përdorur një nga procedurat e mëposhtme:

a) procedura e ekzaminimit të tipit të BE-së (bazuar në modulin B) e përcaktuar në aneksin VIII të këtij ligji e ndjekur nga konformiteti me llojin e BE-së bazuar në kontrollin e brendshëm të prodhimit (bazuar në modulin C) të përcaktuar në aneksin VIII të këtij ligji;
b) një vlerësim i konformitetit bazuar në sigurimin e plotë të cilësisë (bazuar në modulin H) të përcaktuar në aneksin VIII të këtij ligji;
c) aty ku është e disponueshme dhe e zbatueshme, një skemë e certifikimit të sigurisë kibernetike në përputhje me pikën 9 të nenit 27 të këtij ligji në nivel sigurie të paktën 'të konsiderueshëm' në përputhje ligjislacionin në fuqi për sigurinë kibernetike.

4. Produktet kritike me elementë digjitalë të listuar në aneksin IV të këtij ligji tregojnë konformitet me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji duke përdorur një nga procedurat e mëposhtme:
a) një skemë të certifikimit të sigurisë kibernetike në përputhje me pikën 1 të nenit 8 të këtij ligji;
b) kur nuk plotësohen kushtet në pikën 1 të nenit 8 të këtij ligji, një nga procedurat e përmendura në pikën 3 të këtij neni.

5. Prodhuesit e produkteve me elementë digjitalë që kualifikohen si softuer i lirë dhe me burim të hapur, të cilat janë në kategoritë e përcaktuara në aneksin III të këtij ligji, janë në gjendje të tregojnë konformitetin me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji duke përdorur një nga procedurat e përmendura në pikën 1 të këtij neni, me kusht që dokumentacioni teknik i përmendur në nenin 31 të këtij ligji vendoset në dispozicion të publikut në kohën e vendosjes në treg të këtyre produkteve.

6. Interesat dhe nevojat specifike të mikrondërmarrjeve dhe ndërmarrjeve të vogla dhe të mesme, përfshirë startup-et, merren parasysh gjatë përcaktimit të tarifave për procedurat e vlerësimit të konformitetit dhe ato tarifa reduktohen në proporcion me interesat dhe nevojat e tyre specifike.

Neni 33

Masat mbështetëse për mikrondërmarrjet dhe ndërmarrjet e vogla dhe të mesme, duke përfshirë startup-et

1. Ministria përgjegjëse për ekonominë, kur është e përshtatshme, ndërmerr veprimet e mëposhtme, të përshtatura për nevojat e mikrondërmarrjeve dhe ndërmarrjeve të vogla:
a) organizon aktivitete specifike ndërgjegjësimi dhe trajnimi për zbatimin e këtij ligji;
b) krijion një kanal të dedikuar për komunikim me mikrondërmarrjet dhe ndërmarrjet e vogla dhe, sipas rastit, me autoritetet publike vendore për të ofruar këshilla dhe për t'iu përgjigjur kërkesave për informacion në lidhje me zbatimin e këtij ligji;
c) mbështet aktivitetet e testimit dhe vlerësimit të konformitetit, duke përfshirë kur është e nevojshme me mbështetjen e Qendrës Evropiane të Kompetencave të Sigurisë Kibernetike.

2. Ministria përgjegjëse për ekonominë në bashkëpunim me autoritetet e tjera kompetente mund të krijojë sandbox-e rregullator të qëndrueshmërisë kibernetike. Këto sandbox-e rregullatore sigurojnë mjedise testimi të kontrolluara për produkte inovative me elementë digjitalë për të lehtësuar zhvillimin, projektimin, vërtetimin dhe testimin e tyre me qëllim pajtueshmërinë me këtë ligj për një periudhë të kufizuar kohore përpara vendosjes në treg. Sandbox-et rregullatore nuk ndikojnë në kompetencat mbikëqyrëse dhe korrigjuese të autoriteteve kompetente. Autoritetet kompetente sigurojnë qasje të hapur, të drejtë dhe transparente në sandbox-et rregullatore, dhe në veçanti lehtësojnë aksesin e mikrondërmarrjeve dhe ndërmarrjeve të vogla, përfshirë startup-et.

3. Në përputhje me nenin 26 të këtij ligji, ministri përgjegjës për ekonominë jep udhëzime për mikrondërmarrjet dhe ndërmarrjet e vogla dhe të mesme në lidhje me zbatimin e këtij ligji.

4. Ndërmarrjet mikro dhe të vogla mund të ofrojnë të gjitha elementët e dokumentacionit teknik të specifikuar në aneksin VII të këtij ligji duke përdorur një format të thjeshtuar. Për këtë qëllim, me Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale miraton formularin e thjeshtuar të dokumentacionit teknik të synuar për nevojat e mikrondërmarrjeve dhe ndërmarrjeve të vogla, duke përfshirë mënyrën se si duhet të sigurohen elementët e përcaktuar në aneksin VII të këtij ligji. Kur një ndërmarrje mikro ose e vogël zgjedh të japë informacionin e përcaktuar në aneksin VII të këtij ligji në një mënyrë të thjeshtuar, përdor formularin e përmendur në këtë pikë. Organet e notifikuara pranojnë formularin për qëllime të vlerësimit të konformitetit.

Neni 34

Marrëveshjet e njohjes reciproke

Duke marrë në konsideratë nivelin e zhvillimit teknik dhe qasjen për vlerësimin e konformitetit të një shteti tjetër, Republika e Shqipërisë mund të lidhë marrëveshje të njohjes reciproke me shtete të tjera, në përputhje me legjislacionin në fuqi, në mënyrë që të promovojë dhe lehtësojë tregtinë ndërkombëtare.

KREU IV

NJOFTIMI I ORGANEVE TË VLERËSIMIT TË KONFORMITETIT

Neni 35

Njoftimi

Me anëtarësimin në Bashkimin Evropian, autoriteti notifikues njofton Komisionin dhe shtetet e tjera anëtare për organet e autorizuara për të kryer vlerësime të konformitetit në përputhje me këtë ligj.

Neni 36

Autoritetet notifikuese

1. Autoriteti notifikues përcaktohet me vendim të Këshillit të Ministrave dhe është përgjegjës për krijimin dhe kryerjen e procedurave të nevojshme për vlerësimin, caktimin dhe njoftimin e organeve të vlerësimit të konformitetit dhe monitorimin e tyre, duke përfshirë pajtueshmërinë me nenin 41 të këtij ligji.
2. Kur autoriteti notifikues delegon ose i beson vlerësimin, njoftimin ose monitorimin e përmendur në pikën 1 të këtij neni një organi që nuk është institucion qeveritar, organi është një person juridik dhe është në përputhje për aq sa është e mundur me nenin 37 të këtij ligji. Përveç kësaj, organi të ketë marrëveshje për të mbuluar detyrimet që rrjedhin nga aktivitetet e tij.
3. Autoriteti notifikues mban përgjegjësi të plotë për detyrat e kryera nga organi i përmendur në pikën 2 të këtij neni.

Neni 37

Kërkesat për autoritetet notifikuese

1. Autoriteti notifikues krijohet në mënyrë të tillë që të shmanget çdo konflikt interesi me organet e vlerësimit të konformitetit.
2. Autoriteti notifikues organizohet dhe funksionon në mënyrë që të garantojë objektivitetin dhe paanshmërinë e aktiviteteve të tij.
3. Autoriteti notifikues organizohet në mënyrë të tillë që çdo vendim lidhur me njoftimin e një organi të vlerësimit të konformitetit të merret nga persona kompetentë të ndryshëm nga ata që kanë kryer vlerësimin.
4. Autoriteti notifikues nuk ofron ose kryen asnjë aktivitet që kryejnë organet e vlerësimit të konformitetit ose shërbime konsulence për qëllime tregtare ose konkurruese.
5. Autoriteti notifikues garanton konfidencialitetin e informacionit që merr.
6. Autoriteti notifikues ka në dispozicion një numër të mjaftueshëm personeli kompetent për kryerjen e duhur të detyrave.

Neni 38

Detyrimi i informimit për autoritetin notifikues

1. Me anëtarësimin në Bashkimin Evropian , autoriteti notifikues informon Komisionin për procedurat për vlerësimin dhe njoftimin e organeve të vlerësimit të konformitetit dhe monitorimin e organeve të notifikuara, dhe për çdo ndryshim në to.

Neni 39

Kërkesat për organet e notifikuara

1. Për qëllimet e njoftimit, organi i vlerësimit të konformitetit plotëson kërkesat e përcaktuara në pikat 2 deri në 12 të këtij neni.
2. Organi i vlerësimit të konformitetit krijohet sipas legjislacionit në fuqi për akreditimin dhe është person juridik.
3. Organi i vlerësimit të konformitetit është një organ i palës së tretë i pavarur nga subjekti ose produkti me elementë digjitale që vlerëson.

Organi që i përket një shoqate biznesi ose profesionale që përfaqëson ndërmarrjet e përfshira në projektimin, zhvillimin, prodhimin, ofrimin, montimin, përdorimin ose mirëmbajtjen e produkteve me elementë digjitalë që vlerëson, mund të konsiderohet, me kusht që të tregohet pavarësia e tij dhe mungesa e ndonjë konflikti interesi, të konsiderohet si një organ i palës së tretë.

4. Organi i vlerësimit të konformitetit, drejtuesi i nivelit të lartë dhe personeli përgjegjës për kryerjen e detyrave të vlerësimit të konformitetit nuk duhet të jetë projektuesi, zhvilluesi, prodhuesi, furnizuesi, importuesi, shpërndarësi, instaluesi, blerësi, pronari, përdoruesi ose mirëmbajtësi i produkteve me elementë digjitalë që vlerësojnë, as përfaqësuesi i autorizuar i asnjërës prej atyre palëve. Kjo nuk përjashton përdorimin e produkteve të vlerësuara që janë të nevojshme për operacionet e organit të vlerësimit të konformitetit ose përdorimin e produkteve për qëllime personale.

Organi i vlerësimit të konformitetit, drejtuesi i nivelit të lartë dhe personeli përgjegjës për kryerjen e detyrave të vlerësimit të konformitetit nuk përfshihen drejtpërdrejt në projektimin, zhvillimin, prodhimin, importin, shpërndarjen, tregtimin, instalimin, përdorimin ose mirëmbajtjen e produkteve me elementëë digjitalë që vlerësojnë, ose përfaqësojnë palët e angazhuara në aktivitete. Ata nuk angazhohen në asnjë aktivitet që mund të bie ndeshme pavarësinë të gjykimit ose integritetin në lidhje me aktivitetet e vlerësimit të konformitetit për të cilat janë njoftuar. Kjo vlen veçanërisht për shërbimet e konsulencës.

Organet e vlerësimit të konformitetit sigurojnë që aktivitetet e degëve ose nënkontraktorëve të tyre të mos ndikojnë në konfidencialitetin, objektivitetin ose paanshmërinë e aktiviteteve të tyre të vlerësimit të konformitetit.

5. Organet e vlerësimit të konformitetit dhe personeli i tyre kryejnë aktivitetet e vlerësimit të konformitetit me shkallën më të lartë të integritetit profesional dhe kompetencën e nevojshme teknike në fushën specifike dhe janë të lirë nga të gjitha presionet dhe nxitjet, veçanërisht financiare, që mund të ndikojnë në gjykimin e tyre ose rezultatet e aktiviteteve të tyre të vlerësimit të konformitetit, veçanërisht lidhur me personat ose grupet e personave me interes në rezultatet e atyre aktiviteteve.
6. Organi i vlerësimit të konformitetit është në gjendje të kryejë të gjitha detyrat e vlerësimit të konformitetit të përmendura në aneksin VIII të këtij ligji dhe me ato detyra të njoftuara, pavarësisht nëse ato detyra kryhen nga vetë organi i vlerësimit të konformitetit ose në emër të tij dhe nën përgjegjësinë e tij.

Në çdo kohë dhe për çdo procedurë të vlerësimit të konformitetit dhe çdo lloj ose kategori produktesh me elementë digjitale në lidhje me të cilat është njoftuar, një organ i vlerësimit të konformitetit disponon burimet e nevojshme:

a) personel me njohuri teknike dhe përvojë të mjaftueshme dhe të përshtatshme për të kryer detyrat e vlerësimit të konformitetit;
b) përshkrime të procedurave në përputhje me të cilat kryhet vlerësimi i konformitetit, duke siguruar transparencën dhe mundësinë për të riprodhuar ato procedura. Të ketë politika dhe procedura të përshtatshme që bëjnë dallimin midis detyrave që kryen si organ i notifikuar dhe aktiviteteve të tjera;
c) procedura për kryerjen e aktiviteteve dhe të marrin në konsideratë madhësinë e një ndërmarrjeje, sektorin në të cilin operon, strukturën e saj, shkallën e kompleksitetit të teknologjisë së produktit dhe natyrën masive ose seriale të procesit të prodhimit.

Organi i vlerësimit të konformitetit ka mjetet e nevojshme për të kryer detyrat teknike dhe administrative të lidhura me aktivitetet e vlerësimit të konformitetit në një mënyrë të përshtatshme dhe ka akses në të gjitha pajisjet ose objektet e nevojshme.

7. Personeli përgjegjës për kryerjen e aktiviteteve të vlerësimit të konformitetit kanë:
   a) trajnim teknik dhe profesional që mbulon të gjitha aktivitetet e vlerësimit të konformitetit në lidhje me të cilat është njoftuar organi i vlerësimit të konformitetit;
   b) njohuri të kënaqshme të kërkesave të vlerësimeve që ata kryejnë dhe autoritetin e duhur për të kryer vlerësime;
   c) njohuritë dhe kuptimin e duhur të kërkesave thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji, të standardeve të harmonizuara të zbatueshme dhe specifikimeve të përbashkëta, dhe të dispozitave përkatëse të legjislacionit tjetër në fuqi dhe akteve nënligjore;
   ç) aftësi për të përpiluar certifikata, regjistrime dhe raporte që tregojnë kryerjen e vlerësimeve.

8. Organi i vlerësimit të konformitetit, drejtuesit më të lartë administrativë dhe teknikë dhe personeli i vlerësimit të konformitetit garantojnë paanshmëri. Shpërblimi i drejtuesve të nivelit të lartë dhe personelit përgjegjës për kryerjen e detyrave të vlerësimit të konformitetit të organit të vlerësimit të konformitetit, nuk varet nga numri i vlerësimeve të kryera ose nga rezultatet e atyre vlerësimeve.

9. Organi i vlerësimit të konformitetit pajiset me siguracionin për përgjegjësinë civile, me përjashtim të rastit kur përgjegjësia për vlerësimin e konformitetit është mbuluar nga shteti ose kur vetë shteti është përgjegjës për vlerësimin e përputhshmërisë.
10. Personeli i një organi të vlerësimit të konformitetit respekton sekretin profesional në lidhje me të gjitha informacionet e marra gjatë kryerjes së detyrave të tyre sipas aneksit VIII të këtij ligji ose çdo dispozitë të legjislacionit tjetër në fuqi, përveçse në lidhje me strukturat përgjegjëse për mbikëqyrjen e tregut, ku mbrohentë drejtat e pronësisë. Organi i vlerësimit të konformitetit ka procedura të dokumentuara që sigurojnë pajtueshmërinë me këtë pikë.
11. Organet e vlerësimit të konformitetit marrin pjesë ose sigurojnë që personeli i tyre i vlerësimit të informohet për aktivitetet përkatëse të standardizimit dhe aktivitetet e grupit koordinues të organeve të notifikuara të krijuar sipas nenit 48 të këtij ligji dhe zbatojnë si udhëzim të përgjithshëm vendimet dhe dokumentet administrative të prodhuara si rezultat i punës së atij grupi.
12. Organet e vlerësimit të konformitetit operojnë në përputhje me një grup termash dhe kushtesh të qëndrueshme, të drejta, proporcionale dhe të arsyeshme, duke shmangur barrën e panevojshme për operatorët ekonomikë, veçanërisht duke marrë në konsideratë interesat e mikrondërmarrjeve dhe ndërmarrjeve të vogla dhe të mesme në lidhje me tarifat.

Neni 40

Prezumimi i konformitetit të organeve të notifikuara

Kur një organ i vlerësimit të konformitetit tregon konformitetin e tij me kriteret e përcaktuara në standardet përkatëse të harmonizuara ose pjesë të tyre, referencat e të cilave janë publikuar në Fletoren Zyrtare, dhe pas anëtarësimit në Bashkimin Evropian, të botuara në Gazetën Zyrtare të Bashkimit Evropian, prezumohet se është në përputhje me kërkesat e përcaktuara në nenin 39 të këtij ligji për aq sa standardet e harmonizuara të zbatueshme i mbulojnë ato kërkesa.

Neni 41

Degët dhe nënkontraktimi nga organet e notifikuara

1. Kur një organ i notifikuar nënkontrakton detyra specifike që lidhen me vlerësimin e konformitetit ose i drejtohet një dege, ai siguron që nënkontraktori ose dega të plotësojë kërkesat e përcaktuara në nenin 39 të këtij ligji dhe informon autoritetin notifikues në përputhje me rrethanat.
2. Organet e notifikuara marrin përgjegjësinë e plotë për detyrat e kryera nga nënkontraktorët ose degët kudo që ato janë të themeluara.
3. Aktivitetet mund të nënkontraktohen ose kryhen nga një degë vetëm me dakordësinë e prodhuesit.
4. Organet e notifikuara mbajnë në dispozicion të autoritetit notifikues dokumentet përkatëse në lidhje me vlerësimin e kualifikimeve të nënkontraktorit ose degës dhe punën e kryer prej tyre sipas këtij ligji.

Neni 42

Aplikimi për njoftim

1. Organi i vlerësimit të konformitetit paraqet një aplikim për njoftim tek autoriteti notifikues.

2. Aplikimi shoqërohet me një përshkrim të aktiviteteve të vlerësimit të konformitetit, procedurës ose procedurave të vlerësimit të konformitetit dhe produktit ose produkteve me elementë digjitalë për të cilët organi pretendon të jetë kompetent, si dhe, kur është e zbatueshme, nga një certifikatë akreditimi e lëshuar nga organi kombëtar i akreditimit që vërteton se organi i vlerësimit të konformitetit plotëson kërkesat e përcaktuara në nenin 39 të këtij ligji.
3. Kur organi i vlerësimit të konformitetit nuk mund të sigurojë një certifikatë akreditimi, organi i siguron autoritetit notifikues të gjitha provat dokumentare të nevojshme për verifikimin, njohjen dhe monitorimin e rregullt të pajtueshmërisë së tij me kërkesat e përcaktuara në nenin 39 të këtij ligji.

Neni 43

Procedura e njoftimit

1. Autoriteti notifikues njofton vetëm organet e vlerësimit të konformitetit që kanë përmbushur kërkesat e përcaktuara në nenin 39 të këtij ligji.
2. Me anëtarësimin në Bashkimin Evropian, autoriteti notifikues njofton Komisionin dhe shtetet e tjera anëtare duke përdorur sistemin e informacionit të organizatave të notifikuara dhe të caktuara të qasjes së re të zhvilluar dhe të menaxhuar nga Komisioni.
3. Njoftimi përfshin detaje të plota të aktiviteteve të vlerësimit të konformitetit, modulin ose modulet e vlerësimit të konformitetit dhe produktin ose produktet me elementëë digjitalë dhe vërtetimin përkatës të kompetencës.
4. Kur një njoftim nuk bazohet në një certifikatë akreditimi siç përmendet në pikën 2 të nenit 42, autoriteti notifikues, me anëtarësimin në Bashkimin Evropian, i siguron Komisionit dhe shteteve të tjera anëtare prova dokumentare që vërtetojnë kompetencën e organit të vlerësimit të konformitetit dhe rregullimet e vendosura për të siguruar që ai organ do të monitorohet rregullisht dhe do të vazhdojë të përmbushë kërkesat e përcaktuara në nenin 39.
5. Me anëtarësimin në Bashkimin Evropian, organi notifikues mund të kryejë aktivitetet e një organi të notifikuar vetëm kur nuk ngrihen kundërshtime nga Komisioni ose shtetet e tjera anëtare brenda dy javëve nga një njoftim kur përdoret një certifikatë akreditimi ose brenda dy muajve nga një njoftim kur nuk përdoret akreditimi.
Vetëm një organ i tillë do të konsiderohet si një organ i notifikuar për qëllimet e këtij ligji.
6. Me anëtarësimin në Bashkimin Evropian, komisioni dhe shtetet e tjera anëtare njoftohen për çdo ndryshim të mëvonshëm përkatës në njoftim.

Neni 44

Ndryshimet në njoftime

1. Kur autoriteti notifikues ka konstatuar ose është informuar se një organ i notifikuar nuk i plotëson më kërkesat e përcaktuara në nenin 39 të këtij ligji, ose nuk po përmbush detyrimet e tij, autoriteti notifikues kufizon, pezullon ose tërheq njoftimin sipas rastit, në varësi të seriozitetit të mospërmbushjes së këtyre kërkesave ose detyrimeve. Me anëtarësimin në Bashkimin Evropian, autoriteti notifikues informon menjëherë Komisionin dhe shtetet e tjera anëtare në përputhje me rrethanat.
2. Në rast të kufizimit, pezullimit ose tërheqjes së njoftimit, ose kur organi i notifikuar ka ndërprerë veprimtarinë e tij, autoriteti notifikues ndërmerr hapat e duhur për të siguruar që dosjet e organit

notifikues të përpunohen nga një organ tjetër i notifikuar ose të mbahen në dispozicion të autoriteteve notifikuese dhe strukturës përgjegjëse për mbikëqyrjen e tregut me kërkesë të tyre.

Neni 45

Detyrimet operacionale të organeve të notifikuara

1. Organet e notifikuara kryejnë vlerësimet e konformitetit në përputhje me procedurat e vlerësimit të konformitetit të parashikuara në nenin 32 dhe aneksin VIII të këtij ligji.
2. Vlerësimet e konformitetit kryhen në mënyrë proporcionale, duke shmangur barrat e panevojshme për operatorët ekonomikë. Organet e vlerësimit të konformitetit kryejnë aktivitetet e tyre duke marrë në konsideratë madhësinë e ndërmarrjeve, veçanërisht në lidhje me mikrondërmarrjet dhe ndërmarrjet e vogla dhe të mesme, sektorin në të cilin operojnë, strukturën e tyre, shkallën e kompleksitetit të tyre dhe nivelin e riskut të sigurisë kibernetike të produkteve me elementë digjitalë, si dhe teknologjinë dhe natyrën masive ose seriale të procesit të prodhimit.
3. Organet e notifikuara respektojnë shkallën e rigorozitetit dhe nivelin e mbrojtjes së kërkuar për përputhshmërinë e produkteve me elementët digjitalë me këtë ligj.
4. Kur organi i notifikuar zbulon se kërkesat e përcaktuara në aneksin I të këtij ligji ose në standardet e harmonizuara përkatëse ose specifikimet e përbashkëta siç përmenden në nenin 27 të këtij ligji nuk janë përmbushur nga një prodhues, organi kërkon që prodhuesi të marrë masat e duhura korrigjuese dhe nuk lëshon certifikatën e konformitetit.
5. Kur gjatë monitorimit të konformitetit, pas lëshimit të një certifikate, një organ i notifikuar zbulon se një produkt me elementë digjitalë nuk përputhet më me kërkesat e përcaktuara në këtë ligj, ai kërkon që prodhuesi të marrë masat e duhura korrigjuese dhe pezullon ose tërheq certifikatën nëse është e nevojshme.
6. Kur masat korrigjuese nuk merren ose nuk kanë efektin e kërkuar, organi i notifikuar kufizon, pezullon ose tërheq çdo certifikatë, sipas rastit.

Neni 46

Ankesa kundër vendimeve të organeve të notifikuara

Sipas legjislacionit në fuqi të sigurohet që të ndiqet procedura e apelimit kundër vendimeve të organeve të notifikuara.

Neni 47

Detyrimi i informacionit për organet e notifikuara

1. Organet e notifikuara informojnë autoritetin notifikues për sa vijon:
   a) çdo refuzim, kufizim, pezullim ose tërheqje të një certifikate;
   b) çdo rrethanë që ndikon në fushën dhe kushtet e njoftimit;
   c) çdo kërkesë për informacion që ata kanë marrë nga struktura përgjegjëse për mbikëqyrjen e tregut në lidhje me aktivitetet e vlerësimit të konformitetit;
   ç) sipas kërkesës, aktivitetet e vlerësimit të konformitetit të kryera brenda fushës së njoftimit të tyre dhe çdo aktivitet tjetër të kryer, duke përfshirë aktivitetet ndërkufitare dhe nënkontraktimin.

2. Organet e notifikuara u ofrojnë organeve të tjera të notifikuara sipas këtij ligji që kryejnë aktivitete të ngjashme të vlerësimit të konformitetit që mbulojnë të njëjtat produkte me elementë digjitalë informacionin përkatës për çështjet që lidhen me rezultatet negative dhe, sipas kërkesës rezultatet pozitive të vlerësimit të konformitetit.

Neni 48

Koordinimi i organeve të notifikuara

1. Autoriteti notifikues mundëson që të vendoset dhe të funksionojë koordinimi dhe bashkëpunimi i duhur midis organeve të notifikuara në formën e një grupi ndërsektorial të organeve të notifikuara.
2. Autoriteti notifikues siguron që organet e notifikuara të marrin pjesë në punën e grupit, drejtpërdrejt ose me anë të përfaqësuesve të caktuar.

KREU V

MBIKËQYRJA E TREGUT DHE ZBATIMI

Neni 49

Mbikëqyrja e tregut dhe kontrolli i produkteve me elementë digjitale në tregun e brendshëm

1. Legjislacioni në fuqi për mbikëqyrjen e tregut zbatohet për produktet me elementë digjitalë që bien në fushën e këtij ligji.
2. Struktrurat përgjegjëse për mbikëqyrjen e tregut sigurojnë zbatimin efektiv të këtij ligji.
3. Strukturat përgjegjëse për mbikëqyrjen e tregut sipas përcaktimeve të pikës 2 të këtij neni janë përgjegjës për kryerjen e aktiviteteve të mbikëqyrjes së tregut në lidhje me detyrimet për mirëmbajtësit e softuerit me burim të hapur të përcaktuara në nenin 24 të këtij ligji. Kur një strukturë përgjegjëse për mbikëqyrjen e tregut zbulon se një mirëmbajtës i softuerit me burim të hapur nuk përputhet me detyrimet e përcaktuara në atë nen, struktura përgjegjëse për mbikëqyrjen e tregut kërkon nga mirëmbajtësi i softuerit me burim të hapur të sigurojë që të ndërmerren të gjitha veprimet e duhura korrigjuese. Mirëmbajtësit e softuerit me burim të hapur sigurojnë që të ndërmerren të gjitha veprimet e duhura korrigjuese në lidhje me detyrimet e tyre sipas këtij ligji.
4. Kur është e përshtatshme, strukturat përgjegjëse për mbikëqyrjen e tregut bashkëpunojnë me autoritetin kombëtar të sigurisë kibernetike dhe shkëmbejnë informacion rregullisht. Në lidhje me mbikëqyrjen e zbatimit të detyrimeve të raportimit në përputhje me nenin 14 të këtij ligji, strukturat përgjegjëse për mbikëqyrjen e tregut bashkëpunojnë dhe shkëmbejnë informacion rregullisht me CSIRT-in kombëtar .
5. Strukturat përgjegjëse për mbikëqyrjen e tregut mund të kërkojnë nga CSIRT-i i kombëtar këshilla teknike për çështjet që lidhen me zbatimin dhe mbikëqyrjen e këtij ligji. Kur kryejnë një verifikim sipas përcaktimeve të nenit 51 të këtij ligji, strukturat përgjegjëse për mbikëqyrjen e tregut mund t'i kërkojnë CSIRT-it kombëtar të japë një analizë për të mbështetur vlerësimet e pajtueshmërisë së produkteve me elementë digjitalë.
6. Kur është e përshtatshme, autoritetet përgjegjëse për mbikëqyrjen e tregut bashkëpunojnë me strukturat e tjera të mbikëqyrjes së tregut të caktuara sipas legjislacionit tjetër të posaçëm në fuqi, përveç këtij ligji dhe shkëmbejnë informacion rregullisht.

7. Strukturat përgjegjëse për mbikëqyrjen së tregut bashkëpunojnë, sipas rastit, me autoritetin përgjegjës për mbrojtjen e të dhënave personale Bashkëpunimi përfshin informimin e autoritetit për çdo gjetje të rëndësishme për përmbushjen e kompetencave të tyre, duke përfshirë lëshimin e udhëzime dhe këshilla në përputhje me pikën 10 të këtij neni nëse udhëzime dhe këshilla të tilla kanë të bëjnë me përpunimin e të dhënave personale.

Autoriteti përgjegjës për mbrojtjen e të dhënave personale ka kompetencë të kërkojë dhe të ketë akses në çdo dokumentacion të krijuar ose të mirëmbajtur sipas këtij ligji kur aksesi në atë dokumentacion është i nevojshëm për përmbushjen e detyrave të tyre. Autoriteti për mbrojtjen e të dhënave personale informon strukturat përgjegjëse për mbikëqyrjen e tregut për çdo kërkesë të tillë.

8. Strukturat përgjegjëse për mbikëqyrjen e tregut pajisen me burime financiare dhe teknike, duke përfshirë, kur është e përshtatshme, mjetet për automatizimin e përpunimit, si dhe me burime njerëzore me aftësitë e nevojshme të sigurisë kibernetike për të përmbushur detyrat e tyre sipas këtij ligji.

9. Ministria përgjegjëse për fushën inkurajon dhe lehtëson shkëmbimin e përvojës midis strukturave përgjegjëse për mbikëqyrjen e tregut.

10. Strukturat përgjegjëse për mbikëqyrjen e tregut mund të ofrojnë udhëzime dhe këshilla për operatorët ekonomikë për zbatimin e këtij ligji, me mbështetjen e ministrisë përgjegjëse për ekonominë dhe, kur është e përshtatshme, CSIRT-in kombëtar.

11. Strukturat përgjegjëse për mbikëqyrjen e tregut informojnë konsumatorët se ku duhet të paraqesin ankesa që mund të tregojnë mospërputhje me këtë ligj, në përputhje me legjislacionin në fuqi për mbikëqyrjen e tregut, dhe u ofrojnë informacion konsumatorëve se ku dhe si të aksesojnë mekanizmat për të lehtësuar raportimin e vulnerabiliteteve, incidenteve dhe kërcënimeve kibernetike që mund të ndikojnë në produktet me elementë digjitale.

12. Strukturat përgjegjëse për mbikëqyrjen e tregut lehtësojnë, kur është e nevojshme, bashkëpunimin me grupet e interesit, duke përfshirë organizatat shkencore, kërkimore dhe të konsumatorëve.

13. Strukturat përgjegjëse për mbikëqyrjen e tregut i raportojnë ministrisë përgjegjëse në baza vjetore rezultatet e aktiviteteve përkatëse të mbikëqyrjes së tregut. Strukturat përgjegjëse për mbikëqyrjen e tregut i raportojnë menjëherë ministrisë përgjegjëse dhe autoritetit të konkurrencës çdo informacion të identifikuar gjatë aktiviteteve të mbikëqyrjes së tregut që mund të jetë me interes për zbatimin e legjislacionit në fuqi për mbrojtjen e konkurrencës.

14. Për produktet me elementë digjitalë që janë në fushën e zbatimit të këtij ligji, të cilat klasifikohen si sisteme të inteligjencës artificiale me rrezik të lartë në përputhje me dispozitat përkatëse në legjislacionin në fuqi për inteligjencën artificiale, strukturat përgjegjëse për mbikëqyrjen e tregut të caktuara për qëllimet e legjislacionit në fuqi për inteligjencën artificiale janë strukturat përgjegjëse për aktivitetet e mbikëqyrjes së tregut të kërkuara sipas këtij ligji. Strukturat përgjegjëse për mbikëqyrjen e tregut të caktuara në përputhje me legjislacionin në fuqi për inteligjencën artificiale bashkëpunojnë, sipas rastit, me strukturat përgjegjëse për mbikëqyrjen e tregut të caktuara në përputhje me këtë ligj dhe, në lidhje me mbikëqyrjen e zbatimit të detyrimeve të raportimit në përputhje me nenin 14 të këtij ligji, me CSIRT-in kombëtar. Strukturat përgjegjëse për mbikëqyrjen e tregut të caktuara në përputhje me legjislacionin në fuqi për inteligjencën artificiale në veçanti informojnë strukturat përgjegjëse për mbikëqyrjen e tregut të caktuara në përputhje me këtë ligj për çdo gjetje të rëndësishme për përmbushjen e detyrave të tyre në lidhje me zbatimin e këtij ligji.

15. Strukturat përgjegjëse për mbikëqyrjen e tregut monitorojnë se si prodhuesit kanë zbatuar kriteret e përmendura në pikën 8 të nenit 13 të këtij ligji kur përcaktojnë periudhën e mbështetjes së produkteve të tyre me elementë digjitalë.

Neni 50

Aksesi në të dhëna dhe dokumentacion

Kur është e nevojshme për të vlerësuar konformitetin e produkteve me elementë digjitalë dhe proceset e vendosura nga prodhuesit e tyre me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji, strukturave përgjegjëse për mbikëqyrjen e tregut, me një kërkesë të arsyetuar, u jepet akses në të dhënat, në një gjuhë lehtësisht të kuptueshme prej tyre, të nevojshme për të vlerësuar projektimin, zhvillimin, prodhimin dhe trajtimin e vulnerabiliteteve të produkteve të tilla, duke përfshirë dokumentacionin e brendshëm të operatorit ekonomik përkatës.

Neni 51

Procedura në nivel kombëtar në lidhje me produktet me elementë digjitalë që paraqesin një risk të konsiderueshëm të sigurisë kibernetike

1. Kur struktura përgjegjëse për mbikëqyrjen e tregut ka arsye të mjaftueshme për të konsideruar se një produkt me elementë digjitale, duke përfshirë trajtimin e vulnerabilitetit të tij, paraqet një rrezik të konsiderueshëm të sigurisë kibernetike, menjëherë dhe, kur është e përshtatshme, në bashkëpunim me CSIRT-in Kombëtar, kryen një vlerësim të produktit përkatës me elementë digjitalë në lidhje me përputhshmërinë e tij me të gjitha kërkesat e përcaktuara në këtë ligj. Operatorët ekonomikë përkatës bashkëpunojnë me strukturën përgjegjëse për mbikëqyrjen e tregut sipas nevojës.
Nëse, gjatë vlerësimit, struktura përgjegjëse për mbikëqyrjen e tregut konstaton se produkti me elementë digjitalë nuk përputhet me kërkesat e përcaktuara në këtë ligj, kërkon menjëherë nga operatori ekonomik përkatës të ndërmarrë të gjitha veprimet e duhura korrigjuese që produkti me elementë digjitalë të jetë në përputhje me ato kërkesa, për të tërhequr , ose për të kthyer produktin brenda një periudhe të arsyeshme, në proporcion me natyrën e riskut të sigurisë kibernetike, siç mund të përcaktojë struktura përgjegjëse për mbikëqyrjen së tregut.
Struktura përgjegjëse për mbikëqyrjen e tregut informon organin përkatës të notifikuar. Legjislacioni në fuqi për mbikëqyrjen e tregut zbatohet për veprimet korrigjuese.
2. Kur përcaktojnë rëndësinë e një risku të sigurisë kibernetike të përmendur në pikën 1 të këtij neni, strukturat përgjegjës për mbikëqyrjen e tregut marrin gjithashtu në konsideratë faktorët joteknikë të riskut, veçanërisht ata të vendosur si rezultat i vlerësimeve të koordinuara të riskut të sigurisë në nivel kombëtar të zinxhirëve kritikë të furnizimit të kryera në përputhje me legjislacionin në fuqi për sigurinë kibernetike. Kur një strukturë përgjegjëse për mbikëqyrjen e tregut ka arsye të mjaftueshme për të konsideruar se një produkt me elementë digjitalë paraqet një risk të rëndësishëm të sigurisë kibernetike të faktorëve jo-teknikë të riskut, ai informon autoritetin kombëtar për sigurinë kibernetike dhe bashkëpunon me autoritetin sipas nevojës.
3. Me anëtarësimin në BE, kur struktura përgjegjëse për mbikëqyrjen e tregut konsideron se mospërputhja nuk është e kufizuar në territorin e tij kombëtar, ai informon Komisionin dhe shtetet e tjera anëtare për rezultatet e vlerësimit dhe për veprimet që i ka kërkuar operatorit ekonomik të ndërmarrë.
4. Operatori ekonomik siguron që të ndërmerren të gjitha veprimet e duhura korrigjuese në lidhje me të gjitha produktet me elementë digjitalë që ai ka bërë të disponueshme në treg në Republikën e Shqipërisë.
5. Kur operatori ekonomik nuk ndërmerr veprime të përshtatshme korrigjuese brenda periudhës së përmendur në paragrafin e dytë të pikës 1 të këtij neni, struktura përgjegjëse për mbikëqyrjen e tregut merr të gjitha masat e duhura të përkohshme për të tërhequr produktin ose kufizuar tregtimin

e produktit me elementë digjitalë ose për të kthyer produktin. Me anëtarësimin në Bashkimin Evropian, struktura përgjegjëse për mbikëqyrjen e tregut njofton menjëherë Komisionin dhe shtetet e tjera anëtare për këto masa.

6. Informacioni i përmendur në pikën 5 të këtij neni përfshin të gjitha detajet e disponueshme, veçanërisht të dhënat e nevojshme për identifikimin e produktit jo në përputhje me elementë digjitalë, origjinën e atij produkti me elementë digjitalë, natyrën e mospërputhjes së pretenduar dhe riskun e përfshirë, natyrën dhe kohëzgjatjen e masave të marra dhe argumentet e paraqitura nga operatori ekonomik përkatës. Në veçanti, struktura përgjegjëse për mbikëqyrjen e tregut tregon nëse mospërputhja është për shkak të një ose më shumë nga sa vijon:

a) një dështim i produktit me elementë digjitalë ose i proceseve të vendosura nga prodhuesi për të përmbushur kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji;
b) mangësitë në standardet e harmonizuara, skemat e certifikimit të sigurisë kibernetike ose specifikimet e përbashkëta, siç përmendet në nenin 27 të këtij ligji.

7. Me anëtarësimin në Bashkimin Evropian, struktura përgjegjëse për mbikëqyrjen e tregut informon pa vonesë Komisionin dhe shtetet e tjera anëtare për çdo masë të miratuar dhe për çdo informacion shtesë në dispozicion të tyre në lidhje me mospërputhjen e produktit me elementë digjitalë , dhe në rast mosmarrëveshjeje me masën e njoftuar, informon për kundërshtimet e tyre.

8. Nëse, brenda tre muajve nga marrja e njoftimit të përmendur në pikën 5 të këtij neni, nuk është ngritur asnjë kundërshtim nga një shtet anëtar ose Komisioni në lidhje me një masë të përkohshme të marrë nga struktura e mbikëqyrjes së tregut, me anëtarësimin në Bashkimin Evropian, ajo masë konsiderohet e justifikuar. Kjo nuk bie ndesh me të drejtat procedurale të operatorit ekonomik në përputhje me legjislacionin në fuqi për mbikëqyrjen e tregut.

9. Struktura e mbikëqyrjes së tregut siguron që të merren masat e duhura kufizuese në lidhje me produktin me elementë digjitalë, siç është tërheqja e menjëhershme e të produktit.

Neni 52

Produkte me elementë digjitalë në pajtueshmëri me kërkesat, të cilat paraqesin një risk të rëndësishëm për sigurinë kibernetike

1. Struktura përgjegjëse për mbikëqyrjen e tregut kërkon që një operator ekonomik të marrë të gjitha masat e duhura kur, pasi ka kryer një vlerësim sipas nenit 51 të këtij ligji, konstaton se megjithëse një produkt me elementë digjitalë dhe proceset e vendosura nga prodhuesi janë në përputhje me këtë ligj, ato paraqesin një risk të konsiderueshëm të sigurisë kibernetike si dhe një risk për:

a) shëndetin ose sigurinë e personave;
b) pajtueshmërinë me detyrimet sipas legjislacionit në fuqi për mbrojtjen e të drejtave themelore;
c) disponueshmërinë, autenticitetin, integritetin ose konfidencialitetin e shërbimeve të ofruara duke përdorur një sistem informacioni elektronik nga operatoret e infrastrukturave të informacionit me kritikalitet të lartë sipas legjislacionit në fuqi për sigurinë kibernetike; ose
ç) aspekte të tjera të mbrojtjes së interesit publik.

Masat e përmendura më sipër mund të përfshijnë masa për të siguruar që produkti me elementë digjitalë dhe proceset e vendosura nga prodhuesi të mos paraqesin më risqet përkatëse kur bëhen të disponueshme në treg, tërheqjen e produktit me elementë digjitalë ose kthimin e produktit, dhe është në proporcion me natyrën e këtyre risqeve.

2. Prodhuesi ose operatorët e tjerë ekonomikë përkatës sigurojnë që të ndërmerren veprime korrigjuese në lidhje me produktet me elementë digjitalë që ata kanë bërë të disponushme në treg në Republikën e Shqipërisë brenda afatit kohor të përcaktuar nga struktura përgjegjëse për mbikëqyrjen e tregut të përmendur në pikën 1 të këtij neni.

3. Me anëtarësimin në Bashkimin Evropian, struktura përgjegjëse për mbikëqyrjen e tregut informon menjëherë Komisionin dhe shtetet e tjera anëtare për masat e marra në përputhje me pikën 1 të këtij neni. Ky informacion duhet të përfshijë të gjitha detajet e disponueshme, veçanërisht të dhënat e nevojshme për identifikimin e produkteve me elementë digjitalë, origjinën dhe zinxhirin e furnizimit të atyre produkteve me elementë digjitalë, natyrën e riskut të përfshirë dhe natyrën dhe kohëzgjatjen e masave të marra.
4. Kur ministria përgjegjëse ka arsye të mjaftueshme për të konsideruar, duke përfshirë bazuar në informacionin e dhënë nga Autoriteti Kombëtar për Sigurinë Kibernetike, se një produkt me elementë digjitale, megjithëse në përputhje me këtë ligj, paraqet risqet e përmendura në pikën 1 të këtij neni, ai informon dhe mund t'i kërkojë autoritetit ose strukturave përgjegjëse për mbikëqyrjen e tregut të kryejnë një vlerësim dhe të ndjekin procedurat e përmendura në nenin 51 të këtij dhe në pikat 1, 2 dhe 3 të këtij neni.
5. Në rrethana që justifikojnë një ndërhyrje të menjëhershme për të ruajtur funksionimin e duhur të tregut të brendshëm dhe kur ministria përgjegjëse ka arsye të mjaftueshme për të konsideruar se produkti me elementë digjitalë i përmendur në pikën 4 të këtij neni vazhdon të paraqesë risqet e përmendura në pikën 1 të këtij neni dhe nuk janë marrë masa efektive nga strukturat përgjegjëse për mbikëqyrjen e tregut, ministria përgjegjëse kryen një vlerësim të risqeve të paraqitura nga produkti me elementë digjitalë dhe mund t'i kërkojë Autoritetit Kombëtar për Sigurinë Kibernetike të kryejë një analizë për të mbështetur vlerësimin dhe informon strukturat përgjegjëse për mbikëqyrjen e tregut në përputhje me rrethanat. Operatorët ekonomikë përkatës bashkëpunojnë me Autoritetin Kombëtar për Sigurisë Kibernetike sipas nevojës.
6. Bazuar në vlerësimin e përmendur në pikën 5 të këtij neni, ministria përgjegjëse mund të përcaktojë nëse është e nevojshme një masë korrigjuese ose kufizuese në nivel kombëtar. Për këtë qëllim, ministria përgjegjëse konsultohet menjëherë me operatorin ose operatorët ekonomikë përkatës.
7. Në bazë të konsultimit të përmendur në pikën 6 të këtij neni, Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale miraton në përputhje me praktikën përkatëse të Bashkimit Evropian masa korrigjuese ose kufizuese në nivel kombëtar, duke përfshirë kërkesën që produktet me elementë digjitalë të tërhiqen nga vendosja në treg ose të tërhiqen nga bërja e disponueshme në treg , brenda një periudhe të arsyeshme, në proporcion me natyrën e riskut.
8. Ministria përgjegjëse i njofton menjëherë vendimet e Këshillit të Ministrave të përmendura në pikën 7 të këtij neni operatorit ose operatorëve ekonomikë përkatës. Operatorët ekonomikë i zbatojnë ato vendime menjëherë dhe e informojnë ministrinë përgjegjëse në përputhje me rrethanat.
9. Pikat 4 deri në 8 të këtij neni zbatohen për kohëzgjatjen e situatës së jashtëzakonshme që justifikon ndërhyrjen e ministrisë përgjegjëse për aq kohë sa produkti me elementë digjitalë vazhdon të paraqesë risqet e përmendura në pikën 1 të këtij neni.

Neni 53

Mospërputhja formale

1. Kur struktura përgjegjëse për mbikëqyrjen e tregut bën një nga gjetjet e mëposhtme, kërkon që prodhuesi përkatës t'i japë fund mospërputhjes në lidhje me:

a) markimi CE është vendosur në kundërshtim me nenet 29 dhe 30 të këtij ligji;
b) markimi CE nuk është vendosur;
c) deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian nuk është hartuar;

ç) deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian nuk është hartuar saktë;
d) numri i identifikimit të organit të notifikuar që është i përfshirë në procedurën e vlerësimit të konformitetit, kur është e zbatueshme, nuk është vendosur;
dh) dokumentacioni teknik ose nuk është i disponueshëm ose jo i plotë.

2. Kur mospërputhja e përmendur në pikën 1 të këtij neni vazhdon, struktura përgjegjëse merr të gjitha masat e duhura për të kufizuar ose tërhequr produktin me elementë digjitalë nga bërja e disponueshme e produktit në treg ose të sigurojë që produkti të tërhiqet nga bërja e disponueshme në treg ose tërhiqet nga vendosja në treg.

Neni 54

Aktivitetet e përbashkëta të strukturave përgjegjëse për mbikëqyrjen e tregut

1. Strukturat përgjegjëse për mbikëqyrjen së tregut mund të bien dakord me autoritetet e tjera përkatëse për të kryer aktivitete të përbashkëta që synojnë garantimin e sigurisë kibernetike dhe mbrojtjen e konsumatorëve në lidhje me produkte specifike me elementë digjitalë të vendosura në treg ose të bëra të disponueshme në treg, në veçanti produktet me elementë digjitalë që shpesh zbulohen se paraqesin risqe të sigurisë kibernetike.
2. Struktura përgjegjëse për mbikëqyrjen e tregut dhe, kur është e zbatueshme, ministria përgjegjëse, siguron që dakordësia lidhur me aktivitetet e përbashkëta për t'u kryer të mos rezultojnë në konkurrencë të pandershme midis operatorëve ekonomikë dhe nuk ndikojnë negativisht në objektivitetin, pavarësinë dhe paanshmërinë e palëve të dakordësuara.
3. Struktura përgjegjëse për mbikëqyrjen e tregut mund të përdorë çdo informacion të marrë si rezultat i aktiviteteve të përbashkëta të kryera si pjesë e çdo verifikimi që ndërmerr.
4. Struktura përgjegjëse për mbikëqyrjen e tregut dhe, kur është e zbatueshme, ministria përgjegjëse, vënë në dispozicion të publikut dakordësinë për aktivitetet e përbashkëta, duke përfshirë emrat e palëve të përfshira.

Neni 55

Veprime kontrolli

1. Strukturat përgjegjëse për mbikëqyrjen e tregut kryejnë veprime të njëkohshme të koordinuara kontrolli të produkteve specifike me elementë digjitalë ose kategori të tyre për të kontrolluar pajtueshmërinë ose për të zbuluar shkeljet e këtij ligji. Këto kontrolle mund të përfshijnë edhe inspektime të produkteve me elementë digjitalë të marra nën një identitet të fshehtë.
2. Nëse nuk është rënë dakord ndryshe nga strukturat përgjegjëse për mbikëqyrjen e tregut të përfshira, veprimet e kontollit koordinohen nga ministria përgjegjëse. Koordinatori i veprimeve të kontrollit, kur është e përshtatshme, rezultatet e mbledhura i bën të disponueshme publikisht.
3. Kur, në kryerjen e detyrave, përfshirë në bazë të njoftimeve të marra në përputhje me pikat 1 dhe 3 të nenit 14 të këtij ligji, Autoriteti Kombëtar për Sigurinë Kibernetike identifikon kategoritë e produkteve me elementë digjitalë për të cilat mund të organizohen veprime kontrolli, paraqet një propozim për veprim kontrolli tek koordinatori i përmendur në pikën 2 të këtij neni për t'u marrë në konsideratë nga strukturat përgjegjëse për mbikëqyrjen e tregut.

4. Gjatë kryerjes së veprimeve të kontrollit, strukturat përgjegjëse për mbikëqyrjen e tregut të përfshira mund të përdorin kompetencat e verifikimit të përcaktuara në nenet 49 deri në 53 të këtij ligji dhe çdo kompetencë tjetër që u jepet atyre nga legjislacioni tjetër në fuqi.
5. Strukturat përgjegjëse për mbikëqyrjen e tregut mund të ftojnë zyrtarë dhe persona të tjerë shoqërues të autorizuar nga ministria përgjegjëse për të marrë pjesë në veprime kontrolli.

KREUVI

KONFIDENCIALITETI DHE PENALITETET

Neni 56

Konfidencialiteti

1. Të gjitha palët e përfshira në zbatimin e këtij ligji respektojnë konfidencialitetin e informacionit dhe të dhënave të marra në kryerjen e detyrave dhe aktiviteteve të tyre në mënyrë të tillë që të mbrojnë, në veçanti si më poshtë vijon:
   a) të drejtat e pronësisë intelektuale dhe informacionin konfidencial të biznesit ose sekretet tregtare të një personi fizik ose juridik, duke përfshirë kodin burim, përveç rasteve të përmendura në legjislacionin në fuqi;
   b) zbatimin efektiv të këtij ligji, veçanërisht për qëllime inspektimesh, verifikimesh ose auditimesh;
   c) interesat e sigurisë publike dhe kombëtare;
   ç) integritetin e procedurave penale ose administrative.
2. Pa rënë ndesh me pikën 1 të këtij neni, informacioni i shkëmbyer në baza konfidenciale midis strukturave përgjegjëse për mbikëqyrjen e tregut dhe midis dhe ministrisë përgjegjëse si dhe me anëtarësimin në Bashkimin Evropian, midis strukturës përgjegjëse për mbikëqyrjen e tregut të Republikës së Shqipërisë dhe strukturave përgjegjëse për mbikëqyrjen e tregut të vendeve të tjera dhe Komisionit Evropian, nuk do të zbulohet pa pëlqimin paraprak të strukturës iniciuese përgjegjëse të mbikëqyrjes së tregut.
3. Pikat 1 dhe 2 të këtij neni nuk prekin të drejtat dhe detyrimet e ministrisë përgjegjëse dhe organeve të njoftuara në lidhje me shkëmbimin e informacionit dhe shpërndarjen e paralajmërimeve, as detyrimet e personave për të dhënë informacion sipas legjislacionit penal në fuqi.

Neni 57

Kundërvajtjet dhe sanksionet administrative

1. Mosrespektimi i kërkesave thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji dhe detyrimeve të përcaktuara në nenet 13 dhe 14 të këtij ligji dënohet me gjobë administrative deri në 15 000 000 lekë ose, nëse shkelësi është një shoqëri tregtare, deri në 2,5 % të xhiros totale vjetore për vitin financiar paraardhës, nëse kjo e fundit është më e lartë.
2. Mospërmbushja e detyrimeve të përcaktuara në nenet 18 deri në 23, nenin 28, pikat 1 deri në 4 të nenit 30, pikat 1 deri ne 4 të nenit 31, pikat 1, 2 dhe 3 të nenit 32, pika 4 e nenit 33 dhe nenet 39, 41, 45, 47 dhe 50 i dënohen me gjobë administrative deri në 10 000 000 lekë ose, nëse shkelësi është një ndërmarrje, deri në 2 % të xhiros së saj vjetore totale për vitin financiar paraardhës, nëse kjo e fundit është më e lartë.

3. Dhënia e informacionit të pasaktë, jo të plotë ose mashtrues për organet e notifikuara dhe strukturat përgjegjëse për mbikëqyrjen e tregut në përgjigje të një kërkese dënohet me gjobë administrative deri në 5 000 000 lekë ose, nëse shkelësi është një shoqëri tregtare , deri në 1 % të xhiros së saj vjetore totale për vitin financiar paraardhës, nëse kjo e fundit është më e lartë.
4. Kur vendoset për masën e gjobës administrative në çdo rast individual, merren në konsideratë të gjitha rrethanat përkatëse të situatës specifike dhe konsideratë të veçantë për sa vijon:

a) natyrën, seriozitetin dhe kohëzgjatjen e shkeljes dhe pasojat e saj;
b) nëse gjobat administrative janë aplikuar tashmë nga i njëjti autoritet ose struktura të tjera përgjegjëse për mbikëqyrjen e tregut për të njëjtin operator ekonomik për një shkelje të ngjashme;
c) madhësia, veçanërisht në lidhje me mikrondërmarrjet dhe ndërmarrjet e vogla dhe të mesme, përfshirë startup-et, dhe pjesa e tregut të operatorit ekonomik përgjegjës për shkeljen.

5. Këshilli i Ministrave, me propozimin e ministrit përgjegjës për komunikimet elektronike dhe digjitale si dhe ekonominë dhe inovacionin përcakton rregullat në lidhje me rastet dhe masën e vendosjes së gjobave administrative për autoritetet publike dhe organet publike, të themeluara në Republikën e Shqipërisë.
6. Gjobat administrative mund të vendosen, në varësi të rrethanave të çdo rasti individual, përveç çdo mase tjetër korrigjuese ose kufizuese të aplikuar nga strukturat përgjegjëse për mbikëqyrjen e tregut për të njëjtën shkelje.
7. Në përjashtim të pikave 2 deri në 6 të këtij neni, gjobat administrative të përmendura në ato pika nuk zbatohen për sa vijon:

a) prodhuesit që kualifikohen si mikrondërmarrje ose ndërmarrje të vogla në lidhje me çdo mospërmbushje të afatit të përmendur në shkronjën "a" të pikës 2 të nenit 14 ose në shkronjën "a", të pikës 4 të nenit 14 të këtij ligji;
b) çdo shkelje të këtij ligji nga mirëmbajtësit e softuerit me burim të hapur.

KREU VII

DISPOZITA KALIMTARE DHE TË FUNDIT

Neni 58

Aktet nënligjore

1. Ngarkohet Këshilli i Ministrave që brenda 24 muajve nga hyrja në fuqi e këtij ligji të miratojë aktet nënligjore në zbatim të neneve 7, pikat 3, 4 dhe 5, 8, pikat 1 dhe 4, 13, pikat 8 dhe 24, 14, pika 9, 25, 27, pikat 1, 2 dhe 5, 28, pika 5, 30, pika 6, 31, pika 5, 33, pika 4, 36, pika 1, 52, pika 7, 57, pika 5.
2. Ngarkohet ministri përgjegjës për ekonominë që brenda 24 muajve nga hyrja në fuqi e këtij ligji të miratojë aktin nënligjor në zbatim të nenit 26, pika 1 dhe nenit 33, pika 3 e këtij ligji.

Neni 59

Dispozitat kalimtare

1. Certifikatat për ekzaminimin e tipit në përputhje me standardet e Bashkimit Evropian dhe vendimet e miratimit të lëshuara në lidhje me kërkesat e sigurisë kibernetike në përputhje me

standardet e Bashkimit Evropian për produktet me elementë digjitalë që i nënshtrohen legjislacionit në fuqi përveç këtij ligji do të mbeten të vlefshme deri më 31 dhjetor 2029, përveç nëse ato skadojnë para kësaj date, ose nëse nuk specifikohet ndryshe në legjislacionin tjetër në fuqi, në këtë rast ato do të mbeten të vlefshme siç përmendet në legjislacionin përkatës.

2. Produktet me elementë digjitalë që janë vendosur në treg para hyrjes në fuqi të këtij ligji do të jenë subjekt i kërkesave të përcaktuara në këtë ligj vetëm nëse, nga ajo datë, ato produkte pësojnë një modifikimi thelbësor.

3. Në përjashtim të pikës 2 të këtij neni, detyrimet e përcaktuara në nenin 14 të këtij ligji zbatohen për të gjitha produktet me elementë digjitalë që bien në fushën e zbatimit të këtij ligji që janë vendosur në treg para hyrjes në fuqi të këtij ligji.

Neni 60

Vlerësimi dhe rishikimi

1. Ministria përgjegjëse harton një raport mbi vlerësimin dhe rishikimin e këtij ligji . Këto raporte bëhen publike.

Neni 61
Shfuqizime në datën e anëtarësimit të Republikës së Shqipërisë në Bashkimin Evropian

1. Në datën e anëtarësimit të Republikës së Shqipërisë në Bashkimin Evropian të gjitha dispozitat e këtij ligji shfuqizohen me përjashtim të nenit 36, pika 1 dhe nenit 57, pika 5.

2. Ngarkohet Këshilli i Ministrave që me anëtarësimin e Republikës së Shqipërisë në Bashkimin Evropian të shfuqizojë aktet nënligjore në zbatim të këtij ligji, me përjashtim të akteve nënligjore të nxjerra në zbatim të neneve të përcaktuara në pikën 1 të këtij neni.

Neni 62

Hyrja në fuqi dhe zbatimi

Ky ligj hyn në fuqi 3 (tre) vjet pas botimit në Fletoren Zyrtare.

ANEKSI I

KËRKESAT THELBËSORE TË SIGURISË KIBERNETIKE

Pjesa I

Kërkesat e sigurisë kibernetike në lidhje me vetitë e produkteve me elementë digjitalë

1. Produktet me elementë digjitalë projektohen, zhvillohen dhe prodhohen në mënyrë të tillë që të sigurojnë një nivel të përshtatshëm të sigurisë kibernetike bazuar në risqet.
2. Në bazë të vlerësimit të riskut të sigurisë kibernetike të përmendur në pikën 2 të nenit 13 Të këtij ligji dhe kur është e aplikueshme, produktet me elementë digjitalë:

a) bëhen të disponueshme në treg pa vulnerabilitete të njohura të shfrytëzueshme;
b) bëhen të disponueshme në treg me një konfigurim të sigurt si parazgjedhje, përveç nëse është rënë dakord ndryshe ndërmjet prodhuesit dhe përdoruesit të biznesit në lidhje me një produkt të prodhuar sipas kërkesave të veçnta me elementë digjitalë, duke përfshirë mundësinë për të rikthyer produktin në gjendjen e tij origjinale;
c) sigurojnë që vulnerabilitetet mund të adresohen përmes përditësimeve të sigurisë, duke përfshirë, kur është e aplikueshme, përmes përditësimeve automatike të sigurisë që instalohen brenda një afati kohor të përshtatshëm të aktivizuar si një cilësim i paracaktuar, me një mekanizëm të qartë dhe të lehtë për t'u përdorur për çaktivizim, përmes njoftimit të përditësimeve të disponueshme për përdoruesit dhe opsionin për t'i shtyrë ato përkohësisht;
ç) sigurojnë mbrojtjen nga aksesi i paautorizuar nga mekanizmat e duhur të kontrollit, duke përfshirë por pa u kufizuar në sistemet e autentifikimit, identitetit ose menaxhimit të aksesit, dhe raportojnë për aksesin e mundshëm të paautorizuar;
d) mbrojtja e konfidencialitetit të të dhënave të ruajtura, të transmetuara ose të përpunuara ndryshe, personale ose të tjera, si për shembull duke enkriptuar të dhënat përkatëse në të ruajtura ose në gjendje transmetimi me mekanizma më të fundit dhe duke përdorur mjete të tjera teknike;
dh) mbrojtja e integritetit të të dhënave të ruajtura, të transmetuara ose të përpunuara ndryshe, personale ose të tjera, komandave, programeve dhe konfigurimit kundër çdo manipulimi ose modifikimi të paautorizuar nga përdoruesi, dhe raportomi mbi kompromentimet;
e) përpunojnë vetëm të dhëna, personale ose të tjera, që janë të përshtatshme, relevante dhe të kufizuara në atë që është e nevojshme në lidhje me qëllimin e synuar të produktit me elementë digjitalë (minimizimi i të dhënave);
ë) mbrojtja e disponueshmërisë së funksioneve thelbësore dhe bazike, gjithashtu pas një incidenti, duke përfshirë masat e qëndrueshmërisë dhe zbutjes kundër sulmeve të mohimit të shërbimit;
f) minimizon ndikimin negativ nga vetë produktet ose pajisjet që lidhen me disponueshmërinë e shërbimeve të ofruara nga pajisje ose rrjete të tjera;
g) të projektohet, zhvillohet dhe prodhohet për të kufizuar sipërfaqet e sulmit, duke përfshirë ndërfaqet e jashtme;
gj) të projektohet, zhvillohet dhe prodhohet për të zvogëluar ndikimin e një incidenti duke përdorur mekanizmat dhe teknikat e duhura të zbutjes së shfrytëzimit të vulnerabiliteteve;
h) sigurimi i informacionit në lidhje me sigurinë duke regjistruar dhe monitoruar aktivitetin përkatës të brendshëm, duke përfshirë aksesin ose modifikimin e të dhënave, shërbimeve ose funksioneve, me një mekanizëm çaktivizimi për përdoruesin;

i) siguroni mundësinë për përdoruesit që të heqin në mënyrë të sigurt dhe të lehtë në baza të përhershme të gjitha të dhënat dhe cilësimet dhe, kur të dhëna të tilla mund të transferohen në produkte ose sisteme të tjera, siguron që kjo të bëhet në një mënyrë të sigurt.

Pjesa II

Kërkesat e trajtimit të vulnerabiliteteve

Prodhuesit e produkteve me elementë digjitalë:

1. Identifikojnë dhe dokumentojnë vulnerabilitetet dhe komponentët që përmbahen në produkte me elementë digjitale, duke përfshirë përgatitjen e një liste të komponentëve të software-it në një format të zakonshëm dhe të lexueshëm nga makina që mbulon të paktën varësitë e nivelit të lartë të produkteve.
2. Në lidhje me risqet e paraqitura ndaj produkteve me elementë digjitalë, adresojnë dhe korrigjojnë vulnerabilitetet pa vonesë, duke përfshirë mundësimin e përditësimeve e sigurisë; aty ku është e mundur teknikisht, përditësimet e reja të sigurisë ofrohen të ndara nga përditësimet e funksionalitetit;
3. Aplikojnë teste dhe rishikime efektive dhe të rregullta të sigurisë së produktit me elementë digjitalë.
4. Pasi të jetë vënë në dispozicion një përditësim sigurie, ndajnë dhe zbulojnë publikisht informacionin rreth vulnerabiliteteve të korrigjuara, duke përfshirë një përshkrim të vulnerabiliteteve, informacionin që lejon përdoruesit të identifikojnë produktin me elementë digjitalë të prekur, ndikimet e vulnerabiliteteve, ashpërsinë e tyre dhe informacionin e qartë dhe të aksesueshëm që ndihmon përdoruesit të korrigjojnë vulnerabilitetin; Në raste të justifikuara siç duhet, kur prodhuesit konsiderojnë risqet e sigurisë së publikimit si më të mëdha se përfitimet e sigurisë, ata mund të vonojnë bërjen publike të informacionit në lidhje me një vulnerabilitet të korrigjuar derisa përdoruesve t'u jepet mundësia të aplikojnë softuerin korrigjues/korrigjimin (patch) përkatës.
5. Vendosin dhe zbatiojnë e një politike për zbulimin e koordinuar të vulnerabilitetit.
6. Marrin masa për të lehtësuar ndarjen e informacionit në lidhje me vulnerabilitetet e mundshme në produktin e tyre me elementë digjitalë, si dhe në komponentët e palëve të treta që përmbahen në atë produkt, duke përfshirë dhënien e një adrese kontakti për raportimin e vulnerabiliteteve të zbuluara në produkt me elementë digjitalë.
7. Sigurojë mekanizma për shpërndarjen e sigurt të përditësimeve për produktet me elementë digjitalë për të siguruar që vulnerabilitetet të rregullohen ose zbuten në kohën e duhur dhe, kur është e aplikueshme për përditësimet e sigurisë, në një mënyrë automatike.
8. Sigurojnë që, kur përditësimet e sigurisë janë të disponueshme për të adresuar çështjet e identifikuara të sigurisë, ato shpërndahen pa vonesë dhe, përveç nëse është rënë dakord ndryshe midis një prodhuesi dhe një përdoruesi biznesi në lidhje me një produkt i përshtatur sipas kërkesave specifike me elementë digjitalë, pa pagesë, të shoqëruara me mesazhe këshilluese që u ofrojnë përdoruesve informacionin përkatës, duke përfshirë veprimet e mundshme që duhen ndërmarrë.

ANEKSI II

INFORMACION DHE UDHËZIME PËR PËRDORUESIN

Produkti me elementë digjitalë shoqërohet të paktën nga:

1. Emri, emri tregtar i regjistruar ose marka tregtare e regjistruar e prodhuesit dhe adresa postare, adresa e emailit ose kontakti tjetër digjital, si dhe, kur është e disponueshme, faqja e internetit në të cilën mund të kontaktohet prodhuesi.
2. Pika e vetme e kontaktit ku mund të raportohet dhe merret informacioni në lidhje me vulnerabilitetet e produktit me elementë digjitalë dhe ku mund të gjendet politika e prodhuesit për zbulimin e koordinuar të vulnerabilitetit;
3. Emri dhe lloji dhe çdo informacion shtesë që mundëson identifikimin unik të produktit me elementë digjitalë.
4. Qëllimi i synuar i produktit me elementë digjitalë, duke përfshirë mjedisin e sigurisë të ofruar nga atributet e sigurisë.
5. Çdo rrethanë e njohur ose e parashikueshme, në lidhje me përdorimin e produktit me elementë digjitalë në përputhje me qëllimin të synuar ose në kushte të keqpërdorimit të parashikueshëm në mënyrë të arsyeshme, të cilat mund të çojnë në risqe të konsiderueshme të sigurisë kibernetike.
6. Kur është e aplikueshme, adresa e internetit në të cilën mund të aksesohet deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian.
7. Lloji i mbështetjes teknike të sigurisë së ofruar nga prodhuesi dhe data e përfundimit të periudhës së mbështetjes gjatë së cilës përdoruesit mund të presin që vulnerabilitetet të trajtohen dhe të marrin përditësime sigurie.
8. Udhëzime të detajuara ose një adresë interneti që i referohet udhëzimeve dhe informacioneve të tilla të detajuara për:
   a) masat e nevojshme gjatë vënies fillestare në punë dhe gjatë gjithë jetës së produktit me elementë digjitalë për të siguruar përdorimin e tij të sigurt;
   b) se si ndryshimet në produkt me elementë digjitalë mund të ndikojnë në sigurinë e të dhënave;
   c) se si mund të instalohen përditësimet e rëndësishme për sigurinë;
   ç) çmontimi i sigurt i produktit me elementë digjitalë, duke përfshirë informacionin se si të dhënat e përdoruesit mund të hiqen në mënyrë të sigurt;
   d) se si mund të çaktivizohet cilësimi i paracaktuar që mundëson instalimin automatik të përditësimeve të sigurisë, siç kërkohet nga shkronja “c”, pika 2, pjesa I, e aneksit I të këtij ligji;
   dh) kur produkti me elementë digjitalë synohet të integrohet në produkte të tjera me elementë digjitalë, udhëzime të detajuara për informacionin e nevojshëm që integruesi të jetë në përputhje me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji dhe kërkesat e dokumentacionit të përcaktuara në aneksin VII të këtij ligji.
9. Informacioni se ku mund të aksesohet lista e komponentëve të softuerit nëse prodhuesi vendos t'i vërë në dispozicion përdoruesit listën e komponentëve të softuerit .

ANEKSI III

PRODUKTE TË RËNDËSISHME ME ELEMENTË DIGJITALË

Klasa I

1. Sistemet e menaxhimit të identitetit dhe softueri dhe hardueri i menaxhimit të aksesit të privilegjuar, përfshirë lexuesit e vërtetimit dhe kontrollit të aksesit, përfshirë lexuesit biometrikë.
2. Shfletues të pavarur dhe të integruar.
3. Menaxherët e fjalëkalimeve.
4. Softuer që kërkon, heq ose karantinon softuerin me qëllim keqdashës.
5. Produkte me elementë digjitalë që kanë funksionin e rrjetit privat virtual (VPN).

6. Sistemet e menaxhimit të rrjetit.
7. Sistemet e informacionit të sigurisë dhe menaxhimit të ngjarjeve (SIEM).
8. Menaxherët e procesit të nisjes fillestare Boot.
9. Infrastruktura e çelësit publik dhe softueri i lëshimit të certifikatave digjitale.
10. Ndërfaqet e rrjetit fizik dhe virtual.
11. Sistemet operative.
12. Ruterat, modemet e destinuara për lidhjen me internetin dhe switch-et.
13. Mikroprocesorët me funksionalitete të lidhura me sigurinë.
14. Mikrokontrollues me funksionalitete të lidhura me sigurinë.
15. qarqet e integruara specifike të aplikimit (aSIC) dhe grupet e portave të programueshme në terren (FPGa) me funksionalitete të lidhura me sigurinë.
16. Asistentët virtualë për qëllime të përgjithshme të produkteve inteligjente shtëpiake.
17. Produkte shtëpiake inteligjente me funksionalitete sigurie, duke përfshirë bravat inteligjente të dyerve, kamerat e sigurisë, sistemet e monitorimit të foshnjave dhe sistemet e alarmit.
18. Lodra të lidhura me internetin të mbuluara sipas legjislacionit në fuqi për sigurinë e lodrave që kanë veçori interaktive sociale (p.sh. të folurit ose filmimin) ose që kanë veçori të gjurmimit të vendndodhjes.
19. Produktet personale për t'u veshur ose vendosur në trupin e njeriut që kanë qëllim monitorim shëndetësor (siç është gjurmimi) dhe për të cilat nuk zbatohen rregullat për pajisjet mjeksore ose invitro sipas legjislacionit në fuqi, ose produkte personale për t'u veshur që janë të destinuara për përdorim nga fëmijët.

Klasa II

1. Hipervizorët dhe sistemet e kohës së ekzekutimit të kontejnerëve që mbështesin ekzekutimin e virtualizuar të sistemeve operative dhe mjediseve të ngjashme.
2. Firewalls, sisteme të zbulimit dhe parandalimit të ndërhyrjeve.
3. Mikroprocesorë rezistent ndaj manipulimeve.
4. Mikrokontrollues rezistent ndaj manipulimeve.

ANEKSI IV

PRODUKTE KRITIKE ME ELEMENTË DIGJITALE

1. Pajisjet harduerike me kuti sigurie.
2. Portat e matësve inteligjentë brenda sistemeve të matjes inteligjente siç përcaktohet në legjislacionin për tregun e brendshëm të energjisë elektrike pdhe pajisje të tjera për qëllime të avancuara sigurie, përfshirë përpunimin e sigurt të kriptove.
3. Kartat inteligjente ose pajisje të ngjashme, duke përfshirë elementë të sigurt.

ANEKSI V

DEKLARATA EU E KONFORMITETIT

Deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian e përmendur në nenin 28 të këtij ligji, përmban të gjitha informacionet e mëposhtme:
1. Emri dhe lloji dhe çdo informacion shtesë që mundëson identifikimin unik të produktit me elementë digjitalë.

2. Emri dhe adresa e prodhuesit ose përfaqësuesit të autorizuar.
3. Një deklaratë se deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian lëshohet nën përgjegjësinë e vetme të ofruesit.
4. Objekti i deklaratës (identifikimi i produktit me elementë digjitalë që lejojnë gjurmueshmërinë, i cili mund të përfshijë një fotografi, kur është e përshtatshme).
5. Një deklaratë se objekti i deklaratës së përshkruar më sipër është në konformitet me legjislacionin tjetër në fuqi.
6. Referencat për çdo standard përkatës të harmonizuar të përdorur ose ndonjë specifikim tjetër të përbashkët ose certifikim të sigurisë kibernetike në lidhje me të cilin deklarohet konformiteti.
7. Kur është e aplikueshme, emri dhe numri i organit të notifikuar, një përshkrim i procedurës së vlerësimit të konformitetit të kryer dhe identifikimi i certifikatës së lëshuar.
8. Informacion shtesë:

Nënshkruar për dhe në emër të:

(vendi dhe data e lëshimit):

(emri, funksioni)

(nënshkrimi):

ANEKSI VI

DEKLARATA E THJESHTUAR E KONFORMITETIT NË PËRPUTHJE ME STANDARDET E BASHKIMIT EVROPIAN

Deklarata e thjeshtuar e konformitetit në përputhje me standardet e Bashkimit Evropian të përmendur në pikën 20 të nenit 13 të këtij ligji sigurohet si më poshtë:

Me këtë, ... [emri i prodhuesit] deklaron se tipi i produktit me elementë digjitale ... [përcaktimi i llojit të produktit me elementë digjital] është në përputhje me rregullat në lidhje me kërkesat horizontale të sigurisë kibernetike për produktet që përmbajnë elementë digjitale sipas këtij ligji.

Teksti i plotë i deklaratës së konformitetit në përputhje me standardet e Bashkimit Evropian është i disponueshëm në adresën e mëposhtme të internetit: ...

ANEKSI VII

PËRMBAJTJA E DOKUMENTACIONIT TEKNIK

Dokumentacioni teknik i përmendur në nenin 31 të këtij ligji përmban të paktën informacionin e mëposhtëm, siç është e zbatueshme për produktin përkatës me elementë digjitalë:

1. Një përshkrim i përgjithshëm të produktit me elementë digjitalë, duke përfshirë:
   a) qëllimin e synuar të tij;
   b) versionet e softuerit që ndikojnë në pajtueshmërinë me kërkesat thelbësore të sigurisë kibernetike;
   c) kur produkti me elementë digjitalë është një produkt harduerik, fotografi ose ilustrime që tregojnë veçoritë e jashtme, shënimin dhe paraqitjen e brendshme;
   ç) informacioni dhe udhëzimet e përdoruesit siç përcaktohet në aneksin II të këtij ligji.

2. Një përshkrim i projektimit, zhvillimit dhe prodhimit të produktit me elementë digjitalë dhe proceset e trajtimit të vulnerabiliteteve, duke përfshirë:

a) informacionin e nevojshëm mbi projektimin dhe zhvillimin e produktit me elementë digjitalë, duke përfshirë, kur është e aplikueshme, vizatimet dhe skemat dhe një përshkrim të arkitekturës së sistemit që shpjegon se si komponentët e softuerit ndërtohen ose ndërveprojnë me njëri-tjetrin dhe integrohen në përpunimin e përgjithshëm;
b) informacionin e nevojshëm dhe specifikimet e proceseve të trajtimit të vulnerabiliteteve të vendosura nga prodhuesi, duke përfshirë listën e komponentëve të softueriit, politikën e koordinuar të zbulimit të vulnerabiliteteve, evidencë e ofrimit të një adrese kontakti për raportimin e vulnerabiliteteve dhe një përshkrim të zgjidhjeve teknike të zgjedhura për shpërndarjen e sigurt të përditësimeve;
c) informacionin e nevojshme dhe specifikimet e proceseve të prodhimit dhe monitorimit të produktit me elementë digjitalë dhe validimi i këtyre proceseve.

3. Një vlerësim i risqeve të sigurisë kibernetike kundër të cilave projektohet, zhvillohet, prodhohet, dorëzohet dhe mirëmbahet produkti me elementë digjitalë në përputhje me nenin 13 të këtij ligji, duke përfshirë mënyrën se si zbatohen kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij ligji.
4. Informacioni përkatës që është marrë në konsideratë për të përcaktuar periudhën e mbështetjes sipas pikes 8 të nenit 13 të këtij ligji të produktit me elementë digjitalë.
5. Një listë të standardeve të harmonizuara të aplikuara plotësisht ose pjesërisht, referencat e të cilave janë publikuar në Fletoren Zyrtare, specifikimet e përbashkëta të përcaktuara në nenin 27 të këtijj ligji ose skemat e certifikimit të sigurisë kibernetike në përputhje me pikën 8 të nenit 27 të këtij ligji dhe, kur ato standarde të harmonizuara, specifikimet e përbashkëta ose skema të certifikimit të sigurisë kibernetike nuk janë zbatuar, përshkrimet e zgjidhjeve të miratuara për të përmbushur kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesët I dhe II të aneksit I të këtij ligji, duke përfshirë një listë të specifikimeve të tjera teknike përkatëse të aplikuara. Në rast të standardeve të harmonizuara të aplikuara pjesërisht, specifikimeve të përbashkëta ose skemave të certifikimit të sigurisë kibernetike, dokumentacioni teknik specifikon pjesët që janë aplikuar.
6. Raportet e testeve të kryera për të verifikuar konformitetin e produktit me elementët digjitalë dhe të proceseve të trajtimit të vulnerabiliteteve me kërkesat thelbësore të zbatueshme të sigurisë kibernetike të përcaktuara në pjesët I dhe II të aneksit I të këtij ligji.
7. Një kopje të deklaratës së konformitetit në përputhje me standardet e Bashkimit Evropian.
8. Kur është e zbatueshme, lista e komponentëve të softuerit, në bazë të një kërkese të arsyetuar nga një strukturë përgjegjëse për mbikëqyrjen e tregut me kusht që të jetë nevojshme në mënyrë që ai autoritet të jetë në gjendje të kontrollojë pajtueshmërinë me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji.

ANEKSI VIII

PROCEDURAT E VLERËSIMIT TË KONFORMITETIT

Pjesa I
Procedura e vlerësimit të konformitetit bazuar në kontrollin e brendshëm (bazuar në modulin A)

1. Kontrolli i brendshëm është procedura e vlerësimit të konformitetit me anë të së cilës prodhuesi përmbush detyrimet e përcaktuara në pikat 2, 3 dhe 4 të kësaj pjese dhe siguron dhe deklaron me përgjegjësinë e tij të vetme se produktet me elementë digjitalë plotësojnë të gjitha kërkesat thelbësore

të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij ligji dhe prodhuesi plotëson kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksit I të këtij ligji.
2. Prodhuesi harton dokumentacionin teknik të përshkruar në aneksin VII të këtij ligji.
3. Projektimi, zhvillimi, prodhimi dhe trajtimi i vulnerabiliteteve të produkteve me elementë digjitalë.
Prodhuesi marr të gjitha masat e nevojshme në mënyrë që proceset e projektimit, zhvillimit, prodhimit dhe trajtimit të vulnerabiliteteve dhe monitorimi i tyre të sigurojnë përputhshmërinë e produkteve të prodhuara ose të zhvilluara me elementët digjitalë dhe të proceseve të vendosura nga prodhuesi me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesët I dhe II të aneksit I të këtij ligji.
4. Shënimi i konformitetit dhe deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian.
4.1. Prodhuesi vendosë markimin CE në çdo produkt individual me elementë digjitalë që plotëson kërkesat e zbatueshme të përcaktuara në këtë ligj.
4.2. Prodhuesi harton një deklaratë me shkrim të konformitetit për çdo produkt me elementë digjitalë në përputhje me nenin 28 të këtij ligji dhe e mban në dispozicion së bashku me dokumentacionin teknik të autoriteteve kombëtare për 10 vjet pasi produkti me elementë digjitalë është vendosur në treg ose për periudhën e mbështetjes, nëse kjo e fundit është më e gjatë. Deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian identifikon produktin me elementë digjitalë për të cilin është hartuar. Një kopje e deklaratës së konformitetit në përputhje me standardet e Bashkimit Evropian do t'u vihet në dispozicion autoriteteve përkatëse sipas kërkesës.
5. Përfaqësues të autorizuar.
Detyrimet e prodhuesit të përcaktuara në pikën 4 të kësaj pjese mund të përmbushen nga përfaqësuesi i tij i autorizuar, në emër të tij dhe nën përgjegjësinë e tij, me kusht që detyrimet përkatëse të specifikohen në aktin e përfaqësimit me shkrim.

Pjesa II

Ekzaminimi i tipit BE (bazuar në modulin B)

1. Ekzaminimi i tipit të BE-së është pjesa e një procedure të vlerësimit të konformitetit në të cilën një organ i notifikuar shqyrton projektimin teknik dhe zhvillimin e një produkti me elementë digjitalë dhe proceset e trajtimit të vulnerabiliteteve të vendosura nga prodhuesi dhe vërteton se një produkt me elementë digjitalë plotëson kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij ligji dhe se prodhuesi plotëson kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksi I të këtij ligji.
2. Ekzaminimi i tipit të BE-së kryhet duke vlerësuar përshtatshmërinë e projektimit teknik dhe zhvillimit të produktit me elementë digjitalë përmes ekzaminimit të dokumentacionit teknik dhe provave mbështetëse të përmendura në pikën 3 të kësaj pjese dhe ekzaminimit të mostrave të një ose më shumë pjesëve kritike të produktit (kombinimi i llojit të prodhimit dhe llojit të projektimit).
3. Prodhuesi paraqet një aplikim për ekzaminimin e tipit të BE-së në një organ të vetëm të notifikuar sipas zgjedhjes së tij.
Aplikimi përfshin:
3.1. Emrin dhe adresën e prodhuesit dhe, nëse aplikimi paraqitet nga përfaqësuesi i autorizuar, emrin dhe adresën përfaqësuesit të autorizuar;
3.2. Një deklaratë me shkrim se i njëjti aplikim nuk është paraqitur në asnjë organ tjetër të notifikuar;
3.3. Dokumentacioni teknik, i cili bën të mundur vlerësimin e konformitetit të produktit me elementët digjitalë me kërkesat thelbësore të zbatueshme të sigurisë kibernetike siç përcaktohet në pjesën I të aneksit I të këtij ligji dhe proceset e trajtimit të vulnerabiliteteve të prodhuesit të

përcaktuara në pjesën II të aneksit I të këtij ligji dhe përfshin një analizë të përshtatshme dhe vlerësimin e risqeve. Dokumentacioni teknik specifikon kërkesat e zbatueshme dhe mbulon, për aq sa është e rëndësishme për vlerësimin, projektimin, prodhimin dhe funksionimin e produktit me elementë digjitalë. Dokumentacioni teknik përmban, kudo që është e zbatueshme, të paktën elementët e përcaktuar në aneksin VII të këtij ligji;

3.4. Provat mbështetëse për përshtatshmërinë e zgjidhjeve teknike të projektimit dhe zhvillimit dhe proceseve të trajtimit të vulnerabiliteteve. Kjo provë mbështetëse/evidencë përmend çdo dokument që është përdorur, veçanërisht kur standardet përkatëse të harmonizuara ose specifikimet teknike nuk janë zbatuar plotësisht. Provat mbështetëse/evidencat përfshijnë, kur është e nevojshme, rezultatet e testeve të kryera nga laboratori përkatës i prodhuesit, ose nga një laborator tjetër testimi në emër të tij dhe nën përgjegjësinë e tij.

4. Organi i notifikuar:

4.1. Shqyrton dokumentacionin teknik dhe provat mbështetëse/eviencat për të vlerësuar përshtatshmërinë e dizajnit teknik dhe zhvillimit të produktit me elementë digjitalë me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij kigji dhe të proceseve të trajtimit të vulnerabiliteteve të vendosura nga prodhuesi me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksit I të këtij ligji;

4.2. Verifikojnë që kampionet janë zhvilluar ose prodhuar në përputhje me dokumentacionin teknik dhe identifikojnë elementët që janë projektuar dhe zhvilluar në përputhje me dispozitat e zbatueshme të standardeve të harmonizuara përkatëse ose specifikimeve teknike, si dhe elementët që janë projektuar dhe zhvilluar pa zbatuar dispozitat përkatëse të atyre standardeve;

4.3. Të kryejë ekzaminimet dhe testet e duhura, ose t'i kryejë ato, për të kontrolluar që, kur prodhuesi ka zgjedhur të zbatojë zgjidhjet në standardet të harmonizuara përkatëse ose specifikimet teknike për kërkesat e përcaktuara në aneksin I të këtij ligji, ato janë zbatuar saktë;

4.4. Të kryejë ekzaminimet dhe testet e duhura, ose t'i kryejë ato, për të kontrolluar që, kur zgjidhjet në standardet të harmonizuara përkatëse ose specifikimet teknike për kërkesat e përcaktuara në aneksin I të këtij lkigjinuk janë zbatuar , zgjidhjet e miratuara nga prodhuesi plotësojnë kërkesat përkatëse thelbësore të sigurisë kibernetike;

4.5. Dakordësim me prodhuesin për vendndodhjen se ku do të kryhen ekzaminimet dhe testet.

5. Organi i notifikuar harton një raport vlerësimi që regjistron aktivitetet e ndërmarra në përputhje me pikën 4 të kësaj pjese dhe rezultatet e tyre. Pa rënë ndesh me detyrimet e tij ndaj autoriteteve notifikuese, organi i notifikuar publikon përmbajtjen e atij raporti, plotësisht ose pjesërisht, vetëm me dakordësinë e prodhuesit.

6. Kur lloji dhe proceset e trajtimit të vulnerabiliteteve plotësojnë kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji, organi i notifikuar i lëshon prodhuesit një certifikatë ekzaminimi të tipit të BE-së. Certifikata përmban emrin dhe adresën e prodhuesit, përfundimet e ekzaminimit, kushtet nëse ka, për vlefshmërinë e saj dhe të dhënat e nevojshme për identifikimin e llojit të miratuar dhe proceseve të trajtimit të vulnerabiliteteve. Certifikata mund të ketë një ose më shumë anekse të bashkëlidhura.

Certifikata dhe anekset e saj përmbajnë të gjithë informacionin përkatës për të lejuar konformitetin e produkteve të prodhuara ose të zhvilluara me elementët digjitalë të tipit të shqyrtuar dhe procesve të trajtimit të vulnerabiliteteve dhe për të lejuar kontrollin në shërbim.

Kur lloji dhe proceset e trajtimit të vulnerabiliteteve nuk plotësojnë kërkesat thelbësore të zbatueshme të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji, organi i notifikuar refuzon të lëshojë një certifikatë ekzaminimi të tipit të BE-së dhe informon aplikantin në përputhje me rrethanat, duke dhënë arsye të hollësishme për refuzimin e tij.

7. Organi i notifikuar qëndron i informuar për çdo ndryshim të fundit që tregon se tipi i miratuar dhe proceset e trajtimit të vulnerabiliteteve mund të mos jenë më në përputhje me kërkesat thelbësore

të zbatueshme të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji, dhe përcakton nëse ndryshime të tilla kërkojnë verifikim të mëtejshëm. Nëse po, organi i notifikuar informon prodhuesin në përputhje me rrethanat.
Prodhuesi informojnë organin e notifikuar që mban dokumentacionin teknik në lidhje me certifikatën e ekzaminimit të tipit të BE-së për të gjitha ndryshimet në tipin e miratuar dhe proceset e trajtimit të vulnerabiliteteve që mund të ndikojnë në konformitetin me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në aneksin I të këtij ligji, ose kushtet për vlefshmërinë e certifikatës. Ndryshime të tilla kërkojnë miratim shtesë në formën e një shtesë në certifikatën origjinale të ekzaminimit të tipit të BE-së.
8. Organi i notifikuar kryen auditime periodike për të siguruar që proceset e trajtimit të vulnerabiliteteve siç përcaktohet në pjesën II të aneksit I të këtij ligji zbatohen në mënyrë të përshtatshme.
9. Çdo organ i notifikuar informon autoritetet e tij notifikuese në lidhje me certifikatat e ekzaminimit të tipit të BE-së dhe çdo shtesë të tyre që ka lëshuar ose tërhequr dhe vë në dispozicion të autoriteteve të tij njoftuese, në mënyrë periodike ose me kërkesë listën e certifikatave dhe çdo shtesë të tyre të refuzuar, pezulluar ose të kufizuar nëndonjë mënyrë tjetër.
Çdo organ i notifikuar informon organet e tjera të notifikuara në lidhje me certifikatat e ekzaminimit të tipit të BE-së dhe çdo shtesë të tyre që ka refuzuar, tërhequr, pezulluar ose kufizuar në ndonjë mënyrë tjetër, dhe, sipas kërkesës, në lidhje me certifikatat dhe shtesat e tyre që ka lëshuar.
Ministria përgjegjëse dhe organet të notifikuara mund të marrin një kopje të certifikatave të ekzaminimit të tipit të BE-së dhe çdo shtesë të tyre. Sipas kërkesës, ministria përgjegjëse mund të marrë një kopje të dokumentacionit teknik dhe rezultatet e ekzaminimeve të kryera nga organi i notifikuar. Organi i notifikuar mban një kopje të certifikatës së ekzaminimit të tipit të BE-së, anekseve dhe shtesave të saj, si dhe dosjen teknike duke përfshirë dokumentacionin e paraqitur nga prodhuesi, deri në skadimin e vlefshmërisë së certifikatës.
10. Prodhuesi mban një kopje të certifikatës së ekzaminimit të tipit të BE-së, anekseve dhe shtesave të saj së bashku me dokumentacionin teknik në dispozicion të autoriteteve kombëtare për 10 vjet pasi produkti me elementë digjitalë të jetë vendosur në treg ose për periudhën e mbështetjes, nëse kjo e fundit është më e gjatë.
11. Përfaqësuesi i autorizuar i prodhuesit mund të paraqesë aplikimin e përmendur në pikën 3 të kësaj pjese dhe të përmbushë detyrimet e përcaktuara në pikat 7 dhe 10 të kësaj pjese, me kusht që detyrimet përkatëse të specifikohen në aktin e përfaqësimit me shkrim .

Pjesa III

Konformiteti bazuar në llojin në kontrollin e brendshëm të prodhimit (bazuar në modulin C)

1. Konformiteti bazuar në llojin në kontrollin e brendshëm të prodhimit është pjesa e një procedure të vlerësimit të konformitetit me anë të së cilës prodhuesi përmbush detyrimet e përcaktuara në pikat 2 dhe 3 të kësaj pjese dhe siguron dhe deklaron se produktet me elementë digjitalë janë në konformitet me llojin e përshkruar në certifikatën e ekzaminimit të tipit të BE-së dhe plotësojnë kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij ligji dhe se prodhuesi plotëson kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksit I të këtij ligji.
2. Prodhimi.
Prodhuesi marr të gjitha masat e nevojshme në mënyrë që prodhimi dhe monitorimi i tij të sigurojë konformitetin e produkteve të prodhuara me elementët digjitalë me tipin e miratuar të përshkruar në certifikatën e ekzaminimit të tipit të BE-së dhe me kërkesat thelbësore të sigurisë kibernetike siç

përcaktohet në pjesën I të aneksit I të këtij ligji dhe të sigurojë që prodhuesi të plotësojë kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksit I të këtij ligji.
3. Shënimi i konformitetit dhe deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian.
3.1. Prodhuesi vendos markimin CE në çdo produkt individual me elementë digjitalë që është në konformitet me llojin e përshkruar në certifikatën e ekzaminimit të tipit të BE-së dhe plotëson kërkesat e zbatueshme të përcaktuara në këtë ligj.
3.2. Prodhuesi harton një deklaratë me shkrim të konformitetit për një model produkti dhe e mban në dispozicion të autoriteteve kombëtare për 10 vjet pasi produkti me elementë digjitalë të jetë vendosur në treg ose për periudhën e mbështetjes, nëse kjo e fundit është më e gjatë. Deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian identifikon modelin e produktit për të cilin është hartuar. Një kopje e deklaratës së konformitetit në përputhje me standardet e Bashkimit Evropian u vihet në dispozicion autoriteteve përkatëse sipas kërkesës.
4. Përfaqësues i autorizuar.
Detyrimet e prodhuesit të përcaktuara në pikën 3 të kësaj pjese mund të përmbushen nga përfaqësuesi i tij i autorizuar, në emër të tij dhe nën përgjegjësinë e tij, me kusht që detyrimet përkatëse të specifikohen në aktin e përfaqësimit me shkrim.

Pjesa IV

Konformiteti bazuar në sigurimin e plotë të cilësisë (bazuar në modulin H)

1. Konformiteti i bazuar në sigurimin e plotë të cilësisë është procedura e vlerësimit të konformitetit me anë të së cilës prodhuesi përmbush detyrimet e përcaktuara në pikat 2 dhe 5 të kësaj pjese dhe siguron dhe deklaron me përgjegjësinë e tij të vetme se produktet me elementë digjitalë ose kategoritë e produkteve plotësojnë kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksi I të këtij ligji dhe se proceset e trajtimit të vulnerabiliteteve të vendosura nga prodhuesi plotësojnë kërkesat e përcaktuara në pjesën II të aneksit I të këtij ligji.
2. Projektimi, zhvillimi, prodhimi dhe trajtimi i vulnerabiliteteve së produkteve me elementë digjitalë.
Prodhuesi operon një sistem të miratuar të cilësisë siç specifikohet në pikën 3 të kësaj pjese për projektimin, zhvillimin dhe inspektimin dhe testimin e produktit përfundimtar të produkteve me elementë digjitalë dhe për trajtimin e vulnerabiliteteve, të ruajë efektivitetin e tij gjatë gjithë periudhës së mbështetjes dhe do t'i nënshtrohet mbikëqyrjes siç specifikohet në pikën 4 të kësaj pjese.
3. Sistemi i cilësisë.
3.1. Prodhuesi paraqet një aplikim për vlerësimin e sistemit të tij të cilësisë tek organi i notifikuar i zgjedhur prej tij, për produktet me elementë digjitalë përkatës .
Aplikimi përfshin:
a) emrin dhe adresën e prodhuesit dhe, nëse aplikimi paraqitet nga përfaqësuesi i autorizuar, emrin dhe adresën e përfaqësuesit të autorizuar;
b) dokumentacioni teknik për një model të secilës kategori produktesh me elementë digjitalë të synuar për t'u prodhuar ose zhvilluar. Dokumentacioni teknik, kudo që është e aplikueshme, përmban të paktën elementët e përcaktuar në aneksin VII të këtij ligji;
c) dokumentacionin në lidhje me sistemin e cilësisë; dhe
ç) një deklaratë me shkrim se i njëjti aplikim nuk është paraqitur në asnjë organ tjetër të notifikuar.
3.2. Sistemi i cilësisë siguron pajtueshmërinë e produkteve me elementët digjitalë me kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij ligji dhe

përputhshmërinë e proceseve të trajtimit të vulnerabiliteteve të vendosura nga prodhuesi me kërkesat e përcaktuara në pjesën II të aneksit I të këtij ligji.
Të gjithë elementët, kërkesat dhe dispozitat e miratuara nga prodhuesi dokumentohen në mënyrë sistematike dhe të rregullt në formën e politikave, procedurave dhe udhëzimeve të shkruara. Ky dokumentacion i sistemit të cilësisë lejon një interpretim të qëndrueshëm të programeve, planeve, manualeve dhe të dhënave/regjistrave të cilësisë.
Në veçanti, përmban një përshkrim të përshtatshëm të:

a) objektivave të cilësisë dhe struktura organizative, përgjegjësitë dhe kompetencat e drejtuesve të lartë në lidhje me projektimin, zhvillimin, cilësinë e produktit dhe trajtimin e vulnerabiliteteve;
b) specifikimet teknike të projektimit dhe zhvillimit, duke përfshirë standardet, që do të zbatohen dhe, kur standardet të harmonizuara përkatëse ose specifikimet teknike nuk zbatohen plotësisht, mjetet që do të përdoren për të siguruar që kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën I të aneksit I të këtij ligjiqë zbatohen për produktet me elementë digjitale do të përmbushen;
c) specifikimet procedurale, përfshirë standardet, që do të zbatohen dhe, kur standardet të harmonizuara përkatëse ose specifikimet teknike nuk do të zbatohen plotësisht, mjetet që do të përdoren për të siguruar që kërkesat thelbësore të sigurisë kibernetike të përcaktuara në pjesën II të aneksit I të këtij ligji që zbatohen për prodhuesin do të përmbushen;
ç) kontrolli i projektimit dhe zhvillimit, si dhe teknikat e verifikimit të projektimit dhe zhvillimit, proceset dhe veprimet sistematike që do të përdoren gjatë projektimit dhe zhvillimit të produkteve me elementë digjitalë që i përkasin kategorisë së produktit të mbuluar;
d) teknikat përkatëse të prodhimit, kontrollit të cilësisë dhe sigurimit të cilësisë, proceseve dhe veprimeve sistematike që do të përdoren;
dh) ekzaminimet dhe testet që do të kryhen para, gjatë dhe pas prodhimit, dhe frekuenca me të cilën ato do të kryhen;
e) të dhënat e cilësisë, të tilla si raportet e inspektimit dhe të dhënat e testimit, të dhënat e kalibrimit dhe raportet e kualifikimit të personelit;
f) mjetet e monitorimit të arritjes së dizajnit të kërkuar dhe cilësisë së produktit dhe funksionimit efektiv të sistemit të cilësisë.

3.3 Organi i notifikuar vlerëson sistemin e cilësisë për të përcaktuar nëse ai plotëson kërkesat e përmendura në pikën 3.2.
Ai prezumon konformitet me ato kërkesa në lidhje me elementët e sistemit të cilësisë që përputhen me specifikimet përkatëse të standardit kombëtar që zbaton standardin harmonizuar përkatës ose specifikimin teknik.
Përveç përvojës në sistemet e menaxhimit të cilësisë, ekipi i auditimit të ketë të paktën një anëtar me përvojë si vlerësues në fushën përkatëse të produktit dhe teknologjinë e produktit përkatës dhe të ketë njohuri për kërkesat e zbatueshme të përcaktuara në këtë ligj. Auditi përfshin një vizitë vlerësimi në ambientet e prodhuesit, kur ekzistojnë ambiente të tilla. Ekipi i auditimit rishikon dokumentacionin teknik të përmendur në shkronjën "b" të pikës 3.1, për të verifikuar aftësinë e prodhuesit për të identifikuar kërkesat e zbatueshme të përcaktuara në këtë ligj dhe për të kryer ekzaminimet e nevojshme me qëllim të sigurimit të përputhshmërisë së produktit me elementët digjitalë me ato kërkesa.
Prodhuesi ose përfaqësuesi i tij i autorizuar njoftohet për vendimin.
Njoftimi përmban konkluzionet e auditimit dhe vendimin e arsyetuar të vlerësimit.
3.3. Prodhuesi marrë përsipër të përmbushë detyrimet që rrjedhin nga sistemi i cilësisë siç është miratuar dhe ta mbajë atë në mënyrë që të mbetet i përshtatshëm dhe efikas.

3.4. Prodhuesi mbantë informuar organin e notifikuar që ka miratuar sistemin e cilësisë për çdo ndryshim të synuar në sistemin e cilësisë.
Organi i notifikuar vlerëson çdo ndryshim të propozuar dhe vendos nëse sistemi i ndryshuar i cilësisë do të vazhdojë të përmbushë kërkesat e përmendura në pikën 3.2 ose nëse është i nevojshëm një rivlerësim.
Ai njofton prodhuesin për vendimin e tij. Njoftimi përmban konkluzionet e ekzaminimit dhe vendimin e arsyetuar të vlerësimit.
4. Mbikëqyrja nën përgjegjësinë e organit të notifikuar.
4.1. Qëllimi i mbikëqyrjes është të sigurohet që prodhuesi të përmbushë siç duhet detyrimet që rrjedhin nga sistemi i miratuar i cilësisë.
4.2. Prodhuesi, për qëllime vlerësimi, lejon organit të notifikuar të ketë akses në vendet e projektimit, zhvillimit, prodhimit, inspektimit, testimit dhe ruajtjes dhe do t'i sigurojë atij të gjithë informacionin e nevojshëm, në veçanti:

a) dokumentacionin e sistemit të cilësisë;
b) të dhënat e cilësisë siç sigurohen nga pjesa e projektimit të sistemit të cilësisë, të tilla si rezultatet e analizave, llogaritjeve dhe testeve;
c) të dhënat e cilësisë siç sigurohen nga pjesa prodhuese e sistemit të cilësisë, të tilla si raportet e inspektimit dhe të dhënat e testimit, të dhënat e kalibrimit dhe raportet e kualifikimit të personelit përkatës.

4.3. Organi i notifikuar kryen auditime periodike për t'u siguruar që prodhuesi mirëmban dhe zbaton sistemin e cilësisë dhe do t'i sigurojë prodhuesit një raport auditimi.
5. Shënimi i konformitetit dhe deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian
5.1. Prodhuesi vendos markimin CE dhe, nën përgjegjësinë e organit të notifikuar të përmendur në pikën 3.1, numrin e identifikimit të këtij të fundit në çdo produkt individual me elementë digjitalë që plotëson kërkesat e përcaktuara në pjesën I të aneksit I të këtij ligji.
5.2. Prodhuesi harton një deklaratë me shkrim të konformitetit për çdo model produkti dhe do ta mbajë atë në dispozicion të autoriteteve kombëtare për 10 vjet pasi produkti me elementë digjitalë të jetë vendosur në treg ose për periudhën e mbështetjes, nëse kjo e fundit është më e gjatë. Deklarata e konformitetit në përputhje me standardet e Bashkimit Evropian identifikon modelin e produktit për të cilin është hartuar.
Një kopje e deklaratës së konformitetit në përputhje me standardet e Bashkimit Evropian u vihet në dispozicion autoriteteve përkatëse sipas kërkesës.
6. Prodhuesi, për një periudhë që përfundon të paktën 10 vjet pasi produkti me elementë digjitalë është vendosur në treg ose për periudhën e mbështetjes, nëse kjo e fundit është më e gjatë, do të mbajë në dispozicion të autoriteteve kombëtare:

a) dokumentacionin teknik i përmendur në pikën 3.1;
b) dokumentacionin në lidhje me sistemin e cilësisë të përmendur në pikën 3.1;
c) ndryshimin e miratuar të përmendur në pikën 3.5;
ç) vendimet dhe raportet e organit të notifikuar të përmendura në pikat 3.5 dhe 4.3.

7. Çdo organ i notifikuar informon autoritetin notifikues për miratimet e sistemit të cilësisë të lëshuara ose të tërhequra dhe, periodikisht ose sipas kërkesës, vë në dispozicion të autoritetet notifikues listën e miratimeve të sistemit të cilësisë të refuzuara, pezulluara ose të kufizuara në mënyrë tjetër.
Çdo organ i notifikuar informon organet e tjera të notifikuara për miratimet e sistemit të cilësisë që ka refuzuar, pezulluar ose tërhequr dhe, sipas kërkesës, për miratimet e sistemit të cilësisë që ka lëshuar.
8. Përfaqësues i autorizuar.

Detyrimet e prodhuesit të përcaktuara në pikat 3.1, 3.5, 5 dhe 6 mund të përmbushen nga përfaqësuesi i autorizuar, në emër të tij dhe nën përgjegjësinë e tij, me kusht që detyrimet përkatëse të specifikohen në aktin e përfaqësimit me shkrim.

KRYETAR

NIKO PELESHI