RELACION

PËR
PROJEKTLIGJIN "PËR DISA SHTESA DHE NDRYSHIME NË LIGJIN NR.25/2024 PËR SIGURINË KIBERNETIKE"

I. QËLLIMI I PROJEKTAKTIT DHE OBJEKTIVAT QË SYNOHEN TË ARRIHEN

Qëllimi i projektligjit "Për disa shtesa dhe ndryshime në ligjin nr.25/2024, "Për sigurinë kibernetike" është përmirësimi dhe plotësimi i kuadrit ligjor ekzistues në fushën e sigurisë kibernetike, me qëllim rritjen e nivelit të mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit, forcimin e kapaciteteve institucionale për reagimin ndaj incidenteve të sigurisë kibernetike, si dhe përafrimin e mëtejshëm të legjislacionit kombëtar me standardet dhe praktikat e Bashkimit Evropian.

Në funksion të këtij qëllimi, projektligji synon forcimin e rolit, kompetencave dhe përgjegjësive të Autoritetit Kombëtar për Sigurinë Kibernetike në drejtim të koordinimit, mbikëqyrjes dhe reagimit ndaj incidenteve kibernetike, si dhe përmirësimin e organizimit dhe funksionimit të CSIRT-eve sektoriale, duke synuar njëkohësisht forcimin e bashkëpunimit dhe koordinimit ndërinstitucional në nivel kombëtar. Gjithashtu, parashikohet krijimi dhe zbatimi i mekanizmave të rinj të monitorimit dhe vlerësimit të përputhshmërisë, përmes detyrimit të vetëdeklarimit të masave të sigurisë kibernetike dhe raportimit të rregullt nga operatorët e infrastrukturave të informacionit, si dhe rregullimi i procedurave për deklarimin e hostimit dhe administrimin e sistemeve, rrjeteve dhe infrastrukturave të informacionit. Projektligji synon gjithashtu krijimin e Grupit të Bashkëpunimit të Inteligjencës Kibernetike me qëllim shkëmbimin e informacionit dhe forcimin e bashkëpunimit strategjik ndërinstitucional si dhe përmirësimi i mekanizmave të kontrollit dhe rritja e efektivitetit të masave administrative dhe sanksioneve në rast të mosrespektimit të detyrimeve ligjore.

II. VLERËSIMI I PROJEKTAKTIT NË RAPORT ME PROGRAMIN POLITIK TË KËSHILLIT TË MINISTRAVE, ME PROGRAMIN ANALITIK TË AKTEVE DHE DOKUMENTE TË TJERA POLITIKE

Projektligji është në përputhje me Programin Politik të Këshillit të Ministrave për transformimin digjital dhe forcimin e sigurisë kibernetike, si dhe me objektivat e Strategjisë Kombëtare për Sigurinë Kibernetike.

Gjithashtu, projektligji mbështet procesin e integrimit evropian të Republikës së Shqipërisë dhe përafrimin progresiv të legjislacionit kombëtar me acquis communautaire në fushën e sigurisë kibernetike.

III. ARGUMENTIMI I PROJEKTAKTIT LIDHUR ME PËRPARËSITË, PROBLEMATIKAT, EFEKTET E PRITSHME

Zbatimi i ligjit nr.25/2024, "Për sigurinë kibernetike" ka evidentuar nevojën për disa plotësime dhe saktësime të kuadrit ligjor, me qëllim rritjen e efikasitetit të masave të sigurisë dhe të mekanizmave mbikëqyrës.

Projektligji sjell një sërë risish kryesore në kuadër të forcimit të kuadrit ligjor në fushën e sigurisë kibernetike dhe rritjes së nivelit të mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit.

Në radhë të parë, ai përforcon kompetencat e Autoritetit Kombëtar për Sigurinë Kibernetike, duke i njohur funksione shtesë në fushën e prokurimeve të përqendruara për trajnimet në sigurinë kibernetike, si dhe në procesin e autorizimit të organeve të vlerësimit të konformitetit në këtë fushë.

Gjithashtu, projektligji rikoncepton organizimin dhe funksionimin e CSIRT-eve sektoriale, duke forcuar koordinimin ndërmjet strukturave përgjegjëse për menaxhimin e incidenteve të sigurisë kibernetike në nivel sektorial dhe kombëtar.

Një risi tjetër e rëndësishme është krijimi i bazës ligjore për vetëdeklarimin e masave të sigurisë kibernetike nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, si një instrument paraprak për monitorimin dhe vlerësimin e zbatimit të masave të sigurisë kibernetike nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.

Projektligji vendos gjithashtu detyrimin për deklarimin e mënyrës së hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturave të informacionit, duke rritur

transparencën dhe nivelin e kontrollit mbi infrastrukturat që mbështesin shërbimet kritike.
Në të njëjtën kohë, parashikohet zbatimi i detyrueshëm i masave për bllokimin, filtrimin, kufizimin ose neutralizimin e treguesve të kompromet imit (IOC), treguesve të sulmeve (IOA) dhe vulnerabiliteteve të komunikuara nga Autoriteti, me qëllim forcimin e mbrojtjes proaktive ndaj kërcënimeve kibernetike.
Projektligji forcon gjithashtu kuadrin e certifikimit të sigurisë kibernetike, duke nxitur përdorimin e produkteve, shërbimeve dhe proceseve TIK të certifikuara, në përputhje me skemat kombëtare dhe evropiane të certifikimit si dhe parashikimin kur operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin e përdorimit të produkteve, shërbimeve dhe proceseve TIK të certifikuara, në përputhje me skemat kombëtare dhe evropiane të certifikimit të sigurisë kibernetike.
Një risi e rëndësishme institucionale është krijimi i Grupit të Bashkëpunimit për Inteligjencën Kibernetike, si mekanizëm për shkëmbimin e informacionit, analizën e kërcënimeve dhe forcimin e koordinimit strategjik ndërmjet institucioneve përgjegjëse në fushën e sigurisë dhe mbrojtjes.
Gjithashtu, projektligji forcon sistemin e kundërvajtjeve administrative dhe sanksioneve, duke parashikuar shkelje të reja që lidhen me detyrimet e vetëdeklarimit, deklarimin e hostimit dhe moszbatimin e masave të sigurisë të urdhëruara nga Autoriteti, me qëllim rritjen e efektivitetit të zbatimit të ligjit.
Efektet e pritshme të projektligjit konsistojnë në rritjen e nivelit të mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit, përmes forcimit të kuadrit rregullator dhe institucional në fushën e sigurisë kibernetike. Gjithashtu, pritet përmirësimi i aftësive parandaluese, monitoruese dhe reaguese ndaj incidenteve të sigurisë kibernetike, si rezultat i qartësimit të kompetencave dhe rritjes së koordinimit ndërmjet strukturave përgjegjëse. Projektligji sjell gjithashtu rritje të bashkëpunimit ndërinstitucional dhe përmirësim të shkëmbimit të informacionit ndërmjet autoriteteve dhe operatorëve të infrastrukturave të informacionit. Në të njëjtën kohë, parashikohet rritja e nivelit të përputhshmërisë së operatorëve me detyrimet ligjore, përmes mekanizmave të raportimit, vetëdeklarimit dhe mbikëqyrjes. Në tërësi, zbatimi i tij pritet të kontribuojë në forcimin e sigurisë dhe qëndrueshmërisë së shërbimeve publike dhe private që mbështeten në sisteme dhe rrjete të informacionit.

IV. VLERËSIMI I LIGJSHMËRISË, KUSHTETUTSHMËRISË DHE HARMONIZIMI ME LEGJISLACIONIN NË FUQI VENDAS E NDËRKOMBËTAR

Projektligji është hartuar në mbështetje të neneve 78, 81, pika 1 dhe 83 pika 1 të Kushtetutës, dhe është në harmoni me legjislacionin vendas në fuqi. Gjithashtu, ky projektligj nuk bie në kundërshtim me Kushtetutën dhe me marrëveshjet ndërkombëtare të ratifikuara nga Republika e Shqipërisë.

V. VLERËSIMI I SHKALLËS SË PËRAFRIMIT ME ACQUIS COMMUNAUTAIRE (PËR PROJEKTAKTET NORMATIVE)

Projektligji nuk synon përafrimin e mëtejshëm të legjislacionit kombëtar me *acquis* të BE-së dhe nuk përmban dispozita të reja për transpozimin e akteve të Bashkimit Evropian.

Ndryshimet e propozuara kanë karakter organizativ, procedural dhe teknik, me qëllim përmirësimin e kuadrit ekzistues ligjor për sigurinë kibernetike dhe forcimin e mekanizmave institucionalë për zbatimin e tij.

Megjithatë, dispozitat e projektligjit janë hartuar në përputhje me parimet, objektivat dhe praktikat më të mira të Bashkimit Evropian në fushën e sigurisë kibernetike, duke ruajtur harmoninë me Direktivën (BE) 2022/2555 të Parlamentit Evropian dhe të Këshillit, datë 14 dhjetor 2022, "Mbi masat për një nivel të lartë të përbashkët të sigurisë kibernetike në të gjithë Bashkimin Evropian, duke ndryshuar Rregulloren (BE) nr. 910/2014 dhe Direktivën (BE) 2018/1972, si dhe duke shfuqizuar Direktivën (BE) 2016/1148 (NIS 2)".

VI. PËRMBLEDHJE SHPJEGUESE E PËRMBAJTJES SË PROJEKTAKTIT

Projektligji përmban 21 nene, të cilat parashikojnë këto ndryshime dhe shtesa në ligjin nr. 25/2024, “Për sigurinë kibernetike”:

Neni 1 parashikon ndryshime dhe shtesa në nenin 5 të ligjit, duke riformuluar përkufizimin e CSIRT-it sektorial, duke shtuar përkufizimin e inteligjencës kibernetike, si dhe përkufizimet e organit të blerjes së përqendruar për trajnimet në fushën e sigurisë kibernetike dhe të vetëdeklarimit të masave të sigurisë kibernetike.

Neni 2 parashikon ndryshime dhe shtesa në nenin 9 të ligjit, me qëllim zgjerimin e kompetencave të Autoritetit Kombëtar për Sigurinë Kibernetike, duke forcuar rolin e tij në mbrojtjen e qytetarëve dhe grupeve vulnerabël në hapësirën kibernetike, ushtrimin e funksioneve të organit kombëtar të certifikimit të sigurisë kibernetike, autorizimin e organeve të vlerësimit të konformitetit, organizimin e prokurimeve të përqendruara për trajnimet në fushën e sigurisë kibernetike.

Neni 3 parashikon ndryshime në nenin 12 të ligjit, duke saktësuar detyrimin e subjekteve për të dhënë informacion gjatë procesit të identifikimit të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe duke përcaktuar që lista e këtyre operatorëve të përditësohet të paktën një herë në dy vjet.

Neni 4 përmirëson dispozitat që lidhen me kompetencat e CSIRT-it Kombëtar, duke përcaktuar procedurat për kryerjen e simulimeve në rrjetet dhe sistemet e operatorëve mbi bazën e vulnerabiliteteve të evidentuara, si dhe mënyrën e miratimit të procedurave përkatëse.

Neni 5 ndryshon nenin 15 të ligjit, duke përcaktuar institucionet përgjegjëse për ngritjen dhe organizimin e CSIRT-eve sektoriale.

Neni 6 riformulon një nga detyrat e CSIRT-it sektorial lidhur me njoftimin e menjëhershëm të CSIRT-it Kombëtar për incidentet e sigurisë kibernetike dhe informimin e tij edhe në rastet e zgjidhjes së shpejtë të incidenteve.

Neni 7 përmirëson detyrimet e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, duke forcuar bashkëpunimin me CSIRT-in Kombëtar dhe CSIRT-et sektoriale, si dhe duke parashikuar detyrimin për zbatimin e masave teknike për bllokimin, filtrimin, kufizimin, detektimin ose neutralizimin e treguesve të kompromet imit (IOC), treguesve të sulmeve (IOA) dhe korrigjimin e vulnerabiliteteve të komunikuara nga Autoriteti.

Neni 8 parashikon procedurat dhe kriteret për regjistrimin e organeve të vlerësimit të konformitetit për vlerësimin e masave të sigurisë kibernetike.

Neni 9 shton nenet 20/1 dhe 20/2, duke krijuar bazën ligjore për vetëdeklarimin e masave të sigurisë kibernetike, si dhe për vetëdeklarimin e hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturave të informacionit, me qëllim monitorimin e nivelit të sigurisë kibernetike dhe evidentimin e ekspozimit teknologjik të operatorëve.

Neni 10 ndryshon dispozitën lidhur me organizimin dhe funksionimin e CERT-it, duke parashikuar edhe mënyrën e pagesës së ekspertëve të angazhuar në këtë strukturë.

Neni 11 ndryshon nenin 30 të ligjit, duke zgjeruar detyrimet lidhur me mbrojtjen dhe konfidencialitetin e informacionit.
Neni 12 ndryshon nenin 31 të ligjit, duke shtuar detyrimin për raportimin e rezultateve të dokumentimit të aktiviteteve të monitorimit dhe kontrollit.
Neni 13 shton nenin 33/1, duke krijuar Grupin e Bashkëpunimit për Inteligjencën Kibernetike, përcakton institucionet pjesëmarrëse, detyrat kryesore, mënyrën e organizimit dhe funksionimit të tij, si dhe procedurat për koordinimin ndërinstitucional.
Neni 14 ndryshon nenin 39 të ligjit, duke zëvendësuar kriterin e akreditimit me autorizimin nga autoriteti përgjegjës për organet e vlerësimit të konformitetit.
Neni 15 përmirëson dispozitat mbi certifikimin e sigurisë kibernetike, duke inkurajuar përdorimin e produkteve, proceseve dhe shërbimeve TIK të certifikuara dhe duke parashikuar miratimin me vendim të Këshillit të Ministrave të listës së operatorëve për të cilët përdorimi i tyre është i detyrueshëm.
Neni 16 ndryshon nenin 42 të ligjit, duke përcaktuar se tarifat për regjistrimin dhe autorizimin e organeve të vlerësimit të konformitetit miratohen me vendim të Këshillit të Ministrave.
Neni 17 zgjeron rastet e kundërvajtjeve administrative, duke përfshirë mosdhënien e informacionit gjatë procesit të identifikimit, mosplotësimin e vetëdeklarimeve, mosdeklarimin e hostimit dhe administrimit të infrastrukturave të informacionit, si dhe moszbatimin e masave teknike të sigurisë të komunikuara nga Autoriteti.
Neni 18 përditëson masat administrative të gjobave për kundërvajtjet e parashikuara në nenin 44 të ligjit, duke përcaktuar intervalet përkatëse të sanksioneve sipas natyrës së shkeljes.
Neni 19 zgjeron Aneksin I të ligjit, duke përfshirë në sektorin e Administratës Publike edhe subjektet e administratës publike të vetëqeverisjes vendore.
Neni 20 përcakton organet përgjegjëse dhe afatet për nxjerrjen e akteve nënligjore në zbatim të dispozitave të reja të ligjit nr.25/2024, "Për sigurinë kibernetike".
Neni 21 përcakton hyrjen në fuqi të këtij ligji.

VII. INSTITUCIONET DHE ORGANET QË NGARKOHEN PËR ZBATIMIN E KËTIJ PROJEKTAKTI

Për zbatimin e këtij ligji ngarkohen Autoriteti Kombëtar për Sigurinë Kibernetike, operatorët e infrastrukturave kritike të informacionit, operatorët e infrastrukturave të

rëndësishme të informacionit, institucionet rregullatore sipas sektorëve, operatori qeveritar që menaxhon infrastrukturat qeveritare, institucionet anëtare të Grupit i Bashkëpunimit për Inteligjencën Kibernetike.

VIII. PERSONAT DHE INSTITUCIONET QË KANË KONTRIBUAR NË HARTIMIN E PROJEKTAKTIT

Projektligji është hartuar nga Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK).

Projektligji "Për disa shtesa dhe ndryshime në ligjin nr. 25/2024 "Për sigurinë kibernetike"", në zbatim të ligjit nr. 146/2014 "Për njoftimin dhe konsultimin publik", i është nënshtruar procesit të konsultimit publik, nëpërmjet publikimit të tij në portalin "Regjistri Elektronik për Njoftimet dhe Konsultimet Publike" (RENJKP), për një periudhë prej 20 ditësh pune, nga data 23.6.2026 deri më 21.7.2026.

Projektligji dhe relacioni shoqërues u publikuan në portalin "Regjistri Elektronik për Njoftimet dhe Konsultimet Publike", duke iu dhënë mundësi të gjitha palëve të interesuara për të paraqitur komentet, sugjerimet dhe rekomandimet e tyre lidhur me projektaktin.

Gjithashtu, më datë 27.7.2026, Autoriteti Kombëtar për Sigurinë Kibernetike organizoi në ambientet e tij takime konsultative me grupet e interesit të prekura nga projektligji. Pjesëmarrësit në këto takime u njoftuan paraprakisht nga Autoriteti nëpërmjet shkresave zyrtare dhe postës elektronike. Gjatë takimeve u prezantuan risitë dhe ndryshimet kryesore të propozuara në projektligj dhe përfaqësuesit e grupeve të interesit u ftuan të shprehnin komentet dhe sugjerimet e tyre.

Në këto takime morën pjesë përfaqësues të institucioneve shtetërore, operatorë të infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe përfaqësues të sektorit bankar. Numri total i pjesëmarrësve në këto takime ishte 75 persona.

Gjatë procesit të konsultimit publik janë paraqitur komente dhe sugjerime nga subjekte të sektorit të komunikimeve elektronike, sektorit bankar dhe financiar, organizata përfaqësuese të biznesit dhe investitorëve, si dhe institucione publike, ndër të cilat *Abissnet* sh.a., *Vodafone Albania* sh.a., *One Albania*, Dhoma Amerikane e Tregtisë, Shoqata Shqiptare e Bankave, Shoqata e Investitorëve të Huaj në Shqipëri, AKEP dhe AKSIK.

Sugjerimet e dërguara janë shqyrtuar nga Autoriteti, dhe janë reflektuar në raportin individual të konsultimit publik.

Projektligji i është dërguar për mendim të gjitha ministrive, Ministrit të Shtetit për Administratën Publike, Ministrit të Shtetit dhe Kryenegociator, AKSHI-t, APP-së, SHISH, AKEP, Bankës së Shqipërisë dhe Shkollës Shqiptare të Administratës Publike.

Janë shprehur dakord Ministria për Evropën dhe Punët e Jashtme, Ministria e Punëve të Brendshme, Ministria e Mbrojtes, Ministria e Bujqësisë dhe Zhvillimit Rural, Ministri i Shtetit dhe Kryenegociator, Ministria e Arsimit, Ministria e Mjedisit, Ministria e Ekonomisë dhe Inovacionit, Ministria e Turizmit, Kulturës dhe Sportit dhe SHISH.

Nëpërmjet sistemit *e-aktet* kanë sjellë komente institucionet e mëposhtme:

I. **Ministria e Drejtësisë,** është shprehur si vijon:

1. Pika 1, e nenit 1, të projektligjit rekomandojmë që të rishikohet në kushtet kur është e paqartë se përse CSIRT-sektorial do të jetë përgjegjës vetëm për mbikëqyrjen e bankave apo institucionit rregullator për bankat në kushtet kur incidentet e sigurisë kibernetike mund të ndodhin dhe për institucione të tjera financiare. Ky rekomandim vlen edhe për parashikimet e nenit 5 të projektligjit.

<u>Përgjigje:</u> Dispozita e referuar është rishikuar në rëflektim të komentit të Bankës së Shqipërisë dhe si rrjedhojë CSIRT-i sektorial nuk do të ngrihet pranë institucionit rregullator për bankat. (Shih komentin në pjesën përkatëse të bashkërendimit të këtij institucioni).

2. Sa i përket pikës 3, të këtij neni sugjerojmë rishikimin e tij në kushtet kur realizimi i trajnimeve në fushën e sigurisë kibernetike nuk mund të kryhet nëpërmjet procedurave të prokurimit publik. Ky sugjerim, vjen si pasojë e faktit që në shkronjën *"i"*, të nenit 9, të ligjit nr. 25/2024, parashikohet se: *"Autoriteti, me urdhër të drejtorit të përgjithshëm dhe në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, zhvillon dhe nxit, sa herë vlerësohet e nevojshme, trajnime për personelin e këtyre operatorëve, në kuadër të përmbushjes me efektivitet të lartë të detyrave".* Si rrjedhojë, është detyrë funksionale e Autoritetit Kombëtar për Sigurinë Kibernetike, kryerja e trajnimeve

në këtë fushë. Ky rekomandim të mbahet në konsideratë edhe për shkronjën *"k"*, të pikës 3, të nenit 2, të projektligjit.

Përgjigje: Nuk është marrë në konsideratë. Parashikimi i pikës 3 të nenit përkatës të projektligjit nuk bie ndesh me përcaktimet e ligjit nr.25/2024, "Për sigurinë kibernetike" dhe as me kompetencën e Autoritetit Kombëtar për Sigurinë Kibernetike (AKSK) për zhvillimin dhe nxitjen e trajnimeve në fushën e sigurisë kibernetike.

Në këtë drejtim, vlen të theksohet se parashikimi i projektligjit nuk lidhet me trajnime të organizuara ose të zhvilluara drejtpërdrejt nga AKSK-ja, në kuptim të ushtrimit të funksionit të saj për ndërgjegjësimin dhe ngritjen e kapaciteteve në fushën e sigurisë kibernetike. Dispozita synon mundësimin e trajnimeve të specializuara profesionale dhe teknike, të cilat ofrohen nga trupa, organizma ose ofrues të specializuar në fushën e sigurisë kibernetike, të njohur në nivel ndërkombëtar dhe që, në përfundim të programeve përkatëse, ofrojnë certifikime profesionale të njohura në fushën e sigurisë kibernetike.

Për rrjedhojë, bëhet fjalë për shërbime të specializuara që kërkojnë përcaktimin e specifikimeve teknike dhe profesionale në përputhje me nevojat konkrete të operatorëve, si dhe përzgjedhjen e ofruesve që disponojnë ekspertizën, metodologjinë, programet dhe certifikimet përkatëse. Në këto kushte, realizimi i tyre kërkon ndjekjen e procedurave përkatëse të prokurimit publik, në përputhje me legjislacionin në fuqi për prokurimin publik.

Nga ana tjetër, shkronja "i", e nenit 9, të ligjit nr. 25/2024, parashikon se Autoriteti, me urdhër të drejtorit të Përgjithshëm dhe në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, zhvillon dhe nxit, sa herë vlerësohet e nevojshme, trajnime për personelin e këtyre operatorëve. Kjo dispozitë përcakton një kompetencë dhe përgjegjësi funksionale të AKSK-së, por nuk nënkupton që të gjitha trajnimet e nevojshme duhet të zhvillohen nga vetë Autoriteti apo që Autoriteti nuk mund të kontraktojë ofrues të specializuar për realizimin e trajnimeve profesionale.

Në ushtrim të kompetencave të saj, AKSK vlerëson dhe analizon nivelin e sigurisë kibernetike të sistemeve të infrastrukturave kritike dhe të rëndësishme të informacionit dhe, në këtë proces, identifikon edhe boshllëqet në burimet njerëzore,

njohuritë dhe kapacitetet profesionale të operatorëve. Mbi bazën e këtyre vlerësimeve dhe të analizës së riskut në nivel kombëtar, përcaktohen fushat prioritare dhe nevojat konkrete për ngritjen e kapaciteteve profesionale.

Në këtë kuadër, AKSK nuk synon të zëvendësojë detyrimin e operatorëve për trajnimin e vazhdueshëm të personelit të tyre. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të sigurojnë në mënyrë të vazhdueshme trajnimin dhe ndërgjegjësimin e personelit të tyre, si pjesë e masave organizative të sigurisë kibernetike. Ndërhyrja e parashikuar në projektligj synon të adresojë nevoja specifike dhe boshllëqe të identifikuara në nivel sektorial dhe kombëtar, të cilat kërkojnë programe të specializuara dhe certifikime profesionale.

Për këtë arsye, AKSK, bazuar në vlerësimin e nevojave dhe në ekspertizën e saj teknike, do të përcaktojë fushat dhe kërkesat specifike për trajnimet, ndërsa realizimi i trajnimeve do të kryhet nga trupa ose organizma të specializuar dhe të njohur ndërkombëtarisht, nëpërmjet procedurave përkatëse të prokurimit publik. Këto trajnime do të synojnë, sipas rastit, përfitimin e certifikimeve profesionale të njohura ndërkombëtarisht, duke kontribuar në rritjen e kapaciteteve të specializuara të personelit të operatorëve.

Për rrjedhojë, përdorimi i procedurave të prokurimit publik në këtë rast nuk bie ndesh me shkronjën "i", të nenit 9, të ligjit nr.25/2024, por përbën mekanizmin nëpërmjet të cilit Autoriteti siguron ofrimin e trajnimeve të specializuara nga subjektet profesionale përkatëse, në përputhje me nevojat e identifikuara nga Autoriteti.

Kjo qasje siguron njëkohësisht që trajnimet të mos jenë të përgjithshme apo të përsëritura, por të orientohen drejt boshllëqeve konkrete të identifikuara, si dhe të mundësojnë përfitimin e njohurive dhe certifikimeve profesionale me vlerë të njohur në fushën e sigurisë kibernetike.

3. Në lidhje me pikën 1, të nenit 2, është parashikuar që në shkronjën *"c"*, termi *"CERT"*, të hiqet. Ministria e Drejtësisë, sjell në vëmendjen tuaj se në pikën 3, të nenit 5, të ligjit nr. 25/2024, është parashikuar se: *"CERT" është Ekipi i Përgjigjes ndaj Emergjencave të Sigurisë Kibernetike pranë Autoritetit"*. Si rrjedhojë, është e paqartë arsyeja se përse termi *"CERT-it"* do të hiqet.

Përgjigje: Pranuar reflektuar.

4. Sa i përket parashikimit në pikën 2, të nenit 2, të projektligjit të togfjalëshit *"mbron qytetarët dhe grupet vulnerabël",* rekomandojmë që kjo dispozitë të hiqet, konsiderohet deklarative dhe në shkronjën *"h"*, të nenit 9, të ligjit nr. 25/2024, është parashikuar ndërgjegjësimi për të gjitha grupet e shoqërisë.

Përgjigje: Nuk është marrë në konsideratë. Parashikimi i togfjalëshit "mbron qytetarët dhe grupet vulnerabël" nuk konsiderohet një përcaktim thjesht deklarativ, por një shprehje e një objektivi të rëndësishëm të politikës publike në fushën e sigurisë kibernetike, që lidhet drejtpërdrejt me nevojën për garantimin e një niveli të përshtatshëm të mbrojtjes së shoqërisë nga rreziqet dhe kërcënimet kibernetike.

Fakti që shkronja "h", e nenit 9, të ligjit nr. 25/2024 parashikon ndërgjegjësimin për sigurinë kibernetike të të gjitha grupeve të shoqërisë, nuk e bën të panevojshëm këtë parashikim. Përkundrazi, këto dy dispozita kanë natyrë dhe funksion të ndryshëm. Ndërgjegjësimi është një nga mjetet nëpërmjet të cilave rritet niveli i sigurisë kibernetike, ndërsa mbrojtja e qytetarëve dhe e grupeve vulnerabël përfaqëson një nga objektivat që synohet të arrihet nëpërmjet masave dhe politikave të sigurisë kibernetike.

Për më tepër, përdorimi i togfjalëshit "qytetarët dhe grupet vulnerabël" synon të evidentojë shprehimisht dimensionin njerëzor dhe gjithëpërfshirës të sigurisë kibernetike, duke marrë në konsideratë se ekspozimi ndaj rreziqeve kibernetike nuk është i njëjtë për të gjitha kategoritë e shoqërisë. Grupet vulnerabël mund të kenë kapacitete, njohuri ose mundësi më të kufizuara për të identifikuar dhe për t'u mbrojtur nga kërcënimet kibernetike dhe, për këtë arsye, kërkojnë vëmendje të posaçme në kuadër të politikave kombëtare të sigurisë kibernetike.

Ky përcaktim është gjithashtu në përputhje me qasjen e ligjit nr. 25/2024, i cili e koncepton sigurinë kibernetike jo vetëm në funksion të mbrojtjes së sistemeve dhe infrastrukturave kritike e të rëndësishme të informacionit, por edhe në funksion të rritjes së ndërgjegjësimit dhe të nivelit të sigurisë kibernetike në të gjithë shoqërinë.

Për rrjedhojë, shkronja "h", e nenit 9, të ligjit nr. 25/2024, nuk përbën një përsëritje të këtij objektivi, por përcakton një kompetencë konkrete të Autoritetit për ndërgjegjësimin e grupeve të shoqërisë. Ndërsa parashikimi në projektligj përcakton një orientim të përgjithshëm të politikës dhe qëllimit të ndërhyrjes, i cili shërben edhe si bazë për përcaktimin dhe zbatimin e masave konkrete.

5. Në pikën 4, të nenit 42, të ligjit nr. 25/2024, parashikohet se të ardhurat e përfituara nga tarifa e regjistrimit derdhen në buxhetin e shtetit. Në kushtet kur në pikën 2, të nenit 16, të projektligjit është parashikuar se Këshilli i Ministrave do të miratojë edhe tarifën e autorizimit, rekomandojmë që ky ndryshim të reflektohet edhe në pikën 4, të nenit 42, të ligjit.

Përgjigje: Pranuar reflektuar.

6. Gjithashtu, të shpjegohet se përse Këshilli i Ministrave do të miratojë masën e tarifës dhe për autorizimin e organeve të vlerësimit të konformitetit për sigurinë kibernetike që duhet t`i paguajë Autoritetit në kushtet kur në pikën 23, të nenit 5, të ligjit nr. 25/2024, parashikohet se: *"Organe të vlerësimit të konformitetit për sigurinë kibernetike" janë personat juridikë kombëtarë ose ndërkombëtarë, të akredituar nga institucioni përgjegjës për akreditimin për të kryer vlerësimet dhe konformitetin e produkteve, shërbimeve dhe proceseve që lidhen me sigurinë kibernetike në TIK, si dhe vlerësimin e masave të sigurisë kibernetike të implementuara nga infrastrukturat kritike dhe të rëndësishme të informacionit".*

Përgjigje: Parashikimi që Këshilli i Ministrave të miratojë masën e tarifës që paguhet për autorizimin e organeve të vlerësimit të konformitetit (OVK) për sigurinë kibernetike është i nevojshëm për të përcaktuar në mënyrë të qartë kuadrin financiar që lidhet me ushtrimin e funksionit të autorizimit nga Autoriteti Kombëtar për Sigurinë Kibernetike (AKSK).

Përcaktimi në pikën 23, të nenit 5, të ligjit nr. 25/2024, sipas të cilit OVK-të janë persona juridikë kombëtarë ose ndërkombëtarë të akredituar nga institucioni përgjegjës për akreditimin, përcakton kriterin dhe statusin e akreditimit të këtyre organeve, por nuk rregullon çështjen e tarifës që lidhet me procesin e autorizimit të tyre nga AKSK.

Në këtë kuadër, duhet bërë dallimi ndërmjet akreditimit dhe autorizimit. Akreditimi lidhet me kompetencën teknike dhe kapacitetin e OVK-së për të kryer veprimtaritë përkatëse të vlerësimit të konformitetit dhe kryhet nga institucioni përgjegjës për akreditimin. Ndërsa autorizimi nga AKSK lidhet me verifikimin dhe njohjen e OVK-së për ushtrimin e veprimtarisë në fushën e sigurisë kibernetike, në përputhje me kërkesat dhe kuadrin rregullator të përcaktuar në legjislacionin për sigurinë kibernetike.

Për rrjedhojë, fakti që një OVK është e akredituar nuk e bën të panevojshëm procesin e autorizimit nga AKSK dhe as nuk përcakton masën e tarifës që mund të aplikohet për këtë proces. Akreditimi dhe autorizimi janë procese me qëllim, objekt dhe autoritet përgjegjës të ndryshëm.

7. Në kuadër të qartësisë që duhet të kenë aktet normative dhe shmangies së dispozitave evazive, rekomandojmë që në pikën 4, të nenit 9 (20/1), të projektaktit, të parashikohet një afat konkret për paraqitjen, korrigjimin e informacionit dhe sqarimeve përkatëse. Ky rekomandim të mbahet në konsideratë edhe për pikën 3, të nenit 9 (20/2), të projektligjit.

Përgjigje: Nuk është marrë në konsideratë. Përcaktimi i shprehjes "afat i arsyeshëm" në pikën 4 të nenit 20/1 duhet të vlerësohet në lidhje të drejtpërdrejtë me pikën 3 të këtij neni, e cila parashikon shprehimisht se "forma, përmbajtja, mënyra e paraqitjes, afatet dhe procedurat për administrimin e procesit të vetëdeklarimit përcaktohen me urdhër të drejtorit të Përgjithshëm të Autoritetit".

Për rrjedhojë, ligjvënësi ka përcaktuar në nivel ligjor detyrimin e operatorëve për të paraqitur vetëdeklarimin, ndërsa ka deleguar në aktin nënligjor përcaktimin e rregullave të hollësishme për administrimin e këtij procesi, përfshirë edhe afatet përkatëse.

Në këtë kuadër, afati që i jepet operatorit në rast të mosparaqitjes së informacionit, paraqitjes së informacionit të paplotë, nevojës për dhënien e sqarimeve apo korrigjimin e informacionit, do të përcaktohet në aktin nënligjor të parashikuar në pikën 3 të nenit 20/1 dhe në përputhje me natyrën e procesit të vetëdeklarimit.

Përcaktimi i një afati unik dhe të pandryshueshëm drejtpërdrejt në ligj nuk do të ishte i përshtatshëm, pasi mangësitë e konstatuara në vetëdeklarimet e operatorëve mund të ndryshojnë në natyrë, volum dhe kompleksitet. Në varësi të rastit, plotësimi i një të dhëne formale mund të kërkojë një kohë të ndryshme nga plotësimi i informacionit teknik, organizativ ose operacional që lidhet me masat e sigurisë kibernetike.

Në këto kushte, përcaktimi i hollësishëm i afateve në aktin nënligjor mundëson një administrim më efektiv dhe proporcional të procesit, duke garantuar njëkohësisht që operatorët të kenë një afat të përcaktuar dhe të parashikueshëm për plotësimin, sqarimin ose korrigjimin e informacionit.

Gjithashtu, përdorimi i togfjalëshit “afat i arsyeshëm” në pikën 4 duhet kuptuar brenda kuadrit të rregullave dhe afateve që do të përcaktohen në aktin nënligjor të nxjerrë në zbatim të pikës 3 të këtij neni dhe jo si një kompetencë e pakufizuar e Autoritetit për përcaktimin rast pas rasti të afatit. Gjithashtu i njëjti argument vlen edhe për pikën 3, të nenit 9 (20/2), të projektligjit.

8. Në pikën 1, të nenit 20, të projektaktit, të shtohet edhe pika 6, e nenit 41 dhe pika 5 e nenit 15, si akte nënligjore që do të miratohen me vendim të Këshillit të Ministrave.

Përgjigje: Pranuar reflektuar.

II. **Ministri i Shteti për Administratën Pubike dhe Antikorrupsionin,** është shprehur si vijon:

1. Në ndryshimet e propozuara në pikën 5, të nenit 5 dhe pikën 1, të nenit 15, është përfshirë edhe emërtimi “*operatori qeveritar që menaxhon infrastruktura qeveritare*”, si një ndër institucionet përgjegjëse për ngritjen në strukturat e tyre të CSIRT-eve sektoriale përgjegjëse për incidentet e sigurisë kibernetike.

Nga shqyrtimi i përcaktimeve aktuale të ligjit nr. 25/2024 rezulton se emërtimi “*operatori qeveritar që menaxhon infrastruktura qeveritare*” nuk është i përfshirë as në nenin 5 “Përkufizime” dhe as në nenin 11, “Subjektet e tjera përgjegjëse për sigurinë kibernetike”.

Për sa më sipër me synimin e qartësisë së dispozitave të propozuara sugjerojmë që:

- në nenin 5 të përfshihet përkufizimi për “*operatorin qeveritar që menaxhon infrastruktura qeveritare*”, ose;

- në dispozitat e propozuara të vendoset emri i institucionit në vend të “*operatori qeveritar që menaxhon infrastruktura qeveritare*”.

Përgjigje: Nuk është marrë në konsideratë. Parashikimi i shprehjes “operatori qeveritar që menaxhon infrastrukturat qeveritare” në dispozitat e propozuara të projektligjit nuk krijon një institucion të ri apo një kategori të re subjekti të papërcaktuar nga ligji nr. 25/2024.

Në këtë drejtim, vlerësohet se kuptimi dhe funksioni i këtij subjekti përcaktohen në mënyrë të drejtpërdrejtë nga pika 6, e nenit 5, të ligjit nr. 25/2024 "Për sigurinë kibernetike", e cila përcakton se:

"CSIRT qeveritar" është CSIRT-i sektorial, i cili menaxhon të gjitha infrastrukturat kritike dhe të rëndësishme të informacionit për sektorin qeveritar.

Për rrjedhojë, ligji nr. 25/2024 ka përcaktuar në mënyrë të qartë ekzistencën, funksionin dhe fushën e përgjegjësisë së CSIRT-it qeveritar, duke e lidhur atë me menaxhimin e infrastrukturave kritike dhe të rëndësishme të informacionit të sektorit qeveritar. Në këtë kuptim, referimi në projektligj te "operatori qeveritar që menaxhon infrastrukturat qeveritare" duhet lexuar në lidhje me këtë përcaktim ligjor dhe me funksionin që ligji i atribuon CSIRT-it qeveritar.

Për më tepër, qëllimi i dispozitës së projektligjit është të përcaktojë subjektin institucional pranë të cilit ngrihet CSIRT-i sektorial përkatës, dhe jo të krijojë një përkufizim të ri për operatorin qeveritar. Përcaktimi i këtij subjekti nëpërmjet funksionit që ai ushtron mundëson që norma të lidhet me funksionin e menaxhimit të infrastrukturave qeveritare, dhe jo me një emërtim institucional specifik.

Vendosja në ligj e emrit konkret të institucionit nuk konsiderohet e përshtatshme, pasi organizimi dhe ndarja e përgjegjësive për menaxhimin e infrastrukturave qeveritare mund të pësojë ndryshime në kuadër të organizimit të administratës publike, pa qenë e nevojshme që për çdo ndryshim organizativ të ndryshohet edhe ligji për sigurinë kibernetike.

2. Në pikën 59, të propozuar për t'u shtuar në nenin 5, të ligjit aktualisht në fuqi parashikohet që organi i blerjes së përqendruar për trajnimet në fushën e sigurisë kibernetike do të jetë *autoriteti publik*, i cili organizon, kryen prokurimet e qendërzuara për trajnimet në fushën e sigurisë kibernetike, për operatorët e infrastrukturave të informacionit *të administratës shtetërore*, sipas përcaktimeve të këtij ligji dhe legjislacionit të posaçëm.

Gjithashtu:

- Në shkronjën "k", të propozuar për t'u shtuar në nenin 9, parashikohet që ndër kompetencat e Autoritetit Kombëtar të Sigurisë Kibernetike do të jetë edhe organizimi, kryerja e prokurimeve të përqendruara për trajnimet në fushën e sigurisë kibernetike, me vlerë mbi kufirin monetar të prokurimeve me vlera të vogla për

operatorët e infrastrukturave të informacionit *të administratës shtetërore* në përputhje me legjislacionin në fuqi të prokurimeve.

- Nga analiza e përcaktimeve aktuale të ligjit nr. 25/2024, konkretisht nenit 16, rezulton se ndër detyrat e CSIRT-eve sektoriale është edhe sigurimi i rritjes së kapaciteteve të stafit nëpërmjet trajnimeve dhe certifikimeve periodike sipas sektorëve që mbulojnë.

- Sipas propozimeve në këtë projektligj CSIRT-et sektoriale do të krijohen në strukturën dhe organikën e Autoritetit Kombëtar për Sigurinë Kibernetike, institucionin përgjegjës për licencimin dhe mbikëqyrjen e bankave dhe operatorin qeveritar që menaxhon infrastruktura qeveritare.

- Në relacionin e projektligjit nuk sqarohet se çfarë kuptohet me "administratë shtetërore" në kuptim të këtij ligji (ligjit nr. 25/2024).

Nga sa u parashtrua më sipër, nuk është plotësisht e qartë nëse AKSK-ja do të veprojë si operator/organi i blerjes së përqendruar për trajnimet në fushën e sigurisë kibernetike vetëm për institucionet e administratës shtetërore apo për të gjitha institucionet e administratës publike. Sqarojmë se sipas legjislacionit në fuqi për organizimin dhe funksionimin e administratës shtetërore (ligji 90/2012, i ndryshuar) institucione të administratës shtetërore janë institucionet nën përgjegjësinë e Këshillit të Ministrave.

Për sa më sipër me synimin e qartësisë së dispozitave sugjerojmë që:

- të përdoret e njëjta terminologji në pikën 59, që propozohet të shtohet në nenin 5 dhe në shkronjën "k", të propozuar për t'u shtuar në nenin 9;

- të shtohet në nenin 5, një përkufizim për "administratën shtetërore", duke e referuar atë tek ligji nr. 90/2012, i ndryshuar, nëse AKSK-ja do të veprojë si organi i blerjes së përqendruar për trajnimet në fushën e sigurisë kibernetike vetëm për administratën shtetërore;

- të bëhen ndryshimet përkatëse në dispozitat që propozohen të shtohen dhe në ato ekzistuese (të përmendura më sipër në këtë shkresë), nëse AKSK-ja do të veprojë si organi i blerjes së përqendruar për trajnimet në fushën e sigurisë kibernetike për të gjithë administratën publike.

Përgjigje: Pranuar pjesërisht. Reflektuar për pjesën e shtimit të përkufizimit "Administratë shtetërore" sipas kuptimit të ligjiin nr. 90/2012, "Për organizimin dhe funksionim e administratës shtetërore", i ndryshuar.". Refuzuar për pjën tjetër pasi terminiologjia e përdorur është e njëjtë në pikën 59, që propozohet të shtohet në nenin 5 dhe në shkronjën "k", të propozuar për t'u shtuar në nenin 9;.

3. Nëpërmjet propozimeve në këtë projektligji, ndër çështjet e rëndësishme që propozohet të ndryshojë është ngritja dhe pozicionimi i CSIRT-eve sektoriale (pra mënyra e ngritjes), rregullim ky i ndryshëm nga përcaktimet aktuale të ligjit nr. 25/2024. Në këtë kuptim arsyetojmë se autorizimi ligjor për Këshillin e Ministrave, i përcaktuar në pikën 5, të nenit 15, të ligjit nr. 25/2024, për përcaktimin e mënyrës së ngritjes e CSIRT-eve sektoriale, nuk gjen më zbatim.

Si rrjedhim sugjerojmë që:

- pika 5, e nenit 15, të shfuqizohet, ose;

- pika 5, e nenit 15, të riformulohet nëse Këshilli i Ministrave duhet të autorizohet për të përcaktuar çështje të tjera që lidhen me CSIRT-et sektoriale.

Përgjigje: Nuk është marrë në konsideratë. Pika 5 e nenit 15 mbetet e nevojshme, pasi në vendimin e Këshillit të Ministrave do të përcaktohet në mënyrë të detajuar grupimi i nënsektorëve në sektorët përkatës, si dhe institucioni/operatori pranë të cilit do të funksionojë secili CSIRT sektorial. Për rrjedhojë, autorizimi i Këshillit të Ministrave vijon të jetë i nevojshëm për përcaktimin e mënyrës konkrete të organizimit dhe funksionimit të CSIRT-eve sektoriale.

III. **Ministria e Shëndetësisë dhe Mirëqenies Sociale,** është shprehur si vijon:

1. Sugjerojmë që në projektligj të përcaktohen qartë përgjegjësitë e institucioneve kur administrimi funksional i sistemit të informacionit dhe administrimi teknik i infrastrukturës kryhen nga subjekte të ndryshme, veçanërisht lidhur me zbatimin e masave të sigurisë kibernetike, korrigjimin e vulnerabiliteteve, si dhe raportimin e informacionit përkatës. Përgjegjësitë duhet të jenë në përputhje me kompetencat dhe kontrollin efektiv të secilit institucion.

Përgjigje: Nuk është marrë në konsideratë. Propozimi refuzohet, pasi çështja e përgjegjësive për zbatimin e masave të sigurisë kibernetike, menaxhimin e

vulnerabiliteteve dhe raportimin e incidenteve është e rregulluar në mënyrë të shprehur në ligjin nr. 25/2024, "Për sigurinë kibernetike", dhe nuk kushtëzohet nga mënyra e organizimit të administrimit funksional apo teknik të sistemeve të informacionit.

Në mënyrë të veçantë, neni 21 i ligjit përcakton se operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit janë përgjegjës për zbatimin e masave teknike, organizative dhe operacionale për menaxhimin e riskut, duke përfshirë shprehimisht sigurinë në blerjen, zhvillimin dhe mirëmbajtjen e sistemeve të informacionit dhe rrjetit, si dhe trajtimin dhe zbulimin e vulnerabiliteteve.

Gjithashtu, neni 23 përcakton detyrimin e operatorëve për marrjen e masave për parandalimin dhe minimizimin e ndikimit të rreziqeve dhe incidenteve kibernetike, si dhe detyrimin për bashkëpunim me CSIRT-in Kombëtar dhe CSIRT-in sektorial gjatë të gjitha fazave të incidentit. Ndërkohë, neni 30 i jep Autoritetit kompetencën për të mbikëqyrur zbatimin e masave të sigurisë kibernetike nga operatorët dhe për të kërkuar informacionin, dokumentacionin dhe evidencat e nevojshme për verifikimin e zbatimit efektiv të tyre.

Për më tepër, neni 43 përcakton në mënyrë të drejtpërdrejtë detyrimin e operatorëve për marrjen e masave korrigjuese kur konstatohen mangësi në zbatimin e masave të sigurisë kibernetike, si dhe detyrimin për të njoftuar Autoritetin dhe për të paraqitur dokumentacionin mbështetës për masat e marra.

Në këtë kuadër, fakti që administrimi funksional i një sistemi dhe administrimi teknik i infrastrukturës mund të kryhen nga subjekte të ndryshme nuk ndryshon subjektin përgjegjës ndaj Autoritetit sipas ligjit nr. 25/2024 dhe nuk krijon nevojë për një rregullim të veçantë në projektligj. Marrëdhëniet e brendshme të përgjegjësisë ndërmjet institucionit që përdor/administron sistemin dhe subjektit që ofron shërbimet teknike mund të përcaktohen në aktet organizative, marrëveshjet apo kontratat përkatëse, pa cenuar detyrimet që ligji i ngarkon operatorit të infrastrukturës.

2. Në nenin 7 të projektligjit, lidhur me detyrimin për korrigjimin e vulnerabiliteteve të komunikuara nga Autoriteti, sugjerojmë të merret në konsideratë përfshirja e kriterit të realizueshmërisë teknike. Ky formulim do të ishte në koherencë me

parashikimet për masat ndaj treguesve të kompromet imit dhe sulmeve, si dhe me komentet e reflektuara gjatë procesit të konsultimit.

Përgjigje: Nuk është marrë në konsideratë. Sugjerimi për përfshirjen e shprehjes "kur është teknikisht e realizueshme" në lidhje me detyrimin për korrigjimin e vulnerabiliteteve të komunikuara nga Autoriteti nuk pranohet.

Dallimi në formulimin e shkronjave "g" dhe "gj" lidhet me natyrën e ndryshme të masave të parashikuara. Për treguesit e kompromet imit (IOC) dhe treguesit e sulmeve (IOA), shkronja "g" parashikon një sërë masash teknike të menjëhershme, si bllokimi, filtrimi, kufizimi, detektimi ose neutralizimi, zbatimi i të cilave mund të varet nga mundësitë teknike konkrete të sistemeve dhe infrastrukturave të administruara nga operatori.

Ndërkohë, detyrimi i parashikuar në shkronjën "gj" për korrigjimin e vulnerabiliteteve të komunikuara nga Autoriteti përbën një detyrim për marrjen e masave korrigjuese ndaj cenueshmërive të identifikuara dhe synon garantimin e një niveli të përshtatshëm sigurie kibernetike. Për këtë arsye, vendosja e një kushti të përgjithshëm të realizueshmërisë teknike në këtë dispozitë do të mund të krijonte hapësirë për moszbatimin e masave të nevojshme korrigjuese edhe në raste kur ato janë të domosdoshme për adresimin e vulnerabilitetit.

Gjithashtu, detyrimi është i lidhur me rrjetet, sistemet, platformat, pajisjet, aplikacionet dhe shërbimet TIK që administrohen nga vetë operatori dhe, për rrjedhojë, masat kërkohet të zbatohen në përputhje me përgjegjësinë e operatorit për sigurinë e këtyre infrastrukturave.

3. Në nenin 17 të projektligjit, shkronja "gj", sugjerojmë korrigjimin e referencës ndaj "pikave 1 dhe 4 të nenit 20/2", pasi neni 20/2 përmban vetëm tri pika.

Përgjigje: Pranuar reflektuar.

IV. Ministria e Financave, është shprehur si vijon:

1. Nevojitet të evidentohet nëse burimet njerëzore dhe fondet buxhetore të miratuara aktualisht për institucionet përgjegjëse, sipas ligjit nr. 87/2025, "Për buxhetin e vitit 2026", të ndryshuar, janë të mjaftueshme për të përballuar efektet financiare që rrjedhin nga zbatimi i projektligjit për pjesën e mbetur të vitit 2026.

Përgjigje: Po, burimet njerëzore dhe fondet buxhetore të miratuara për institucionet përgjegjëse, sipas ligjit nr. 87/2025, "Për buxhetin e vitit 2026", të ndryshuar, janë të mjaftueshme për të përballuar efektet financiare që rrjedhin nga zbatimi i projektligjit për pjesën e mbetur të vitit 2026.

Konkretisht, me aktin normativ nr. 2, datë 30.6.2026, "Për disa ndryshime dhe shtesa në ligjin nr. 87/2025, 'Për buxhetin e vitit 2026'", janë parashikuar fondet buxhetore përkatëse për mbulimin e efekteve financiare që lidhen me zbatimin e projektligjit. Këto fonde mbulojnë shpenzimet për paga dhe sigurime shoqërore për periudhën përkatëse të vitit 2026.

Për rrjedhojë, efektet financiare që rrjedhin nga zbatimi i projektligjit për pjesën e mbetur të vitit 2026 janë adresuar nëpërmjet ndryshimeve të miratuara në buxhetin e shtetit, në përputhje me aktin normativ nr. 2, datë 30.06.2026.

2. Në nenin 2 të projektligjit, e cila i ngarkon Autoritetit Kombëtar për Sigurinë Kibernetike organizimin dhe kryerjen e prokurimeve të përqendruara për trajnimet në fushën e sigurisë kibernetike, vlerësojmë se ushtrimi i kësaj kompetence të re për institucionin përbën një funksion shtesë, për rrjedhojë, kërkojmë të vlerësohet nëse ka apo jo efekte financiare. Gjithashtu, vërejmë se ndryshimi i propozuar mund të kërkojë nevojë për përshtatje të kuadrit ligjor për prokurimin publik.

Përgjigje: Shkronja "i", e nenit 9, të ligjit nr. 25/2024 "Për sigurinë kibernetike", parashikon se Autoriteti Kombëtar për Sigurinë Kibernetike, me urdhër të drejtorit të përgjithshëm dhe në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, zhvillon dhe nxit, sa herë vlerësohet e nevojshme, trajnime për personelin e këtyre operatorëve. Në këtë kuadër, ngarkimi i Autoritetit me organizimin dhe kryerjen e prokurimeve të përqendruara për trajnimet në fushën e sigurisë kibernetike nuk përbën krijimin e një funksioni të ri institucional, por përcakton mënyrën e ushtrimit dhe realizimit të një funksioni që lidhet drejtpërdrejt me kompetencat e Autoritetit në fushën e trajnimit dhe ngritjes së kapaciteteve në sigurinë kibernetike.

Gjithashtu, parashikimi për organizimin dhe kryerjen e prokurimeve të përqendruara nuk synon të ndryshojë rregullat dhe procedurat e përgjithshme të prokurimit publik, por përcakton institucionin përgjegjës për realizimin e kësaj procedure për kategorinë përkatëse të trajnimeve. Për rrjedhojë, zbatimi i kësaj dispozite bëhet në

përputhje me kuadrin ligjor në fuqi për prokurimin publik dhe nuk krijon nevojë për ndryshimin e tij.

Sa më sipër, ndryshimi i propozuar synon të sigurojë një mënyrë të unifikuar dhe të koordinuar të organizimit të trajnimeve specifike qe ofrohen nga subjekte të licencuar të cilat nuk mund të ofrohen nga Autoriteti për operatorët e infrastrukturave kritike dhe të rëndësishme në fushën e sigurisë kibernetike, në funksion të ngritjes dhe zhvillimit të kapaciteteve të personelit të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, në përputhje me funksionet e përcaktuara për Autoritetin nga ligji nr. 25/2024.

3. Në nenet 5 dhe 15, lidhur me funksionimin e CSIRT-ve sektoriale, kërkojmë të identifikohen dhe të detajohen të gjithë elementët përbërës të kostos vjetore të përllogaritur prej 111.1 milionë lekësh dhe të argumentohet burimi i financimit të këtyre kostove.

Përgjigje: Siç është pasqyruar në relacion, në pjesën "Vlerësimi buxhetor", shuma prej 111.1 milionë lekësh në vit është përllogaritur kryesisht për mbulimin e kostove të pagave të punonjësve shtesë që parashikohet të angazhohen në strukturat e CSIRT-eve sektoriale. Kjo vlerë përfaqëson koston e përllogaritur për një periudhë njëvjeçare dhe është përcaktuar në funksion të numrit të punonjësve shtesë dhe kostos së pagave përkatëse.

Kostot e mësipërme do të përballohen nga fondet e buxhetit të shtetit, nëpërmjet alokimeve buxhetore për institucionet përgjegjëse për ngritjen dhe funksionimin e CSIRT-eve sektoriale. Elementë të kostos per CSIRT qeveritar do të përballohen, sipas rastit, nga burimet dhe fondet e miratuara të institucionit përkatës.

4. Në nenin 10 të projektligjit parashikohet se mënyra e pagesës së ekspertëve të angazhuar pranë CERT-it do të përcaktohet me vendim të Këshillit të Ministrave. Megjithëse, objekti i kësaj dispozite është delegimi i rregullimit të mënyrës së pagesës me akt nënligjor, vlerësojmë se ndryshimi i propozuar krijon bazën ligjore për kryerjen e pagesave ndaj ekspertëve, të angazhuar pranë CERT-it dhe, si rrjedhojë, gjeneron efekte financiare shtesë për buxhetin e shtetit, të cilat duhet të identifikohen dhe të përllogariten në relacion, si dhe të përcaktohet burimi i financimit.

Gjithashtu, kërkojmë të argumentohet nevoja për angazhimin me pagesë të ekspertëve pranë CERT-it, duke mbajtur në konsideratë se stafi i Autoritetit Kombëtar për Sigurinë Kibernetike trajtohet me një regjim të veçantë pagash dhe përfiton shtesë për natyrë të veçantë pune, në nivele të konsiderueshme, me qëllim tërheqjen dhe mbajtjen e kapaciteteve njerëzore të specializuara në fushën e sigurisë kibernetike.

Përgjigje: Komenti nuk pranohet. Sipas nenit 29 të ligjit nr. 25/2024 "Për sigurinë kibernetike", sipas të cilit CERT-i është një strukturë *ad-hoc,* rast pas rasti, e krijuar pranë Autoritetit me qëllim trajtimin në kohë dhe me eficiencë të emergjencave dhe krizave të sigurisë kibernetike, te cilat përbëjnë ngjarje madhore dhe kërkojnë edhe angazhimin e strukturave te tjera krahas stafit të autoritetit. Në këtë kuadër, parashikimi i angazhimit të ekspertëve të jashtëm synon të mundësojë përfshirjen, sipas nevojës, të personave me ekspertizë, përvojë profesionale dhe trajnime të specializuara, të cilat mund të jenë të nevojshme për trajtimin dhe zgjidhjen e situatave komplekse të krizës kibernetike.

Angazhimi dhe pagesa e këtyre ekspertëve nuk lidhet me punonjësit e përhershëm të Autoritetit, të cilët trajtohen sipas regjimit të posaçëm të pagave dhe përfitimeve të parashikuara për funksionet në fushën e sigurisë kibernetike. Bëhet fjalë për ekspertë të jashtëm, të cilët mund të angazhohen në mënyrë të kufizuar dhe vetëm kur kërkohet ekspertizë e specializuar që nuk mund të sigurohet nëpërmjet kapaciteteve të strukturave ekzistuese.

Gjithashtu, duhet të theksohet se krizat kibernetike përbëjnë situata të jashtëzakonshme, të paparashikueshme ndaj angazhimi i ekspertëve dhe për rrjedhojë, pagesa e tyre nuk përbën një shpenzim të përhershëm apo periodik të buxhetit, por prek fondet rezervë. Pagesa do të kryhet vetëm në rastet e jashtëzakonshme kur lind nevoja konkrete për angazhimin e ekspertëve të jashtëm në funksion të menaxhimit dhe zgjidhjes së një krize kibernetike.

Për këtë arsye, dispozita nuk krijon një efekt financiar të përhershëm dhe të parashikueshëm në buxhetin e shtetit. Mënyra, kushtet dhe kufijtë e pagesës do të përcaktohen me vendim të Këshillit të Ministrave, në përputhje me nevojën konkrete për angazhimin e ekspertëve dhe me kuadrin ligjor në fuqi. Për rrjedhojë, në relacion nuk është parashikuar një fond i posaçëm vjetor për këtë qëllim, pasi shpenzimi do

të lindë vetëm në raste të jashtëzakonshme dhe do të përballohet nga fondet buxhetore të miratuara, sipas legjislacionit në fuqi.

5. Në pikën 6 të nenit 15 të projektligjit parashikohet që me vendim të Këshillit të Ministrave të përcaktohet periudha e zbatimit të detyrimit për përdorimin e produkteve, shërbimeve dhe proceseve TIK të certifikuara të sigurisë kibernetike. Vlerësojmë se, kjo dispozitë mund të sjellë nevojën për përshtatjen ose zëvendësimin e produkteve, shërbimeve dhe proceseve TIK ekzistuese nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, duke u shoqëruar me kosto shtesë financiare. Në këtë kuadër, kërkojmë të vlerësohen implikimet financiare që mund të rrjedhin nga zbatimi i kësaj dispozite, si dhe të përcaktohet burimi i financimit për përballimin e tyre.

Përgjigje: Detyrimi i parashikuar në pikën 6 të nenit 15 të projektligjit nuk sjell, në mënyrë automatike, detyrimin për përshtatjen ose zëvendësimin e të gjitha produkteve, shërbimeve dhe proceseve TIK ekzistuese të përdorura nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit dhe, për rrjedhojë, nuk mund të konsiderohet se gjeneron në mënyrë të drejtpërdrejtë dhe të menjëhershme një kosto financiare të përcaktueshme për këta operatorë. Aktualisht perdorimi i produkteve te certifikuara eshte vullnetar

Në këto kushte, duhet të mbahet në konsideratë edhe pika 4 e të njëjtit nen, sipas së cilës lista e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit për të cilët zbatohet detyrimi për përdorimin e produkteve, shërbimeve dhe proceseve TIK të certifikuara të sigurisë kibernetike miratohet me vendim të Këshillit të Ministrave, me propozimin e Autoritetit. Përcaktimi i kësaj liste do të bazohet në nje vendimmarrje te Komisionit Evropian mbi bazën vlerësimit e ndikimit, nivelin e rrezikut, rezultatet e vlerësimeve të sigurisë kibernetike, si dhe konsultimet me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit.

Për rrjedhojë, zbatimi i këtij detyrimi nuk shtrihet në mënyrë të përgjithshme dhe automatike mbi të gjithë operatorët, por do të përcaktohet në mënyrë të diferencuar, në bazë të nivelit konkret të rrezikut dhe ndikimit që paraqet infrastruktura përkatëse. Kjo qasje mundëson që detyrimi të aplikohet në mënyrë proporcionale dhe të marrë në konsideratë edhe situatën konkrete teknike të operatorëve.

Gjithashtu, periudha e zbatimit të detyrimit do të përcaktohet me vendim të Këshillit të Ministrave, mbi bazen e vendimit të Komisionit Evropian duke krijuar mundësinë për një periudhë të përshtatshme transitore për operatorët që do të përfshihen në fushën e zbatimit të këtij detyrimi. Për rrjedhojë, çdo përshtatje, përditësim ose zëvendësim i produkteve, shërbimeve apo proceseve TIK do të realizohet në mënyrë të planifikuar dhe në përputhje me nivelin e rrezikut dhe kërkesat e sigurisë kibernetike.

Në këto kushte, në fazën e hartimit të projektligjit nuk mund të përcaktohet një kosto financiare konkrete, pasi ajo do të varet nga lista e operatorëve që do t'i nënshtrohen detyrimit, rezultatet e vlerësimeve të sigurisë kibernetike, lloji dhe niveli i certifikimit të kërkuar, si dhe periudha e përcaktuar për zbatimin e detyrimit sipas Komisionit Evropian.

Sa më sipër, dispozita e propozuar nuk gjeneron në këtë fazë një efekt financiar të drejtpërdrejtë dhe të përcaktueshëm për buxhetin e shtetit, pasi kostot eventuale që mund të lindin do të varen nga zbatimi konkret i detyrimit dhe nga përcaktimet që do të bëhen në vijim për operatorët që do t'i nënshtrohen këtij detyrimi. Gjithashtu, duhet të evidentohet se operatorët të cilët do t'i nënshtrohen këtij detyrimi mund të jenë edhe subjekte private dhe jo domosdoshmërisht operatorë shtetërorë, ndaj kostot eventuale që mund të rrjedhin nga përdorimi i produkteve, shërbimeve dhe proceseve TIK të certifikuara nuk do të përbëjnë domosdoshmërisht efekte financiare mbi buxhetin e shtetit.

6. Në nenin 16 të projektligjit, nëpërmjet të cilit ndryshohet pika 3 e nenit 42 të ligjit në fuqi, parashikohet, përveç tarifës së regjistrimit, edhe tarifa e autorizimit për organet e vlerësimit të konformitetit për sigurinë kibernetike. Në këtë kuadër, nëse është e mundur kërkojmë të përllogaritet efekti i pritshëm në të ardhurat buxhetore që rrjedhin nga aplikimi i kësaj tarife shtesë.

Përgjigje: Parashikimi i tarifës së autorizimit për organet e vlerësimit të konformitetit për sigurinë kibernetike, krahas tarifës së regjistrimit, nuk sjell efekte negative në buxhetin e shtetit. Përkundrazi, aplikimi i kësaj tarife do të ndikojë në rritjen e të ardhurave në buxhetin e shtetit, si rezultat i pagesës së saj nga organet e vlerësimit të konformitetit për sigurinë kibernetike. Gjithësesi duke konsideruar faktin qe pagesa per autorizim është një tarifë (baraz kosto për lëshimin), vlera e

tarifës do të përcaktohet me vendim të Këshillit të Ministrave, ku në relacionin përkatës do të prezantohet vlera dhe përllogaritja.

Në këtë kuadër, tarifa e autorizimit nuk krijon një kosto shtesë për buxhetin e shtetit, por synon të mbulojë kostot administrative dhe teknike të lidhura me procesin e autorizimit dhe, njëkohësisht, gjeneron të ardhura shtesë për buxhetin e shtetit. Për këtë arsye, efekti financiar i parashikuar nga kjo dispozitë është pozitiv në drejtim të të ardhurave buxhetore.

7. Lidhur me nenin 18 të projektligjit, vlerësojmë se për disa prej sanksioneve administrative intervali ndërmjet kufirit minimal dhe atij maksimal të gjobës paraqitet mjaft i gjerë, duke arritur deri në 10-fishin e vlerës minimale. Për rrjedhojë, kërkojmë të argumentohet metodologjia e përdorur për përcaktimin e intervaleve të gjobave, si dhe mekanizmat që garantojnë një zbatim objektiv dhe proporcional të tyre, duke shmangur trajtime të ndryshme për raste me karakteristika të ngjashme.

Përgjigje: Përcaktimi i intervaleve të gjobave të parashikuara në nenin 18 të projektligjit është bërë duke mbajtur në konsideratë natyrën dhe rëndësinë e detyrimeve që rrjedhin nga ligji nr. 25/2024, "Për sigurinë kibernetike", si dhe nevojën për garantimin e një niveli të përshtatshëm të sigurisë së infrastrukturave të informacionit.

Në këtë drejtim, Direktiva (BE) 2022/2555 (NIS2) kërkon që gjobat administrative të jenë efektive, proporcionale dhe me efekt bindës, duke marrë në konsideratë rrethanat e çdo rasti individual. Për shkeljet e detyrimeve të përcaktuara në nenet 21 dhe 23 të Direktivës, NIS2 përcakton si kufij maksimalë minimalë, për subjektet thelbësore, shumën prej të paktën 10 000 000 euro ose 2% të xhiros vjetore botërore, cilado që është më e lartë, ndërsa për subjektet e rëndësishme, shumën prej të paktën 7 000 000 euro ose 1,4% të xhiros vjetore botërore, cilado që është më e lartë. Për subjektet e administratës publike, neni 34, pika 7, i NIS2 u lë shteteve anëtare përcaktimin nëse dhe në ç'masë mund të aplikohen gjoba administrative.

Në këtë kuadër, rritja e masës së sanksioneve të parashikuara në projektligj synon të forcojë efektivitetin e mekanizmit të zbatimit të ligjit dhe të rrisë nivelin e ndërgjegjësimit dhe përgjegjshmërisë së subjekteve të detyruara. Në kushtet e një mjedisi gjithnjë e më të digjitalizuar, siguria kibernetike përbën një faktor thelbësor

për garantimin e vazhdimësisë dhe qëndrueshmërisë së shërbimeve dhe proceseve me rëndësi për shoqërinë dhe ekonominë. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të zbatojnë masat e sigurisë kibernetike dhe detyrimet e tjera të përcaktuara në ligjin nr. 25/2024, me qëllim parandalimin, menaxhimin dhe minimizimin e pasojave të incidenteve dhe cenimeve të sigurisë kibernetike.

Intervalet e gjobave janë parashikuar për t'i dhënë mundësi Autoritetit të përshtatë masën e sanksionit me rrethanat konkrete të shkeljes. Diferencimi ndërmjet kufirit minimal dhe maksimal nuk nënkupton zbatim arbitrar të sanksioneve, por krijon hapësirën e nevojshme për vlerësimin e karakteristikave të çdo rasti, përfshirë natyrën dhe rëndësinë e shkeljes, pasojat e saj, kohëzgjatjen dhe rrethanat konkrete në të cilat është kryer shkelja, në përputhje me parimet e proporcionalitetit dhe objektivitetit dhe me kriteret e përcaktuara nga legjislacioni në fuqi për kundërvajtjet administrative.

Rritja e masës së sanksioneve administrative nuk synon penalizimin në vetvete, por nxitjen e përmbushjes efektive të detyrimeve ligjore dhe garantimin e zbatimit të masave të sigurisë nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit. Në këtë kuptim, sanksionet administrative shërbejnë edhe si instrument për rritjen e llogaridhënies së subjekteve përgjegjëse, përfshirë titullarët dhe strukturat drejtuese, në raport me detyrimet që u ngarkohen nga kuadri ligjor i sigurisë kibernetike.

Sa më sipër, intervalet e përcaktuara në projektligj synojnë të sigurojnë një raport të përshtatshëm ndërmjet natyrës së shkeljes dhe masës së sanksionit, duke marrë në konsideratë rëndësinë që paraqet mbrojtja e infrastrukturave të informacionit dhe nevojën për një zbatim efektiv të kërkesave të ligjit nr. 25/2024. Garantimi i zbatimit të këtyre kërkesave kontribuon në krijimin e një mjedisi digjital të qëndrueshëm, të sigurt dhe të besueshëm.

8. Në nenin 19 të projektligjit, propozohet përfshirja e subjekteve të administratës publike të vetëqeverisjes vendore, në Aneksin I të ligjit, në kategorinë "Sektorë me kritikalitet të lartë". Duke qenë se Aneksi III i Ligji nr. 25/2024, "Për sigurinë kibernetike" përmban vlerësimin e kostove financiare për zbatimin e detyrimeve të sigurisë kibernetike, ku institucionet rajonale dhe institucionet e pavarura/ligjzbatuese ngarkohen me 30% të kostove për çdo vit, vlerësojmë se në

kushtet e zgjerimit të fushës së zbatimit të ligjit edhe mbi njësitë e vetëqeverisjes vendore, është e nevojshme që të vlerësohen dhe të reflektohen në analizën financiare shoqëruese të projektligjit edhe kostot e mundshme që mund të rrjedhin për njësitë e vetëqeverisjes vendore.

Për këtë arsye, sugjerojmë kryerjen e një vlerësimi të ndikimit financiar të masave të propozuara për njësitë e vetëqeverisjes vendore, si dhe përcaktimin e qartë të mekanizmit të financimit të kostove përkatëse. Në veçanti, kërkojmë të adresohet mënyra e mbulimit të këtyre kostove për bashkitë me kapacitete të kufizuara financiare, për të cilat përballimi i tyre nga burimet e veta buxhetore mund të rezultojë i vështirë ose i pamundur. Në këtë kuadër, sugjerojmë që të mbahen në konsideratë, përcaktimet e nenit 22 të ligjit nr.139/201,5 "Për vetëqeverisjen vendore", i ndryshuar sipas të cilit, kur njësitë e vetëqeverisjes vendore nuk disponojnë fonde apo mjete të mjaftueshme për përmbushjen e standardeve dhe normave kombëtare, qeverisja qendrore u siguron mbështetjen e nevojshme financiare

Përgjigje: Përfshirja e subjekteve të administratës publike të vetëqeverisjes vendore në kategorinë "Sektorë me kritikalitet të lartë" nuk përbën një zgjerim të papritur të detyrimeve të sigurisë kibernetike ndaj këtyre subjekteve.

Në këtë drejtim, organet e vetëqeverisjes vendore janë aktualisht të identifikuara si operatorë të infrastrukturave të informacionit, nëpërmjet VKM nr.364, datë 30.6.2025, "Për miratimin e listës së infrastrukturave kritike dhe të rëndësishme të informacionit" (konfidenciale), e sndryshuar me VKM nr. 688, datë 11.9.2026, "Për miratimin e listës së infrastrukturave kritike dhe të rëndësishme të informacionit". Për rrjedhojë, njësitë e vetëqeverisjes vendore të përfshira në këtë listë kanë tashmë detyrimin për të zbatuar kërkesat dhe masat e sigurisë kibernetike të parashikuara në ligjin nr. 25/2024 "Për sigurinë kibernetike".

Në këtë kuptim, ndryshimi i propozuar në nenin 19 nuk krijon për herë të parë detyrime për njësitë e vetëqeverisjes vendore, por synon të reflektojë në Aneksin I të ligjit klasifikimin përkatës të subjekteve që tashmë janë identifikuar si operatorë të infrastrukturave kritike dhe të rëndësishme të informacionit.

Gjithashtu, kostot që lidhen me përmbushjen e detyrimeve të sigurisë kibernetike nga këto subjekte nuk burojnë nga vetë ndryshimi i propozuar, por janë të lidhura

me detyrimet që tashmë rrjedhin nga ligji nr.25/2024 dhe me statusin e tyre si operatorë të infrastrukturave të informacionit. Për këtë arsye, nuk vlerësohet se ndryshimi i propozuar sjell një efekt financiar të ri dhe shtesë, të ndryshëm nga kostot që lidhen me zbatimin e detyrimeve ekzistuese të ligjit.

Për rrjedhojë, nuk vlerësohet e nevojshme kryerja e një vlerësimi financiar shtesë vetëm për shkak të përfshirjes së këtyre subjekteve në Aneksin I të projektligjit, pasi detyrimet përkatëse të sigurisë kibernetike kanë filluar të zbatohen tashmë nga subjektet e identifikuara si operatorë të infrastrukturave kritike dhe të rëndësishme të informacionit.

V. Autoriteti i Komunikimeve Elektronike dhe Postare është shprehur me komente dhe sugjerime si vijon:

1. Konkretisht, lidhur me riformulimin e përkufizimit "CSIRT sektorial", AKEP vlerëson se, për sektorin e komunikimeve elektronike, funksioni i CSIRT-it sektorial duhet të organizohet pranë AKEP-it, duke pasur parasysh kompetencat ligjore që ky autoritet ushtron ndaj operatorëve të rrjeteve dhe shërbimeve të komunikimeve elektronike.

Operatorët bien në fushën e kompetencës së AKEP-it, në bazë të ligiit nr. 54/2024, i nënshtrohen tashmë detyrimeve për njoftim, raportim dhe bashkëpunim me AKEP-in lidhur me sigurinë dhe integritetin e rrjeteve dhe shërbimeve të komunikimeve elektronike. Nëse për këtë sektor CSIRT- i sektorial do të ngrihej dhe funksiononte jashtë AKEP-it, operatorëve do t'u lindte në praktikë detyrimi për të raportuar dhe bashkëpunuar paralelisht me dy autoritete, AKEP-in dhe AKSK-në, për çështje që në një masë të konsiderueshme lidhen me njëjtat incidente, rreziqe dhe masa te sigurisë.

Sektori i komunikimeve elektronike përbën një infrastrukturë kritike me karakteristika teknike specifike dhe me detyrime të veçanta. AKEP, si autoriteti rregullator i sektorit, disponon kompetencat mbikëqyrëse, ekspertizën teknike dhe marrëdhëniet institucionale me opetatorët e rrjeteve dhe shërbimeve të komunikimeve elektronike.

Ky model nuk përjashton rolin koordinues kombëtar të AKSK-së. Përkundrazi, CSIRT-i sektorial pranë AKEP-it funksionon si strukturë e specializuar për sektorin e komunikimeve elektronike, duke garantuar shkëmbimin e informacionit dhe

koordinimin e nevojshëm me CSIRT-in Kombëtar dhe AKSK-në sipas kuadrit të përgjithshem të sigurisë kibernetike.

Nëse riformulimi i përkufizimit të CSIRT sektorial, do të ruhet në formën e propozuar në këtë projektligi, ky formulim kërkon rishikim, pasi krijon përshtypjen se CSIRT sektoriale, duhet të funksionojnë pranë autoriteteve ose institucioneve te sektorit përkatës. Duke qënë se ngrihen nga AKSK, ushtrojnë funksionet e tyre në mënyrë të pavarur dhe aktiviteti i tyre koordinohet dhe raportohet pranë AKSK-së, vendosja e tyre organizative apo fizike pranë institucioneve sektoriale nuk përbën element thelbësor për përmbushjen efektive të detyrave funksionale.

Në këto kushte, referimi në perkufizim ndaj funksionimit pranë institucioneve të sektorit përkatës, nuk sjell vlerë inovative shtesë dhe mund të krijojë paqartësi lidhur me statusin organizativ dhe varësinë funksionale të CSIRT-eve sektoriale.

Përgjigje: Nuk është marrë në konsideratë. Direktiva (BE) 2022/2555 (NIS 2) ka sjellë një ndryshim të rëndësishëm në trajtimin e sigurisë kibernetike në sektorin e komunikimeve elektronike. Ofruesit e rrjeteve publike të komunikimeve elektronike dhe të shërbimeve të komunikimeve elektronike përfshihen shprehimisht në fushën e zbatimit të NIS 2 dhe i nënshtrohen kërkesave të saj për menaxhimin e riskut, raportimin e incidenteve dhe mbikëqyrjen në fushën e sigurisë kibernetike.

Në këtë kuadër, neni 43 i NIS 2 ka shfuqizuar nenet 40 dhe 41 të Direktivës (BE) 2018/1972, të cilat parashikonin kërkesa dhe kompetenca specifike në fushën e sigurisë dhe raportimit të incidenteve për ofruesit e komunikimeve elektronike. Kjo tregon qartë orientimin e kuadrit evropian drejt përfshirjes së sigurisë kibernetike të këtij sektori në kuadrin horizontal të NIS 2 dhe jo trajtimit të saj vetëm nëpërmjet kuadrit rregullator sektorial.

Për rrjedhojë, fakti që AKEP ushtron kompetenca rregullatore dhe mbikëqyrëse ndaj operatorëve të komunikimeve elektronike nuk përcakton në vetvete kompetencën për ngritjen dhe organizimin e CSIRT-it sektorial. NIS 2 e lidh funksionin e CSIRT-eve, mbikëqyrjen dhe koordinimin e sigurisë kibernetike me arkitekturën kombëtare të sigurisë kibernetike dhe autoritetet kompetente të përcaktuara për këtë qëllim. Në zbatim të kësaj qasjeje, ligji nr. 25/2024 “Për sigurinë kibernetike” i ka atribuar Autoritetit Kombëtar për Sigurinë Kibernetike përgjegjësitë në fushën e sigurisë kibernetike dhe koordinimin kombëtar përkatës.

Përcaktimi i CSIRT-it sektorial në kuadër të AKSK-së nuk cenon kompetencat rregullatore të AKEP-it dhe nuk përjashton bashkëpunimin me të. Përkundrazi, bashkëpunimi ndërmjet AKSK-së, CSIRT-it sektorial dhe AKEP-it do të mundësojë koordinimin, shkëmbimin e informacionit dhe shmangien e mbivendosjeve në ushtrimin e kompetencave përkatëse.

Gjithashtu, pretendimi se ky organizim krijon detyrime të dyfishta për operatorët nuk qëndron. Çështja e shmangies së mbivendosjeve ndërmjet kuadrit të sigurisë kibernetike dhe kuadrit sektorial zgjidhet nëpërmjet përcaktimit të qartë të kompetencave dhe mekanizmave të koordinimit, dhe jo nëpërmjet vendosjes së CSIRT-it sektorial pranë autoritetit rregullator të sektorit.

2. **Lidhur me shtimin e nenit 20/1 "Vetëdeklarimi i masave të sigurisë kibernetike"**, AKEP vlereson se dispozita e propozuar për vetëdeklarimin e masave të sigurisë kibernetike, krijon rrezik për mbivendosje të detyrimeve ligjore dhe kompetencave mbikeqyrëse ndaj ofruesve të rrjeteve publike të komunikimeve elektronike dhe shërbimeve të komunikimeve elektronike të disponueshme për publikun.

Ligji nr. 54/2024, "Per komunikimet elektronike në Republiken e Shqiperise", në nenet 54 dhe 56 të tij, parashikon tashmë detyrimin e këtyre subjekteve për të marrë masa të përshtatshme teknike, organizative dhe proporcionale për garantimin e sigurisë së rrjeteve dhe shërbimeve, si dhe ngarkon AKEP me kompetenca për monitorimin dhe mbikëqyrjen e zbatimit të këtyre detyrimeve. Në ushtrim të këtyre kompetencave, AKEP ka të drejtë të kërkojë informacion, dokumentacion dhe evidenca për verifikimin e masave të zbatuara nga operatoret.

Në këto kushte, vendosja e një detyrimi të përgiithshëm për vetëdeklarim pranë Autoritetit të Sigurisë Kibernetike, pa përcaktuar marrëdhënien me kompetencat sektoriale të AKEP, mund të çojë në raportim të dyfishtë të të njëjtit informacion dhe paqartësi lidhur me autoritetin përgjegjës për kontrollin dhe verifikimin e përmbushjes së detyrimeve në sektorin e komunikimeve elektron ike.

AKEP ka propozuar shtimin e një paragrafi në fund të pikës 1 të këtij neni, me përmbajtje: operatorët e rrjeteve dhe ofruesit e shërbimeve të komunikimeve elektronike të disponueshme për publikun, administrimi i vetëdeklarimit realizohet

në koordinim me AKEP, duke shmangur kërkimin dhe raportimin e dyfishtë të të njëjtit informacion.

Përgjigje: Nuk është marrë në konsideratë. Argumenti i paraqitur nga AKEP mbështetet në nenet 54 dhe 56 të ligjit nr. 54/2024 "Për komunikimet elektronike në Republikën e Shqipërisë", të cilat transpozojnë respektivisht nenet 40 dhe 41 të Direktivës (BE) 2018/1972 për krijimin e Kodit Evropian të Komunikimeve Elektronike. Megjithatë, këto dispozita të Direktivës 2018/1972 janë shfuqizuar nga Direktiva (BE) 2022/2555 (NIS 2), me efekt nga 18 tetori 2024.

Nëpërmjet NIS 2, kërkesat për sigurinë kibernetike të ofruesve të rrjeteve publike të komunikimeve elektronike dhe të shërbimeve të komunikimeve elektronike janë përfshirë në kuadrin e posaçëm të sigurisë kibernetike të kësaj Direktive. Për rrjedhojë, këta ofrues i nënshtrohen kërkesave dhe mbikëqyrjes në fushën e sigurisë kibernetike në kuadër të regjimit të NIS 2.

Në Shqipëri, ligji nr.25/2024, "Për sigurinë kibernetike", në përputhje me këtë arkitekturë, ka përcaktuar Autoritetin Kombëtar për Sigurinë Kibernetike si autoritetin përgjegjës për zbatimin dhe mbikëqyrjen e legjislacionit për sigurinë kibernetike. Për rrjedhojë, detyrimi për vetëdeklarimin e masave të sigurisë kibernetike përbën një instrument të ushtrimit të kompetencave mbikëqyrëse që AKSK-ja ushtron drejtpërdrejt në bazë të ligjit nr.25/2024 dhe nuk mund të kufizohet nëpërmjet përcaktimit të një detyrimi për koordinim paraprak me AKEP-in.

Pretendimi për mbivendosje të kompetencave nuk buron nga vetë neni 20/1, por nga fakti që kuadri kombëtar sektorial i komunikimeve elektronike nuk ka reflektuar ende ndryshimet e sjella nga NIS 2 në Direktivën 2018/1972, përfshirë shfuqizimin e neneve 40 dhe 41. Për këtë arsye, shmangia e mbivendosjeve duhet të adresohet nëpërmjet harmonizimit të legjislacionit shqiptar për komunikimet elektronike me *acquis*-in e përditësuar të Bashkimit Evropian dhe jo nëpërmjet kufizimit të kompetencave të AKSK-së të përcaktuara nga ligji nr. 25/2024.

3. **Lidhur me shtimin e nenit 20/2 "Vetëdeklarimi i hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit",** AKEP vlerëson se dispozita nuk përmban garanci lidhur me trajtimin dhe mbrojtjen e informacionit që deklarohet nga operatorët, mbajtur parasysh që të dhënat e kërkuara përmbajnë

informacion me karakter konfidencial, publikimi ose aksesimi i paautorizuar i të cilit mund të cenojë sigurinë e sistemeve dhe infrastrukturave kritike të informacionit. Mungesa e këtyre garancive krijon pasiguri juridike për subjektet e detyruara dhe mund të rrisë ekspozimin ndaj rreziqeve të sigurisë kibernetike.

Në këto kushte, AKEP ka propozuar shtimin e një paragrafi me këtë përmbajtje*: "Autoriteti merr masa t*ë *nevojshme teknike organizative dhe ligjore për garantimin e konfidencialitetit integritetit dhe disponueshmërisë së këtij informacioni, si dhe kufizon aksesin n*ë *vetëm për persona të autorizuar,. në perputhje me legjislacionin në fuqi".*

Përgjigje: Nuk është marrë në konsideratë. Shqetësimi i ngritur nga AKEP lidhur me mbrojtjen, ruajtjen dhe aksesin në informacionin e përftuar nëpërmjet vetëdeklarimit është adresuar në mënyrë të shprehur në projektligj. Konkretisht, nëpërmjet ndryshimit të shkronjës "dh" të pikës 2 të nenit 30 të ligjit, pas fjalës "mbrojtjen" shtohet fjala "dhe konfidencialitetin", duke përcaktuar detyrimin e Autoritetit për garantimin jo vetëm të mbrojtjes, por edhe të konfidencialitetit të informacionit që administron në ushtrimin e funksioneve të tij.

Ky detyrim zbatohet në përputhje me natyrën dhe përmbajtjen e informacionit të administruar nga Autoriteti dhe me legjislacionin në fuqi për sigurinë e informacionit të klasifikuar. Për rrjedhojë, garancitë e kërkuara nga AKEP për trajtimin dhe mbrojtjen e informacionit janë tashmë të parashikuara në projektligj.

VI. Agjencia Kombëtar e Shoqërisë së Informacionit është shprehur me komente dhe sugjerime si vijon:

I. VËREJTJE PARIMORE: NDARJA E FUNKSIONEVE RREGULLATORE, MBIKËQYRËSE DHE OPERACIONALE

Ligji nr. 25/2024 ndërton një arkitekturë institucionale të qartë me tri nivele. Në krye qëndron Autoriteti, i cili është "organ rregullator përgjegjës për mbikëqyrjen dhe zbatimin e legjislacionit për sigurinë kibernetike" dhe ushtron njëkohësisht funksionin e CSIRT-it Kombëtar. Në nivelin e dytë qëndrojnë CSIRT-et sektoriale, të ngritura nga subjektet përgjegjëse sipas sektorëve. Në nivelin e tretë

qëndrojnë CSIRT-et pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit. I njëjti model është riafirmuar nga vetë Autoriteti në rregulloren e tij për funksionimin teknik të CSIRT-eve, e cila përcakton se CSIRT-i sektorial ngrihet nga subjektet përgjegjëse të sigurisë kibernetike sipas sektorëve dhe se rezultatet e vetëvlerësimit të CSIRT-eve sektoriale i dërgohen CSIRT-it Kombëtar për analizë.

Kjo arkitekturë nuk është formale. Ajo mbështetet në parimin se ai që vendos rregullat dhe mbikëqyr zbatimin e tyre nuk mund të jetë njëkohësisht subjekti që i zbaton ato. Vetëm kështu garantohet që mbikëqyrja të jetë reale, që përgjegjësia të jetë e identifikueshme dhe që veprimtaria të jetë e audituеshme. Direktiva NIS2 e ndërton në të njëjtën mënyrë marrëdhënien ndërmjet autoriteteve kompetente, që mbikëqyrin dhe zbatojnë masat ndaj subjekteve, dhe subjekteve të mbikëqyrura, organet drejtuese të të cilave mbajnë përgjegjësi për masat e menaxhimit të riskut. Po ashtu, Akti i Sigurisë Kibernetike kërkon shprehimisht që autoriteti kombëtar i certifikimit të jetë i pavarur nga subjektet që mbikëqyr dhe që veprimtaritë e lëshimit të certifikatave të jenë rreptësisht të ndara nga veprimtaritë mbikëqyrëse.

Projektligji i propozuar e cenon këtë parim në disa drejtime njëkohësisht. Në të njëjtin institucion ai përqendron këto funksione:

a) rregullatorin dhe mbikëqyrësin e të gjitha infrastrukturave kritike dhe të rëndësishme të informacionit;
b) CSIRT-et sektoriale, pra ekipet operacionale që ligji i vendos nën koordinimin dhe mbikëqyrjen e Autoritetit;
c) organin qendror blerës për trajnimet e operatorëve që i mbikëqyr;
d) organin kombëtar të certifikimit, organin që autorizon dhe regjistron organet e vlerësimit të konformitetit, si dhe organin që përcakton me udhëzim të brendshëm kriteret e hyrjes në këtë treg;
e) institucionin që propozon listën e operatorëve të detyruar të blejnë produkte të certifikuara. Në këtë model, i njëjti institucion krijon kërkesën në treg, kontrollon ofertën, vendos rregullat e hyrjes, mbledh tarifat dhe mbikëqyr zbatimin.
Ky grumbullim rolesh përbën konflikt strukturor interesi dhe është në kundërshtim me frymën e ligjit bazë dhe me aktet e BE-së me të cilat ai është

përafruar. Vërejtjet specifike që vijojnë janë shprehje konkrete e këtij problemi parimor.

Përgjigje: Pretendimi se projektligji cenon parimin e ndarjes së funksioneve rregullatore, mbikëqyrëse dhe operacionale dhe se krijon një mbivendosje të funksioneve të autoritetit kompetent për sigurinë kibernetike nuk qëndron. Ky përfundim buron nga një interpretim i zgjeruar i parimit të ndarjes së funksioneve, i cili nuk gjen mbështetje as në ligjin nr. 25/2024, "Për sigurinë kibernetike" dhe as në Direktivën (BE) 2022/2555 (NIS2).

Së pari, duhet bërë dallimi ndërmjet funksioneve të autoritetit kompetent dhe përgjegjësive të subjekteve të mbikëqyrura. NIS2 e ndërton këtë marrëdhënie mbi një ndarje të qartë ndërmjet autoriteteve kompetente, të cilat janë përgjegjëse për mbikëqyrjen dhe zbatimin e kuadrit ligjor, dhe subjekteve thelbësore dhe të rëndësishme, të cilat mbajnë përgjegjësi për zbatimin e masave të menaxhimit të riskut të sigurisë kibernetike. Neni 8 i Direktivës përcakton se autoritetet kompetente janë përgjegjëse për sigurinë kibernetike dhe për detyrat mbikëqyrëse, ndërsa detyrimet për menaxhimin e riskut u ngarkohen subjekteve të përcaktuara në anekset përkatëse.

Ky dallim ruhet plotësisht nga projektligji. Autoriteti Kombëtar për Sigurinë Kibernetike nuk merr përsipër administrimin, operimin apo menaxhimin e përditshëm të infrastrukturave të operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit. Përgjegjësia për organizimin dhe zbatimin e masave të sigurisë kibernetike, menaxhimin e riskut, funksionimin e sistemeve dhe përmbushjen e detyrimeve ligjore mbetet te vetë operatorët dhe strukturat e tyre përgjegjëse. Për rrjedhojë, nuk ekziston mbivendosje ndërmjet subjektit që mbikëqyr dhe subjektit që është përgjegjës për zbatimin e masave të mbikëqyrura.

Së dyti, pretendimi se CSIRT-i sektorial duhet të jetë domosdoshmërisht i ndarë institucionalisht nga autoriteti kompetent nuk mbështetet në NIS2. Përkundrazi, neni 10, pika 1, i Direktivës (BE) 2022/2555 përcakton shprehimisht se shtetet anëtare caktojnë ose krijojnë një ose më shumë CSIRT-e dhe se CSIRT-et mund të caktohen ose të ngrihen brenda një autoriteti kompetent.

Në këtë kuptim, vetë Direktiva e konsideron të pajtueshme me arkitekturën institucionale të sigurisë kibernetike që një autoritet kompetent të ketë, krahas funksioneve të tij mbikëqyrëse, edhe një ose disa CSIRT-e të vendosur në

strukturën e tij. Kjo nuk përbën përzierje të funksioneve në kuptimin e pretenduar nga komenti, por një organizim institucional të lejuar shprehimisht nga e drejta e Bashkimit Evropian.
Për më tepër, funksionet e CSIRT-it sipas nenit 11 të NIS2 janë të natyrës teknike dhe operacionale, duke përfshirë monitorimin dhe analizimin e kërcënimeve, dobësive dhe incidenteve, dhënien e paralajmërimeve, reagimin ndaj incidenteve, analizën forensike, asistencën ndaj subjekteve dhe, në kushte të caktuara, skanimin proaktiv të sistemeve. Fakti që këto funksione ushtrohen nga një strukturë e vendosur brenda Autoritetit Kompetent nuk e shndërron Autoritetin në operator të infrastrukturave të subjekteve të mbikëqyrura dhe as nuk e zhvesh operatorin nga përgjegjësia e tij ligjore.
Së treti, nuk qëndron pretendimi se vendosja e CSIRT-eve sektoriale pranë autoritetit kompetent për sigurinë kibernetike krijon mbivendosje të funksioneve. Ky pretendim mbështetet në një barazim të gabuar të CSIRT-eve sektoriale me subjektet thelbësore dhe të rëndësishme që janë objekt i mbikëqyrjes.
NIS2 i trajton CSIRT-et si pjesë të arkitekturës institucionale kombëtare të sigurisë kibernetike dhe jo si subjekte të mbikëqyrura në kuptimin e regjimit të mbikëqyrjes së subjekteve thelbësore dhe të rëndësishme. Për më tepër, neni 10 i Direktivës lejon shprehimisht që CSIRT-et të caktohen ose të ngrihen brenda një autoriteti kompetent. Funksionet e tyre janë të natyrës teknike dhe operacionale, të lidhura me parandalimin, zbulimin, analizimin dhe trajtimin e incidenteve, ndërsa përgjegjësia për zbatimin e masave të sigurisë dhe menaxhimin e riskut mbetet te subjektet thelbësore dhe të rëndësishme.
Për rrjedhojë, organizimi i CSIRT-eve sektoriale pranë Autoritetit, sipas projektligjit, nuk e bën Autoritetin njëkohësisht rregullator dhe subjekt të mbikëqyrur. Funksionet rregullatore dhe mbikëqyrëse ushtrohen nga Autoriteti, ndërsa funksionet teknike të CSIRT-it ushtrohen sipas kompetencave të tij, duke ruajtur ndarjen e përgjegjësive ndërmjet Autoritetit, CSIRT-eve dhe subjekteve të mbikëqyrura.

II. VËREJTJE SIPAS DISPOZITAVE TË PROJEKTLIGJIT

1. CSIRT-et sektoriale pranë Autoritetit (neni 1, pika 1, neni 5 dhe neni 6 i projektligjit; nenet 5, pika 5, 15, pika 1, dhe 16, shkronja “dh”, e ligjit)

1.1. Ndryshimi i propozuar

Ligji në fuqi përcakton se CSIRT-i sektorial vendoset "pranë një operatori që administron infrastruktura kritike dhe të rëndësishme të informacionit ose institucionit përgjegjës të linjës"dhe se ai ngrihet nga subjektet përgjegjëse për ofrimin e shërbimeve, sipas nenit 11 të ligjit. Projektligji i ndryshon të dyja dispozitat. Me ndryshimin e propozuar, CSIRT-et sektoriale ngrihen nga Autoriteti, nga institucioni përgjegjës për licencimin dhe mbikëqyrjen e bankave dhe nga operatori qeveritar. Njëkohësisht hiqet detyrimi i subjekteve të nenit 11, pra i ministrive dhe i institucioneve të linjës, për të ngritur CSIRT-in e sektorit të tyre. Pasoja praktike është se Autoriteti bëhet CSIRT sektorial për të gjithë sektorët e tjerë të aneksit I dhe II: energjinë, transportin, shëndetësinë, ujin, infrastrukturën digjitale, komunikimet elektronike, arsimin e të tjerë. Kjo konfirmohet edhe nga relacioni, i cili i llogarit kostot e këtyre strukturave në 111,123,252,43 lekë në vit.

a. Konflikti strukturor i interesit: Autoriteti mbikëqyr vetëveten

Detyrat e CSIRT-it sektorial nuk janë detyra të Autoritetit. Ato janë detyra të një subjekti që i nënshtrohet Autoritetit. Neni 16 i ligjit e ngarkon CSIRT-in sektorial të "bashkëpunojë me Autoritetin", të "bashkërendojë punën me CSIRT-in kombëtar", të "njoftojë CSIRT-in Kombëtar menjëherë" për incidentet, të caktojë pikën e kontaktit dhe ta "raportojë pranë
CSIRT-it Kombëtar" brenda afateve ligjore, si dhe të ruajë log-e sipas rregullores së miratuar nga drejtori i përgjithshëm i Autoritetit.12 Neni 33 i ligjit e bën këtë bashkëpunim detyrim ligjor: "CSIRT-et sektoriale kanë detyrimin për të bashkëpunuar në çdo kohë me CSIRT-in Kombëtar dhe Autoritetin".
Nëse CSIRT-i sektorial ngrihet brenda Autoritetit, të gjitha këto detyrime kthehen në detyrime të Autoritetit ndaj vetëvetes. Autoriteti do të njoftojë veten, do t'i raportojë vetes, do të bashkëpunojë me veten dhe do të vlerësojë maturitetin e ekipeve të veta sipas rregullores që vetë ka miratuar. Neni 6 i projektligjit, i cili riformulon shkronjën "dh" të nenit 16, nuk e zgjidh këtë problem. Përkundrazi, ai e thellon, sepse detyrimi i njoftimit "menjëherë pas marrjes dijeni" humbet çdo kuptim kur dërguesi dhe marrësi janë i njëjti institucion.
Në këto kushte nuk ka përgjigje për tri pyetje themelore:
a) Kush garanton zbatimin e detyrave të nenit? Mekanizmi i vetëm i zbatimit që parashikon ligji është mbikëqyrja nga Autoriteti. Kur subjekti i mbikëqyrur është vetë Autoriteti, mekanizmi mbetet pa objekt.

b) Kush e mbikëqyr CSIRT-in sektorial? Neni 44, shkronja “a”, e ligjit e cilëson kundërvajtje administrative mosraportimin e incidentit pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial. Kundërvajtjen e konstaton dhe gjobën e vendos Autoriteti. Autoriteti nuk mund të konstatojë shkelje të veta, as të vendosë gjoba ndaj vetes.
c) Si garantohet auditueshmëria? Operatorët raportojnë incidentet brenda 4 orëve “pranë CSIRT-it Kombëtar dhe CSIRT-it sektorial”, ndërsa pikat e kontaktit njoftohen pranë të dyjave. Qëllimi i këtij raportimi të dyfishtë është kontrolli i ndërsjellë ndërmjet dy niveleve. Kur të dy nivelet bashkohen në një institucion, raportimi i dyfishtë kthehet në burokraci pa vlerë dhe gjurma e auditueshme e veprimtarisë së nivelit sektorial zhduket.
1.3. Përputhshmëria me Direktivën NIS2 dhe me Rregulloren DORA
Për korrektësi, pranojmë se Direktiva NIS2 lejon që CSIRT-et të caktohen ose të ngrihen brenda një autoriteti kompetent. Mbi këtë bazë, ligji nr. 25/2024 e ka vendosur tashmë CSIRT-in Kombëtar pranë Autoritetit. Megjithatë, kjo dispozitë nuk e mbështet ndryshimin e propozuar, për tri arsye:
a) Neni 10 i NIS2 rregullon CSIRT-et kombëtare që përmbushin detyrat e nenit 11 të Direktivës. Niveli sektorial është krijim i ligjit shqiptar, dhe ligji shqiptar e ka ndërtuar qëllimisht si nivel të dallueshëm, që i raporton dhe i nënshtrohet nivelit kombëtar. Zhbërja e këtij dallimi nuk është kërkesë e Direktivës. Ajo është zgjedhje që bie ndesh me vetë logjikën e ligjit.
b) Direktiva NIS2 parashikon shprehimisht bashkëpunimin ndërmjet autoriteteve kompetente, pikës së vetme të kontaktit dhe CSIRT-eve si subjekte të dallueshme. Ajo e ndërton mbikëqyrjen si marrëdhënie ndërmjet autoritetit kompetent dhe subjektit të mbikëqyrur. Kjo marrëdhënie nuk mund të ekzistojë brenda të njëjtit person juridik.
c) Rregullorja DORA konfirmon parimin e kundërt me atë që propozohet. Për sektorin financiar, menaxhimi dhe raportimi i incidenteve lidhen me autoritetin kompetent sektorial, që është institucioni që njeh dhe licencon subjektet e sektorit. Pikërisht për këtë arsye, parashikimi i CSIRT-it sektorial pranë institucionit përgjegjës për mbikëqyrjen e bankave është në përputhje me logjikën e DORA-s. Ky argument e mbështet vendosjen e CSIRT-it sektorial pranë institucionit të sektorit, jo pranë një rregullatori horizontal.
1.4. Paqartësia juridike e përkufizimit të ri

Përkufizimi i propozuar për pikën 5 të nenit 5 përcakton se CSIRT-i sektorial është "i ngritur nga Autoriteti…, institucioni përgjegjës për licencimin dhe mbikëqyrjen e bankave dhe operatori qeveritar… dhe funksionon pranë ministrive përgjegjëse, institucionit rregullator për bankat, Autoritetit apo operatorit qeveritar". Formulimi nuk bën të qartë nëse CSIRT-i ngrihet nga një institucion dhe funksionon pranë një tjetrit, cili institucion mban përgjegjësi për të, ose cili CSIRT mbulon cilin sektor. Një dispozitë që përcakton subjektin përgjegjës për reagimin ndaj incidenteve në infrastrukturat kritike duhet të jetë e qartë dhe e parashikueshme. Kjo paqartësi, në vetëvete, është arsye e mjaftueshme për rikthimin e tekstit në fuqi.

1.5. Propozimi

Propozojmë heqjen e pikës 1 të nenit 1 dhe të nenit 5 të projektligjit dhe ruajtjen e teksteve në fuqi të nenit 5, pika 5, dhe të nenit 15, pika 1, të ligjit. Nëse Këshilli i Ministrave gjykon të nevojshme që disa institucione të emërtohen shprehimisht, si institucioni përgjegjës për mbikëqyrjen e bankave, kjo mund të bëhet me një shtesë në nenin 15, pika 1, për subjektet sektoriale, pa e përfshirë në asnjë rast Autoritetin. Në këtë rast, neni 6 i projektligjit mund të ruhet si saktësim teknik i afatit të njoftimit, sepse ai ka kuptim vetëm kur CSIRT-i sektorial është subjekt i dallueshëm nga CSIRT-i Kombëtar.

Përgjigje: Nuk është marrë në konsideratë. Ndryshimi i propozuar për organizimin e CSIRT-eve sektoriale buron nga nevoja për të përqendruar kapacitetet e kufizuara teknike dhe njerëzore në struktura që mund të garantojnë në mënyrë efektive funksionet e reagimit ndaj incidenteve. Modeli aktual i parashikuar në ligjin 25/2024, "Për sigurinë kibernetike", i cili e lidh ngritjen e CSIRT-eve sektoriale me ministritë dhe institucionet përgjegjëse të linjës sipas nenit 11 të ligjit, ka evidentuar vështirësi në sigurimin e burimeve financiare për ngritjen e tyre si dhe kapaciteteve të specializuara. Për këtë arsye, projektligji riorganizon mënyrën e ofrimit të funksionit CSIRT në nivel sektorial, pa cenuar përgjegjësinë e operatorëve për sigurinë e infrastrukturave të tyre.

Nuk qëndron pretendimi se ky ndryshim krijon një situatë të "vetëmbikëqyrjes" së Autoritetit. Objekt i funksioneve mbikëqyrëse të Autoritetit janë operatorët e infrastrukturave kritike dhe të rëndësishme dhe jo CSIRT-et sektoriale. Nenet 30 dhe 31 të ligjit përcaktojnë kompetencat e Autoritetit për mbikëqyrjen e

operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, ndërsa detyrimi dhe kundërvajtja e parashikuar në nenin 44, shkronja "a", lidhen me mosraportimin e incidentit nga operatori. Këto përgjegjësi dhe mekanizma mbikëqyrës nuk ndryshohen nga projektligji.

Gjithashtu, fakti që një CSIRT sektorial organizohet brenda Autoritetit nuk nënkupton që funksionet e tij teknike dhe operative bëhen funksione mbikëqyrëse të Autoritetit. CSIRT-i dhe Autoriteti kanë funksione të ndryshme për nga natyra dhe objekti. Autoriteti ushtron funksionet rregullatore, mbikëqyrëse dhe koordinuese të përcaktuara në ligj, ndërsa CSIRT-i ushtron funksione teknike dhe operative lidhur me parandalimin, zbulimin, analizimin dhe trajtimin e incidenteve. Detyrimet e brendshme të raportimit dhe koordinimit mund të zbatohen përmes procedurave dhe hierarkisë administrative, ndërsa gjurma e veprimtarisë sigurohet përmes ruajtjes së log-eve dhe mekanizmave të kontrollit dhe auditimit të administratës publike.

Për më tepër, NIS2 nuk vendos një ndalim për organizimin e CSIRT-eve brenda autoritetit kompetent. Përkundrazi, neni 10, pika 1, lejon shprehimisht që një ose më shumë CSIRT-e të caktohen ose të ngrihen brenda një autoriteti kompetent. Vetë komenti pranon se niveli sektorial është një zgjidhje e legjislacionit shqiptar dhe jo një strukturë që NIS2 e imponon në një formë të caktuar. Për rrjedhojë, mënyra e organizimit të këtij niveli mbetet në kompetencën e ligjvënësit kombëtar, për sa kohë garantohen funksionet dhe kapacitetet e kërkuara nga Direktiva NIS2.

Në këtë kuptim, vendosja e CSIRT-it sektorial pranë Autoritetit nuk bie ndesh me parimin e ndarjes së funksioneve të NIS2, pasi ndarja që kërkohet nga Direktiva është ndërmjet autoritetit kompetent dhe subjekteve thelbësore e të rëndësishme që janë objekt i mbikëqyrjes. CSIRT-et janë pjesë e arkitekturës institucionale të sigurisë kibernetike dhe nuk janë operatorë të infrastrukturave të mbikëqyrura.

Edhe referimi në DORA nuk e mbështet kundërshtimin. Projektligji e ruan shprehimisht CSIRT-in sektorial pranë institucionit përgjegjës për licencimin dhe mbikëqyrjen e bankave, pikërisht për shkak të veçantisë së sektorit financiar. Për sektorët e tjerë, projektligji ka përcaktuar një model të centralizuar të

kapaciteteve të CSIRT-ve, i cili synon të shmangë fragmentimin e burimeve teknike dhe të sigurojë reagim më të koordinuar.

Sa i përket pretendimit për "raportim të dyfishtë", përqendrimi i funksionit CSIRT në një strukturë të vetme, aty ku kjo është zgjedhur nga projektligji, nuk e eliminon gjurmën e raportimit apo përgjegjësinë e operatorit të infrastrukturës së informacionit. Përkundrazi, synon të shmangë kanale paralele dhe të reduktojë barrën administrative, duke mundësuar që informacioni për incidentin të trajtohet nga struktura me kapacitetin teknik përkatës.

2. Autoriteti si organ i blerjes së përqendruar për trajnimet (neni 1, pika 3, për pikën 59 të nenit 5, dhe neni 2, për shkronjën "k" të nenit 9 të ligjit)

Projektligji i shton Autoritetit kompetencën për të organizuar dhe kryer prokurimet e përqendruara për trajnimet në fushën e sigurisë kibernetike për operatorët e infrastrukturave të informacionit të administratës shtetërore, për vlera mbi kufirin e prokurimeve me vlerë të vogël. Operatorët detyrohen t'i dërgojnë Autoritetit kërkesat e tyre deri më 30 prill. Vlerësojmë se kjo kompetencë nuk ka asnjë justifikim ligjor apo funksional, për arsyet e mëposhtme.

2.1. Prokurimi i përqendruar është i rregulluar tashmë nga ligji i posaçëm

Prokurimi publik rregullohet nga ligji nr. 162/2020, i cili përcakton organet qendrore blerëse dhe mënyrën e krijimit dhe funksionimit të tyre. Në zbatim të tij, Këshilli i Ministrave ka krijuar institucione të specializuara për këtë qëllim, përfshirë shoqërinë "Operatori i Blerjeve të Përqendruara" sh.a. Caktimi i një organi të ri qendror blerës përmes një ligji sektorial krijon regjim paralel me atë të ligjit të prokurimit. Vetë emërtimi i propozuar, "organi i blerjes së përqendruar për trajnimet", nuk përputhet me terminologjinë e ligjit të prokurimit, i cili njeh vetëm "organin qendror blerës".

Për më tepër, ligji i prokurimit e ngarkon çdo autoritet kontraktor me përgjegjësinë për të planifikuar në kohë dhe në cilësi nevojat e tij dhe fondet publike. Rregullat e prokurimit publik përcaktojnë afate dhe procedura të detajuara për dërgimin e nevojave te organi qendror blerës.

Afati i 30 prillit, i vendosur në ligjin sektorial dhe i lidhur me "buxhetin e miratuar", krijon mospërputhje me ciklin e planifikimit buxhetor dhe me rregullat e prokurimit. Pasoja e mundshme është zhvillimi i procedurave në gjysmën e dytë të vitit ushtrimor.

2.2. Prokurimi i trajnimeve nuk kërkon ekspertizë specifike të Autoritetit

Prokurimi i trajnimeve të sigurisë kibernetike nuk ka asnjë veçori procedurale që ta dallojë nga prokurimi i shërbimeve të tjera intelektuale. Rezultati i një procedure prokurimi është lidhja e kontratës dhe zbatimi i saj nga një operator ekonomik privat. Ekspertiza e Autoritetit do të kishte vlerë nëse trajnimi do të realizohej nga vetë Autoriteti, me platformat dhe ekspertët e tij.

Ligji në fuqi e parashikon tashmë këtë mundësi, sepse Autoriteti "zhvillon dhe nxit… trajnime për personelin" e operatorëve në bashkëpunim me ta. Në prokurimin e përqendruar, përkundrazi, zbatimin e bën operatori ekonomik, ndërsa roli i Autoritetit reduktohet në administrim procedure. Për këtë administrim ekzistojnë institucione të specializuara.

Ekspertiza e Autoritetit ka vlerë reale në një rol tjetër: në përcaktimin e standardeve minimale, kurrikulave dhe kërkesave të kualifikimit për trajnimet sipas fushave (p.sh. qeverisja dhe menaxhimi i riskut, reagimi ndaj incidenteve, siguria e rrjeteve, forenzika digjitale, higjiena kibernetike për përdoruesit) dhe sipas niveleve. Këto standarde duhet të jenë të detyrueshme për t'u marrë parasysh nga operatorët kur planifikojnë dhe prokurojnë trajnime. Ky është roli natyror i një rregullatori. Ai garanton cilësi të njëtrajtshme pa e shndërruar rregullatorin në blerës.

2.3. Konflikti i interesit dhe zhvendosja e përgjegjësisë

Trajnimi është masë e menaxhimit të riskut që ligji ua ngarkon operatorëve dhe CSIRT-eve sektoriale. Edhe Direktiva NIS2 e trajton trajnimin si detyrim të vetë subjektit dhe të organeve të tij drejtuese. Nëse trajnimet i prokuron Autoriteti, operatori mbetet përgjegjës për masën para Autoritetit, por humbet kontrollin mbi zgjedhjen e saj. Autoriteti, nga ana tjetër, do të kontrollojë efektivitetin e trajnimeve që ka prokuruar vetë. Gjithashtu, Autoriteti do të ketë marrëdhënie kontraktore me operatorë ekonomikë të tregut të sigurisë kibernetike, shpesh të njëjtët që ofrojnë këshillim, vlerësim konformiteti ose shërbime të menaxhuara për operatorët që ai mbikëqyr. Kjo krijon rrezikun e konfliktit të interesit që ligji i prokurimit kërkon të shmanget "rreptësisht".

2.4. E njëjta logjikë vlen për çdo prokurim tjetër në fushën e sigurisë kibernetike. Arsyetimi i mësipërm vlen edhe më fort për çdo zgjerim të mundshëm të këtij roli te prokurimi i produkteve, shërbimeve ose zgjidhjeve të sigurisë kibernetike. Autoriteti që mbikëqyr masat e sigurisë, përcakton kërkesat teknike dhe certifikon produktet nuk mund të jetë edhe blerësi i tyre për llogari të subjekteve të mbikëqyrura. Për administratën shtetërore, zbatimi i masave të sigurisë kibernetike në infrastrukturat qeveritare i është ngarkuar me ligj operatorit qeveritar, drejtpërdrejt ose nëpërmjet shoqërive operatore TIK. Një rol blerës i Autoritetit do të mbivendosej me këtë kuadër.

2.5. Propozimi

Propozojmë heqjen e pikës 59 të nenit 5 dhe të shkronjës "k" të nenit 9, si dhe zëvendësimin e shkronjës "k" me këtë tekst:

"k) harton dhe miraton standardet minimale, kurrikulat dhe kërkesat e kualifikimit për trajnimet në fushën e sigurisë kibernetike, sipas fushave dhe niveleve, të cilat merren parasysh nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit në planifikimin, prokurimin dhe zbatimin e trajnimeve;".

Nëse Këshilli i Ministrave gjykon të dobishëm përqendrimin e blerjeve të trajnimeve për administratën shtetërore, ky përqendrim duhet të bëhet sipas nenit 53 të ligjit nr. 162/2020, nëpërmjet organeve qendrore blerëse ekzistuese. Autoriteti në këtë rast kontribuon vetëm me specifikimet teknike dhe standardet.

<u>Përgjigje</u>: Nuk është marrë në konsideratë. Kompetenca e parashikuar për Autoritetin për organizimin dhe kryerjen e prokurimeve të përqendruara për trajnimet në fushën e sigurisë kibernetike nuk krijon një regjim paralel prokurimi. Dispozita e projektligjit përcakton shprehimisht se këto prokurime kryhen në përputhje me legjislacionin në fuqi për prokurimin publik. Për rrjedhojë, rregullat mbi procedurat, afatet, kriteret, konfliktin e interesit, transparencën dhe mjetet e ankimit të parashikuara nga ligji nr. 162/2020, "Për prokurimin publik" i ndryshuar zbatohen plotësisht. Përcaktimi i një institucioni si përgjegjës për blerjen e përqendruar në një fushë të caktuar me ligj sektorial nuk krijon një regjim të veçantë prokurimi. Ndryshimi terminologjik ndërmjet "organit të blerjes së përqendruar" dhe "organit qendror blerës" nuk ndryshon përmbajtjen e kompetencës dhe, nëse është e nevojshme, mund të trajtohet si çështje terminologjie.

Kompetenca ka gjithashtu lidhje të drejtpërdrejtë me funksionet ekzistuese të Autoritetit. NIS2 e përfshin edukimin dhe trajnimin në politikat kombëtare të sigurisë kibernetike dhe e konsideron trajnimin pjesë të masave të menaxhimit të riskut. Në të njëjtën linjë, neni 9 i ligjit nr. 25/2024 i ngarkon Autoritetit zhvillimin dhe nxitjen e trajnimeve për personelin e operatorëve. Prokurimi i përqendruar përbën një mjet për realizimin efektiv të këtij funksioni, dhe jo një funksion të shkëputur nga kompetencat e Autoritetit.
Nuk qëndron as pretendimi se ekspertiza e Autoritetit nuk është e nevojshme në këtë proces. Në prokurimin e trajnimeve të specializuara, ekspertiza teknike është veçanërisht e rëndësishme për përcaktimin e specifikimeve teknike, kërkesave minimale, kritereve të kualifikimit dhe vlerësimit teknik të ofertave. Kjo mundëson që trajnimet e prokuruara të jenë në përputhje me nevojat reale të sigurisë kibernetike dhe me kërcënimet e identifikuara.
Gjithashtu, operatorët nuk e humbasin përgjegjësinë dhe kontrollin mbi nevojat e tyre. Projektligji parashikon që vetë operatorët t'i identifikojnë dhe t'i përcjellin nevojat për trajnim brenda afatit të përcaktuar dhe në përputhje me buxhetin e miratuar. Autoriteti konsolidon këto nevoja dhe realizon procedurën e blerjes së përqendruar, ndërsa përgjegjësia e operatorit për zbatimin e masave të sigurisë dhe menaxhimin e riskut mbetet e pandryshuar. Afati i 30 prillit është një mekanizëm për planifikimin dhe konsolidimin e nevojave dhe nuk ndryshon rregullat e planifikimit buxhetor apo procedurat e përcaktuara nga legjislacioni i prokurimit publik. Procedura zhvillohet mbi bazën e buxhetit të miratuar dhe në përputhje me rregullat përkatëse të prokurimit.
Nuk rezulton as krijimi i një konflikti interesi të natyrës së pretenduar. Organizimi i prokurimit të trajnimeve nuk e bën Autoritetin subjekt të mbikëqyrur dhe nuk i transferon atij përgjegjësinë e operatorit për masat e sigurisë. Autoriteti vepron si institucion publik që realizon një procedurë të përqendruar për një nevojë të përcaktuar me ligj, ndërsa operatorët ekonomikë përzgjidhen nëpërmjet procedurave dhe kritereve të parashikuara nga ligji nr. 162/2020.
Përsa i përket komentit të pikes 2.4 shprehemi që ky koment nuk gjen referencë në projektligj.

3. Heqja e CERT-it nga shkronja “c” e nenit 9 (neni 2, pika 1, e projektligjit)

Projektligji heq fjalët “dhe CERT-it” nga shkronja “c” e nenit 9. Megjithatë, neni 29 i ligjit, i cili mbetet në fuqi, e krijon CERT-in “pranë Autoritetit”, dhe vetë projektligji, në nenin 10, ndryshon pikën 4 të nenit 29 për të rregulluar pagesën e ekspertëve të CERT-it. Edhe neni 1, pika 2, shkronja “b”, dhe neni 5, pika 3, e ligjit e referojnë CERT-in si ekip pranë Autoritetit. Relacioni nuk jep asnjë shpjegim për këtë heqje. Propozojmë ose ruajtjen e tekstit në fuqi, ose, nëse synohet një model tjetër për CERT-in, harmonizimin e të gjitha dispozitave të lidhura me të.

Përgjigje: Në vijim të rishikimit të projektligjit, është hequr nga teksti i projektligjit ndryshimi i parashikuar në këtë pikë, që lidhej me heqjen e fjalëve “dhe CERT-it” nga shkronja “c” e nenit 9 të ligjit nr. 25/2024.
Për rrjedhojë, kjo pikë e projektligjit nuk është më pjesë e tekstit të rishikuar, dhe dispozita në fuqi mbetet e pandryshuar.

4. Organi kombëtar i certifikimit dhe autorizimi i organeve të vlerësimit të konformitetit (neni 2, pika 3, për shkronjat “l” dhe “ll” të nenit 9; neni 14, për pikën 5 të nenit 39; neni 16, për nenin 42 të ligjit).
4.1. Marrëdhënia me VKM-në nr. 813/2025 dhe me Aktin e Sigurisë Kibernetike VKM-ja nr. 813/2025 ia ka ngarkuar tashmë Autoritetit kompetencat e organit kombëtar të certifikimit të sigurisë kibernetike. Akti i Sigurisë Kibernetike u jep shteteve anëtare lirinë të caktojnë një ose më shumë autoritete të tilla. Për rrjedhojë, shkronja “l” e propozuar, në vetvete, i jep bazë ligjore një roli të caktuar me akt nënligjor. AKSHI nuk e kundërshton që Autoriteti të ushtrojë funksionin e mbikëqyrjes së certifikimit. Ajo që kundërshtojmë është mënyra se si ky funksion shtohet në projektligj: pa asnjë nga garancitë që kërkon e drejta e BE së dhe vetë VKM-ja nr. 813/2025.
Akti i Sigurisë Kibernetike vendos dy kërkesa të detyrueshme për autoritetin kombëtar të certifikimit:
a) autoriteti duhet të jetë i pavarur nga subjektet që mbikëqyr, për nga organizimi, vendimet e financimit, struktura juridike dhe vendimmarrja;
b) veprimtaritë që lidhen me lëshimin e certifikatave duhet të jenë rreptësisht të ndara nga veprimtaritë mbikëqyrëse dhe të kryhen në mënyrë të pavarur nga njëra-tjetra.

Këto kërkesa nuk janë formale. VKM-ja nr. 813/2025 i vendos si kushte për lidhjen e marrëveshjes së njohjes reciproke me Bashkimin Evropian, pa të cilën certifikatat e lëshuara në Shqipëri nuk njihen në tregun evropian. Projektligji i shton Autoritetit funksionin e certifikimit pa parashikuar asnjë nga këto garanci. Në të njëjtën kohë, ai i shton edhe funksione që e thellojnë mungesën e pavarësisë: autorizimin e organeve të vlerësimit (shkronja "ll"), regjistrimin e tyre me kritere të përcaktuara me udhëzim të brendshëm (neni 20, pika 7), tarifat (neni 42) dhe propozimin e listës së operatorëve të detyruar të përdorin produkte të certifikuara (neni 41). Kështu, i njëjti institucion do të krijonte kërkesën për certifikim, do të kontrollonte ofertën dhe hyrjen në treg dhe do të mbikëqyrte zbatimin.

4.2. Autorizimi nuk mund të zëvendësojë akreditimin (neni 39, pika 5)

Neni 14 i projektligjit zëvendëson në pikën 5 të nenit 39 fjalët "të akredituar" me "të autorizuara nga autoriteti përgjegjës". Ky ndryshim është i gabuar juridikisht dhe duhet hequr, për këto arsye:

a) Bie ndesh me vetë ligjin. Neni 5, pika 23, e ligjit, e cila nuk ndryshohet, i përkufizon organet e vlerësimit të konformitetit si persona juridikë "të akredituar nga institucioni përgjegjës për akreditimin". Po ashtu, neni 50, pika 7, i referohet njoftimit të organeve "që janë akredituar".

b) Bie ndesh me VKM-në nr. 813/2025. VKM-ja i përkufizon organet certifikuese dhe laboratorët e vlerësimit (ITSEF) si subjekte të akredituara nga institucioni përgjegjës për akreditimin dhe të autorizuara nga autoriteti. Autorizimi kërkohet vetëm për lëshimin e certifikatave në nivelin e sigurisë "të lartë", gjithmonë si kërkesë shtesë mbi akreditimin. Për nivelin "i konsiderueshëm" nuk kërkohet autorizim. Nëse lista publikohet vetëm për organet "e autorizuara", organet e akredituara për nivelin "i konsiderueshëm" do të përjashtoheshin nga lista, gjë që shtrembëron tregun.

c) Bie ndesh me Aktin e Sigurisë Kibernetike. Organet e vlerësimit të konformitetit akreditohen nga organi kombëtar i akreditimit. Vetëm kur skema vendos kërkesa të veçanta ose shtesë, ato autorizohen edhe nga autoriteti kombëtar i certifikimit. Kjo është edhe logjika e legjislacionit shqiptar për akreditimin.

ç) Krijon paqartësi. Shprehja "autoriteti përgjegjës" nuk është e përkufizuar në ligj, i cili përdor termin "Autoriteti" për AKSK-në dhe "institucioni përgjegjës për akreditimin" për organin e akreditimit.

4.3. Propozimi

Propozojmë heqjen e nenit 14 të projektligjit. Nëse synohet saktësimi i pikës 5 të nenit 39, teksti duhet të jetë: "…listën e organeve të vlerësimit të konformitetit për sigurinë kibernetike, të akredituara nga institucioni përgjegjës për akreditimin dhe, kur skema e certifikimit e kërkon, të autorizuara nga Autoriteti…".

Për shkronjat "l" dhe "ll" të nenit 9, kërkesa jonë parësore është heqja e tyre, sepse funksionet përkatëse janë të rregulluara tashmë në mënyrë të plotë nga VKM-ja nr. 813/2025 në zbatim të nenit 42 të ligjit. Si propozim alternativ, nëse Këshilli i Ministrave gjykon të nevojshme bazën ligjore në nivel ligji, propozojmë këtë formulim:

"l) ushtron funksionet e organit kombëtar të certifikimit të sigurisë kibernetike, duke garantuar pavarësinë nga subjektet që mbikëqyr dhe ndarjen e rreptë të veprimtarive që lidhen me lëshimin e certifikatave të sigurisë kibernetike nga veprimtaritë mbikëqyrëse, të cilat kryhen në mënyrë të pavarur nga njëra-tjetra, në përputhje me aktet e Bashkimit Evropian për certifikimin e sigurisë kibernetike;

ll) autorizon, në rastet kur skema e certifikimit e kërkon, organet e vlerësimit të konformitetit të akredituara nga institucioni përgjegjës për akreditimin, duke specifikuar kategoritë e produkteve TIK dhe profilet e mbrojtjes në të cilat shtrihet autorizimi.". Heqja e pikës 2 të nenit 42 (neni 16 i projektligjit) është në përputhje me këtë qëndrim, sepse autorizimi rregullohet tashmë nga VKM-ja nr. 813/2025. Megjithatë, kjo heqje humbet kuptimin nëse e njëjta zgjidhje, domethënë përcaktimi i kritereve me udhëzim të drejtorit, rifutet në pikën 7 të nenit 20. Për këtë shihni pikën 8 më poshtë.

Përgjigje: Nuk është marrë në konsideratë. Përcaktimi në nivel ligji i funksioneve të Autoritetit si organ kombëtar i certifikimit të sigurisë kibernetike dhe i kompetencës për autorizimin e organeve të vlerësimit të konformitetit nuk krijon funksione të reja, por konsolidon në nivel ligjor kompetenca që tashmë ushtrohen nga Autoriteti në zbatim të ligjit nr. 25/2024, "Për sigurinë kibernetike" dhe të VKM-së nr. 813, datë 30.12.2025, "Për miratimin e skemës kombëtare të certifikimit të sigurisë kibernetike, si dhe të niveleve të sigurisë së skemës".

Neni 42 i ligjit nr. 25/2024 parashikon miratimin e skemës kombëtare të certifikimit të sigurisë kibernetike dhe nxjerrjen e akteve nënligjore për zbatimin

e saj. Në zbatim të kësaj dispozite është miratuar VKM-ja nr. 813/2025, e cila përcakton Autoritetin si organ kombëtar të certifikimit të sigurisë kibernetike dhe rregullon procedurat për autorizimin e organeve të vlerësimit të konformitetit. Përfshirja e këtyre kompetencave në nenin 9 të ligjit synon të forcojë bazën ligjore të funksioneve të Autoritetit dhe të sigurojë koherencën ndërmjet ligjit dhe akteve nënligjore në fuqi.

Nuk qëndron pretendimi se përcaktimi i Autoritetit si organ kombëtar i certifikimit të sigurisë kibernetike, në vetëvete, bie ndesh me kërkesat e Aktit të Sigurisë Kibernetike të Bashkimit Evropian. Neni 58 i Rregullores (BE) 2019/881 kërkon që autoriteti kombëtar i certifikimit të jetë i pavarur nga subjektet që mbikëqyr, për sa i përket organizimit, vendimmarrjes për financimin, strukturës juridike dhe procesit vendimmarrës. Kjo kërkesë nuk nënkupton që autoriteti kombëtar i certifikimit duhet të jetë domosdoshmërisht një institucion i veçantë dhe i ndarë nga autoriteti kombëtar përgjegjës për sigurinë kibernetike, por që, në ushtrimin e funksioneve të tij, të mos jetë i varur nga subjektet ndaj të cilave ushtron kompetenca mbikëqyrëse.
Në rastin konkret, subjektet që mbikëqyren në kuadër të certifikimit janë subjektet dhe organet ndaj të cilave zbatohen kërkesat e skemës së certifikimit, ndërsa Autoriteti, në cilësinë e organit kombëtar të certifikimit, nuk është pjesë e tregut të produkteve, shërbimeve apo proceseve TIK që certifikohen dhe nuk është subjekt i mbikëqyrjes së vet. Për rrjedhojë, fakti që funksioni i organit kombëtar të certifikimit ushtrohet nga Autoriteti nuk krijon, në vetvete, marrëdhënien e varësisë që neni 58(3) i Rregullores (BE) 2019/881 i synon të shmangë.
Për rrjedhojë, përcaktimi i Autoritetit si organ kombëtar i certifikimit nuk cenon kërkesën e pavarësisë së parashikuar në nenin 58(3), për sa kohë që Autoriteti është i pavarur nga subjektet që mbikëqyr dhe garanton ndarjen funksionale dhe të pavarur të veprimtarive të certifikimit nga ato mbikëqyrëse, në përputhje me nenin 58(3) dhe (4) të Rregullores (BE) 2019/881.

Po ashtu, nuk qëndron pretendimi se Autoriteti krijon njëkohësisht kërkesën dhe ofertën në tregun e certifikimit. Autoriteti nuk ushtron veprimtari ekonomike, *nuk lëshon certifikata* për produktet, shërbimet apo proceset TIK *dhe nuk vepron si organ i vlerësimit të konformitetit*. Veprimtaria e vlerësimit të konformitetit

kryhet nga subjekte të pavarura, ndërsa Autoriteti ushtron funksione publike të natyrës rregullatore, mbikëqyrëse dhe autorizuese, në përputhje me modelin e parashikuar në Rregulloren (BE) 2019/881 dhe VKM-në nr. 813/2025.
Lidhur me nenin 39, pika 5, zëvendësimi i referimit nga organet "të akredituara" në organet "të autorizuara nga autoriteti përgjegjës" nuk synon të zëvendësojë akreditimin dhe as të shmangë rolin e institucionit përgjegjës për akreditimin. Akreditimi dhe autorizimi janë procedura me natyrë dhe funksione të ndryshme dhe plotësuese. Akreditimi vijon të kryhet nga institucioni përgjegjës për akreditimin, sipas legjislacionit përkatës, ndërsa autorizimi ushtrohet nga Autoriteti në rastet dhe sipas kushteve të përcaktuara në VKM-në nr. 813/2025.
Në këtë kuptim, autorizimi nuk zëvendëson akreditimin, por përbën një kërkesë shtesë, kur kjo parashikohet nga skema e certifikimit. Organi i vlerësimit të konformitetit duhet të plotësojë fillimisht kërkesat për akreditim dhe, në rastet e përcaktuara nga skema, t'i nënshtrohet edhe procedurës së autorizimit nga Autoriteti në rolin e organit kombëtar të certifikimit të sigurië kibernetike. Për rrjedhojë, dispozitat e projektligjit dhe VKM-ja nr. 813/2025 duhet të interpretohen në mënyrë sistematike dhe plotësuese, dhe jo si rregullime konkurruese apo përjashtuese ndaj njëra-tjetrës.
Sa i përket terminologjisë "autoriteti përgjegjës", kjo i referohet Autoritetit Kombëtar për Sigurinë Kibernetike, si organi kombëtar i certifikimit të sigurisë kibernetike, sipas përcaktimeve të ligjit nr. 25/2024 dhe VKM-së nr. 813/2025.
Për sa i përket heqjes së pikës 2 të nenit 42 të ligjit, kjo lidhet me faktin se procedurat, kriteret dhe kushtet për autorizimin e organeve të vlerësimit të konformitetit rregullohen tashmë në mënyrë të detajuar nga VKM-ja nr. 813/2025. Për rrjedhojë, shmanget përsëritja e panevojshme e dispozitave në nivel ligjor dhe nënligjor.
Për sa më sipër, përcaktimi në nivel ligji i funksioneve të Autoritetit si organ kombëtar i certifikimit dhe i kompetencës për autorizimin e organeve të vlerësimit të konformitetit është në përputhje me ligjin nr. 25/2024, me VKM-në nr. 813/2025 dhe me kërkesat e Rregullores (BE) 2019/881. Projektligji nuk zëvendëson akreditimin me autorizimin, nuk krijon konflikt interesi dhe nuk cenon kërkesat për pavarësi dhe ndarje funksionale.

5. Lista e operatorëve dhe heqja e konfidencialitetit (neni 3 i projektligjit; neni 12 i ligjit) Neni 12, pika 5, i ligjit në fuqi përcakton se lista e infrastrukturave

kritike dhe të rëndësishme të informacionit "është konfidenciale". Teksti i propozuar e riformulon këtë pikë dhe heq cilësimin e konfidencialitetit, pa asnjë shpjegim në relacion. Lista e infrastrukturave kritike është informacion me ndjeshmëri të lartë për sigurinë kombëtare, sepse u tregon aktorëve keqdashës objektivat me vlerë më të lartë. Asnjë akt i BE-së nuk kërkon publikimin e saj. Shtetet anëtare me përvojë të gjatë në këtë fushë e trajtojnë atë si informacion të mbrojtur. Propozojmë ruajtjen e fjalëve "është konfidenciale" në tekstin e pikës 5. Shtesa në pikën 4, "japin informacion dhe", nuk ka vërejtje nga ana jonë.

Përgjigje: Pranuar reflektuar.

6. Simulimet me shfrytëzim vulnerabilitetesh në infrastrukturat kritike (neni 4 i projektligjit; neni 13, shkronjat "g" dhe "ll", e ligjit)
Shkronja "ll" e propozuar e autorizon CSIRT-in Kombëtar të kryejë simulime në rrjetet dhe sistemet e infrastrukturave kritike "duke shfrytëzuar vulnerabilitetet e evidentuara". Operatori vetëm njoftohet dhe dakordësohet për fashat orare, ndërsa procedura miratohet me urdhër të drejtorit të përgjithshëm. Shfrytëzimi aktiv i vulnerabiliteteve në sisteme në prodhim që ofrojnë shërbime publike kritike mund të shkaktojë ndërprerje shërbimi, humbje ose korruptim të dhënash dhe dëme ndaj palëve të treta. Për këtë arsye, një veprimtari e tillë kërkon rregulla angazhimi të miratuara paraprakisht me shkrim, kufizim të fushës, mekanizma ndalimi të menjëhershëm, përcaktim të përgjegjësisë për dëmet dhe garanci për konfidencialitetin e gjetjeve. Direktiva NIS2 i njeh autoritetit kompetent të drejtën për auditime të sigurisë dhe për skanime sigurie. Këto duhet të bazohen në kritere objektive, jodiskriminuese, të drejta dhe transparente të vlerësimit të riskut, dhe kur është e nevojshme të kryhen në bashkëpunim me subjektin. Direktiva nuk parashikon shfrytëzim aktiv të vulnerabiliteteve pa pëlqimin e subjektit. Propozojmë që procedura e simulimeve, rregullat e angazhimit, pëlqimi paraprak me shkrim i operatorit dhe regjimi i përgjegjësisë të përcaktohen me vendim të Këshillit të Ministrave, jo me urdhër të drejtorit. Për infrastrukturat e administratës shtetërore, këto veprime duhet të kryhen në koordinim me operatorin qeveritar.

Përgjigje: Nuk është marrë në konsideratë. Kompetenca e parashikuar për CSIRT-in Kombëtar për kryerjen e simulimeve në rrjetet dhe sistemet e

infrastrukturave kritike nuk bie ndesh me kërkesat e Direktivës NIS2. Neni 32 i kësaj Direktive u njeh autoriteteve kompetente kompetencën për të kryer inspektime, auditime dhe skanime sigurie, mbi bazën e një vlerësimi objektiv dhe të bazuar në risk, për skanimet, Direktiva parashikon edhe bashkëpunimin, kur është e nevojshme, me subjektin përkatës.

Në rastin konkret, projektligji vendos kufizime të qarta: simulimet kryhen mbi *vulnerabilitete të evidentuara paraprakisht*, në vijim të skanimeve të sigurisë, ndërsa operatori i infrastrukturës së informacionit *njoftohet dhe dakordësohet paraprakisht për fashat kohore* të kryerjes së tyre. Për rrjedhojë, nuk bëhet fjalë për ndërhyrje të pakontrolluar në sistemet e operatorit, por për një veprimtari të planifikuar dhe të koordinuar, me qëllim verifikimin praktik të nivelit të ekspozimit dhe të qëndrueshmërisë së masave mbrojtëse.

Projektligji parashikon shprehimisht se simulimet kryhen *duke njoftuar dhe dakordësuar paraprakisht me operatorët për fashat orare të kryerjes së simulimeve.* Ky parashikim garanton koordinimin paraprak me operatorët dhe mundëson që, në përcaktimin e kohës së simulimeve, të merren në konsideratë natyra, funksionimi dhe vijueshmëria e sistemeve dhe shërbimeve që ato mbështesin. Për rrjedhojë, kërkesa për një pëlqim të veçantë paraprak për vetë kryerjen e simulimit nuk është e nevojshme, pasi projektligji parashikon mekanizmin e nevojshëm të njoftimit dhe dakordësimit paraprak për kryerjen e tij në mënyrë të koordinuar dhe të sigurt.

Rregullat teknike dhe procedurale të simulimeve përcaktohen me urdhër të Drejtorit të Përgjithshëm, duke mundësuar përshtatjen e tyre me natyrën e sistemeve, vulnerabilitetet e evidentuara dhe zhvillimin e kërcënimeve kibernetike.

Edhe referimi në DORA nuk mbështet pretendimin për ndalimin e testimeve aktive. Përkundrazi, DORA parashikon, për subjektet financiare që i nënshtrohen TLPT-së, testime të avancuara që mund të kryhen mbi sisteme aktive në prodhim, duke përcaktuar njëkohësisht kërkesa dhe masa mbrojtëse për kryerjen e tyre.

Për infrastrukturat e administratës shtetërore, koordinimi me operatorin qeveritar garantohet përmes njoftimit dhe dakordësimit të fashave kohore të testimit.

7. Detyrimet e reja të operatorëve për treguesit e kompromet imit dhe vulnerabilitetet (neni 7 i projektligjit; neni 17, pika 3, shkronjat “g” dhe “gj”, e ligjit)

AKSHI e mbështet shkëmbimin e treguesve të kompromet imit (IOC) dhe të sulmeve (IOA). Megjithatë, detyrimi për të zbatuar "masat për bllokimin, filtrimin, kufizimin, detektimin ose neutralizimin" e treguesve të komunikuar nga Autoriteti, i shoqëruar me gjobë deri në 1 000 000 lekë (neni 17 dhe 18 i projektligjit), nuk parashikon asnjë vlerësim të ndikimit operacional nga operatori. Treguesit mund të gjenerojnë "pozitivë të rremë". Bllokimi automatik i tyre në infrastruktura qeveritare mund të ndërpresë shërbime publike thelbësore. Kriteri "kur është teknikisht e realizueshme" është i paqartë dhe e lë të papërcaktuar se kush vendos për realizueshmërinë. Propozojmë që detyrimi të formulohet si detyrim për të vlerësuar dhe zbatuar, sipas vlerësimit të riskut të operatorit, masat e komunikuara, dhe për të raportuar arsyet kur një masë nuk zbatohet. Sanksioni duhet të lidhet vetëm me mosreagimin, jo me vendimin e argumentuar të operatorit.

Përgjigje: Nuk është marrë në konsideratë. NIS2 i njeh autoritetit kompetent të drejtën të nxjerrë udhëzime detyruese, përfshirë masat e nevojshme për parandalimin ose korrigjimin e një incidenti, ndërsa trajtimi i vulnerabiliteteve përbën pjesë të masave të detyrueshme të menaxhimit të riskut. Në këtë kuadër, përcaktimi i detyrimeve për operatorët për marrjen e masave ndaj treguesve të kompromet imit dhe të sulmeve është në përputhje me qasjen e NIS2 për parandalimin dhe reagimin ndaj kërcënimeve kibernetike.
Vërejtja e AKSHI-t nuk merr në konsideratë përmbajtjen konkrete të dispozitës. Së pari, detyrimi për marrjen e masave parashikohet *"kur është teknikisht e realizueshme",* duke përjashtuar një zbatim mekanik të masës në rastet kur ajo nuk mund të zbatohet në mënyrë të sigurt nga pikëpamja teknike dhe operacionale. Së dyti, masat përcaktohen në mënyrë alternative, konkretisht *"bllokimin, filtrimin, kufizimin, detektimin ose neutralizimin",* duke i dhënë operatorit mundësinë të zbatojë masën që është e përshtatshme në rrethanat konkrete. Për rrjedhojë, në rastet kur bllokimi ose neutralizimi mund të cenojë vijueshmërinë e një shërbimi, operatori i infrastrukturës mund të zbatojë masa të tjera, përfshirë detektimin ose filtrimin. Pra, qasja e bazuar në vlerësimin e riskut që propozon AKSHI është tashmë pjesë e dispozitës. Treguesit komunikohen pas verifikimit nga CSIRT-i Kombëtar, ndërsa gjoba e parashikuar (500 000 deri në 1 000 000 lekë) është ndër më të ultat e ligjit dhe është proporcionale.

8. Përcaktimi i kritereve të regjistrimit të organeve të vlerësimit me udhëzim të drejtorit (neni 8 i projektligjit; neni 20, pika 7, e ligjit)

Pika 7 e propozuar parashikon që procedurat dhe kriteret për regjistrimin e organeve të vlerësimit të konformitetit për vlerësimin e masave të sigurisë kibernetike përcaktohen me udhëzim të drejtorit të përgjithshëm të Autoritetit. Për korrektësi, vëmë në dukje se ligji në fuqi përmban një zgjidhje të ngjashme për organet e vlerësimit sipas skemës së certifikimit. Megjithatë, për organet që vlerësojnë masat e sigurisë, zgjidhja është edhe më problematike, për këto arsye:

a) Këto organe janë portierët e një tregu të detyrueshëm dhe periodik. Çdo operator i infrastrukturës kritike dhe të rëndësishme të informacionit është i detyruar t'i paraqesë Autoritetit raportin e vlerësimit të konformitetit të paktën një herë në dy vjet. Kush e përcakton listën e organeve të lejuara përcakton në fakt se cilët operatorë ekonomikë hyjnë në këtë treg. Kriteret e regjistrimit kanë, pra, pasoja të drejtpërdrejta në lirinë e veprimtarisë ekonomike dhe në konkurrencë.

b) Delegimi është i paplotë. Kushtetuta kërkon që ligji që autorizon nxjerrjen e akteve nënligjore të caktojë organin kompetent, çështjet që do të rregullohen dhe parimet në bazë të të cilave nxirren këto akte. Pika 7 e propozuar nuk përmban asnjë parim ose kriter orientues. Ajo i lë drejtorit të përgjithshëm liri të plotë për përcaktimin e kritereve.

c) Mungojnë garancitë kundër abuzimit dhe favorizimit. Një udhëzim i brendshëm mund të ndryshohet në çdo kohë, pa konsultim publik dhe pa kontroll ndërinstitucional. Kriteret mund të ndryshojnë me ndryshimin e drejtuesit të institucionit, duke lënë hapësirë për trajtim të pabarabartë dhe favorizim.

ç) Mbivendosje me akreditimin. Organet e vlerësimit janë, sipas ligjit, subjekte të akredituara. Çdo kriter shtesë regjistrimi duhet të jetë objektiv, proporcional dhe të mos dublojë kërkesat e akreditimit.

Propozojmë që pika 7 të formulohet si më poshtë: "7. Kriteret dhe procedurat për regjistrimin e organeve të vlerësimit të konformitetit për vlerësimin e masave të sigurisë kibernetike përcaktohen me vendim të Këshillit të Ministrave, me propozimin e Autoritetit, pas konsultimit me institucionin përgjegjës për akreditimin dhe me palët e interesit. Kriteret janë objektive, transparente, jodiskriminuese dhe proporcionale dhe nuk mbivendosen me kërkesat e akreditimit." Në të njëjtën frymë, amendimi në nenin 20 të projektligjit për ngarkimin e drejtorit të përgjithshëm duhet të ndryshohet përkatësisht (shih pikën 14 më poshtë).

Përgjigje: Nuk është marrë në konsideratë. Përcaktimi me udhëzim të Drejtorit të Përgjithshëm të Autoritetit i kritereve dhe procedurave për regjistrimin e organeve të vlerësimit të konformitetit nuk përbën delegim të pakufizuar të kompetencës dhe as krijon një regjim të ri për akreditimin e këtyre organeve. Dispozita ligjore përcakton në mënyrë të shprehur objektin e rregullimit, konkretisht kriteret dhe procedurat për regjistrimin e organeve që kryejnë vlerësimin e masave të sigurisë kibernetike, ndërsa akti nënligjor shërben për përcaktimin e rregullave teknike dhe procedurale të nevojshme për zbatimin e kësaj dispozite.
Në këtë drejtim, duhet bërë dallimi ndërmjet *akreditimit dhe regjistrimit*. Akreditimi vlerëson kompetencën dhe aftësinë e organit për të kryer veprimtari të caktuara të vlerësimit të konformitetit, ndërsa regjistrimi lidhet me ushtrimin e kësaj veprimtarie në kuadër të kërkesave specifike të legjislacionit për sigurinë kibernetike. Për rrjedhojë, regjistrimi nuk zëvendëson akreditimin dhe nuk synon të përsërisë vlerësimin e kryer nga institucioni përgjegjës për akreditimin.
Gjithashtu, fakti që organet e vlerësimit mund të ushtrojnë një veprimtari që lidhet me përmbushjen e detyrimeve periodike të operatorëve nuk e shndërron regjistrimin në një mekanizëm për përcaktimin e operatorëve ekonomikë që mund të hyjnë në treg. E drejta për ushtrimin e veprimtarisë buron nga përmbushja e kërkesave ligjore dhe teknike të zbatueshme, ndërsa regjistrimi shërben për të evidentuar organet që plotësojnë kërkesat përkatëse për ushtrimin e kësaj veprimtarie në fushën e sigurisë kibernetike.
Për sa i përket pretendimit për mungesën e parimeve orientuese, kriteret e regjistrimit nuk mund të shkëputen nga kuadri ligjor në të cilin vendoset kjo kompetencë. Ato duhet të jenë në përputhje me kërkesat e ligjit nr. 25/2024, legjislacionin për akreditimin dhe kuadrin përkatës të vlerësimit të konformitetit. Për më tepër, akti i drejtorit të përgjithshëm është akt zbatues i ligjit dhe nuk mund të vendosë kërkesa në kundërshtim me dispozitat ligjore apo me kompetencat e institucionit përgjegjës për akreditimin.
Nuk qëndron as pretendimi se forma e aktit krijon, në vetëvete, rrezik për trajtim të pabarabartë ose favorizim. Kriteret e regjistrimit do të zbatohen në mënyrë të njëjtë ndaj të gjitha organeve që kërkojnë regjistrimin dhe i nënshtrohen parimeve dhe kërkesave të përgjithshme të ligjshmërisë, objektivitetit dhe proporcionalitetit. Ndryshimi ose përditësimi i kritereve për shkak të zhvillimeve teknike apo të nevojave të fushës së sigurisë kibernetike është pikërisht një nga arsyet që justifikon

përcaktimin e tyre në një akt nënligjor zbatues dhe jo ngrirjen e tyre në një vendim të Këshillit të Ministrave.
Për rrjedhojë, nuk vlerësohet e nevojshme kalimi i kësaj kompetence në nivel vendimi të Këshillit të Ministrave. Zgjidhja e propozuar në projektligj ruan dallimin ndërmjet akreditimit dhe regjistrimit, mundëson përcaktimin e rregullave teknike dhe procedurale në përputhje me zhvillimet e fushës dhe nuk cenon kompetencat e institucionit përgjegjës për akreditimin.

9. Vetëdeklarimi i masave të sigurisë dhe i hostimit (neni 1, pika 3, për pikën 60 të nenit 5, dhe neni 9 i projektligjit; nenet 20/1 dhe 20/2 të ligjit)
Vetëdeklarimi mund të jetë instrument i dobishëm monitorimi. Megjithatë, dispozitat e propozuara kanë tri mangësi:
a) Forma, përmbajtja, afatet dhe procedurat e vetëdeklarimit përcaktohen me urdhër të drejtorit të përgjithshëm, ndërkohë që mosdorëzimi ose pasaktësia sanksionohen me gjoba deri në 2 000 000 lekë. Elementet thelbësore të një detyrimi të sanksionuar duhet të përcaktohen në ligj ose me vendim të Këshillit të Ministrave, në përputhje me nenin 118 të Kushtetutës dhe me legjislacionin për kundërvajtjet administrative.
b) Për operatorët e administratës publike, informacioni për mënyrën e hostimit është i përcaktuar tashmë me ligj. Nyja primare hostohet pranë Qendrës së të Dhënave Qeveritare, nyja sekondare pranë Qendrës së Vazhdueshmërisë së Punës, dhe monitorimi kryhet nga Qendra Kombëtare Operacionale e Sigurisë Kibernetike. Për këto operatorë, neni 20/2 krijon një detyrim të dyfishtë administrativ pa vlerë shtesë.
c) Një regjistër i centralizuar që përmban identitetin e hostuesve, vendndodhjen e infrastrukturave dhe masat e sigurisë së zbatuara për të gjitha infrastrukturat kritike të vendit përbën, në vetëvete, objektiv me vlerë shumë të lartë për aktorët keqdashës. Projektligji nuk përmban asnjë dispozitë për klasifikimin, ruajtjen dhe aksesin në këtë informacion.
Propozojmë që: forma dhe afatet e vetëdeklarimit të përcaktohen me vendim të Këshillit të Ministrave; operatorët që i nënshtrohen nenit 32 të ligjit të përjashtohen nga neni 20/2, sepse informacioni i tyre ekziston tashmë; dhe të shtohet një pikë e re që ky informacion trajtohet sipas legjislacionit për informacionin e klasifikuar.

Përgjigje: Nuk është marrë në konsideratë. Lidhur me pretendimin se forma, përmbajtja, afatet dhe procedurat e vetëdeklarimit duhet të përcaktohen në nivel vendimi të Këshillit të Ministrave, vlerësohet se dispozita e propozuar përcakton në

nivel ligji detyrimin për vetëdeklarim, subjektet që i nënshtrohen këtij detyrimi dhe pasojat në rast të mosrespektimit të tij, ndërsa elementet teknike dhe procedurale mund të përcaktohen me urdhër të Drejtorit të Përgjithshëm. Kjo zgjidhje mundëson përshtatjen e kërkesave të vetëdeklarimit me zhvillimet teknike dhe nevojat e mbikëqyrjes, pa ndryshuar thelbin e detyrimit të përcaktuar nga ligji. Për rrjedhojë, nuk kemi delegim të pakufizuar të kompetencës, pasi akti nënligjor kufizohet në rregullimin e mënyrës së zbatimit të një detyrimi të përcaktuar në ligj.
Sa i përket pretendimit për krijimin e një detyrimi të dyfishtë për operatorët e administratës publike, qëllimi i nenit 20/2 nuk është të kërkojë riparaqitjen e informacionit që është tashmë i disponueshëm nga institucioni që i administron këto të dhëna, por të sigurojë një pasqyrë të unifikuar dhe të përditësuar mbi mënyrën e hostimit dhe masat e sigurisë të aplikuara nga operatorët që janë subjekt i ligjit. Ekzistenca e detyrimeve të tjera ligjore apo institucionale për hostimin dhe monitorimin nuk e bën të panevojshëm këtë informacion për qëllimet e mbikëqyrjes së sigurisë kibernetike.
Neni 32 i ligjit nr.25/2024 përcakton ku duhet të hostohen sistemet, ndërsa vetëdeklarimi verifikon ku janë realisht të hostuara. Mbikëqyrësi nuk mund të mbështetet në të dhënat e operatorit të mbikëqyrur për të verifikuar vetë atë operator.
Lidhur me pretendimin për mungesën e dispozitave për mbrojtjen, ruajtjen dhe aksesin në informacionin e përftuar nëpërmjet vetëdeklarimit, ky shqetësim është adresuar në mënyrë të shprehur në projektligj. Konkretisht, nëpërmjet ndryshimit të shkronjës "dh" të pikës 2 të nenit 30 të ligjit, pas fjalës "mbrojtjen" shtohet fjala *"dhe konfidencialitetin",* duke përcaktuar detyrimin e Autoritetit për garantimin jo vetëm të mbrojtjes, por edhe të konfidencialitetit të informacionit që administron në ushtrimin e funksioneve të tij. Ky detyrim zbatohet në përputhje me natyrën dhe përmbajtjen e informacionit, si dhe me legjislacionin në fuqi për sigurinë e informacionin të klasifikuar.

10. Grupi i Bashkëpunimit për Inteligjencën Kibernetike (neni 1, pika 2, dhe neni 13 i projektligjit; neni 33/1 i ligjit)

AKSHI e mbështet krijimin e një mekanizmi të strukturuar për shkëmbimin e informacionit paralajmërues dhe përkufizimin e "inteligjencës kibernetike". Megjithatë, përbërja e propozuar e grupit përjashton institucionin që administron infrastrukturat qeveritare, pikërisht infrastrukturat që grupi synon të mbrojë. Kjo

përbën mangësi thelbësore. Propozojmë **shtimin e AKSHI-t si anëtar të Grupit**, për arsyet e mëposhtme:

a) **Statusi ligjor.** Ligji për sigurinë kibernetike e rendit AKSHI-n ndër "institucionet përgjegjëse të sigurisë dhe mbrojtjes kibernetike". Ligji për qeverisjen elektronike e ngarkon të garantojë zbatimin e masave të sigurisë kibernetike për të gjitha infrastrukturat kritike të informacionit, në cilësinë e operatorit qeveritar që i menaxhon ato. Përjashtimi i një institucioni të tillë nga grupi bie ndesh me vetë nenin 33 të ligjit, sipas të cilit Autoriteti koordinon veprimtarinë e tij me institucionet e sigurisë dhe të mbrojtjes.

b) **Pozicioni operacional.** AKSHI administron infrastrukturën qendrore të shërbimeve elektronike, përfshirë platformën "e-Albania", platformën qeveritare të ndërveprimit, Qendrën e të Dhënave Qeveritare, qendrat e rikuperimit dhe të vazhdueshmërisë së punës dhe rrjetin qeveritar (Govnet). Ligji e bën të detyrueshëm hostimin e infrastrukturave kritike të administratës publike në këto qendra. Pra, AKSHI zotëron të dhënat operacionale të drejtpërdrejta mbi përqendrimin më të madh të infrastrukturave kritike qeveritare në vend. Detyrat e grupit, si shkëmbimi i treguesve paralajmërues dhe vlerësimi i ndikimit të kërcënimeve "ndaj sigurisë kombëtare, ekonomisë dhe shërbimeve publike", nuk mund të kryhen në mënyrë të plotë pa këtë burim informacioni.

c) **Kapaciteti i njohur ndërkombëtarisht.** CSIRT-i qeveritar i AKSHI-t (NAIS G-CSIRT) është i akreditуar nga *Trusted Introducer* i TF-CSIRT që nga 8 janari 2025 dhe ka statusin e kandidatit për certifikim që nga 11 dhjetori 2025. Ai është anëtar i plotë i *FIRST (Forum of Incident Response and Security Teams*) që nga 1 maji 2025. Këto anëtarësime i japin AKSHI-t akses në rrjete të besuara të shkëmbimit të informacionit mbi kërcënimet. Ky informacion është pikërisht lënda e parë e inteligjencës kibernetike që grupi synon të shkëmbejë.

ç) **Informacioni i klasifikuar.** Për sistemet që përpunojnë informacion të klasifikuar, përfshirë atë të NATO-s dhe të BE-së, AKSHI zbaton politikat e institucionit përgjegjës për sigurinë e informacionit të klasifikuar. Kjo e bën AKSHI-n partner të përshtatshëm për pjesëmarrje në një grup që shkëmben informacion me institucionet e inteligjencës dhe të mbrojtjes.

d) **Përvoja.** Sulmet kibernetike ndaj infrastrukturave qeveritare shqiptare në vitin 2022 treguan se objektivi kryesor i aktorëve shtetërorë armiqësorë janë pikërisht sistemet që administron operatori qeveritar. Një mekanizëm inteligjence kibernetike që nuk e përfshin këtë operator do të kishte vlerë të kufizuar.

Propozojmë që në pikën 1 të nenit 33/1 të shtohet shkronja: “e) Agjencisë Kombëtare të Shoqërisë së Informacionit, në cilësinë e operatorit qeveritar që menaxhon infrastrukturat qeveritare;”. Rekomandojmë gjithashtu shtimin e një pike që i lejon grupit të ftojë, sipas nevojës, institucione të tjera të nenit 11, shkronja “a”, të ligjit.

Përgjigje: Nuk është marrë në konsideratë. Krijimi i Grupit të Bashkëpunimit për Inteligjencën Kibernetike synon të krijojë një mekanizëm të posaçëm ndërinstitucional për shkëmbimin, analizimin dhe vlerësimin e informacionit mbi kërcënimet kibernetike që mund të ndikojnë në sigurinë kombëtare. Përbërja e Grupit është përcaktuar duke pasur në konsideratë funksionet dhe kompetencat ligjore të institucioneve që marrin pjesë në të, si dhe nevojën për të ruajtur një ndarje të qartë ndërmjet funksionit të inteligjencës kibernetike dhe funksioneve operacionale të operatorëve të infrastrukturave.
Përfshirja e AKSHI-t në cilësinë e operatorit qeveritar nuk është e nevojshme për ushtrimin e funksioneve të Grupit. Fakti që AKSHI administron infrastruktura dhe sisteme qeveritare nuk e përcakton automatikisht atë si institucion përgjegjës për vlerësimin strategjik të inteligjencës kibernetike apo për koordinimin ndërinstitucional në nivel kombëtar. Informacioni teknik dhe operacional që lidhet me infrastrukturat qeveritare mund të përcillet dhe të shkëmbehet nëpërmjet mekanizmave të bashkëpunimit dhe koordinimit të parashikuara në legjislacionin për sigurinë kibernetike, pa qenë e nevojshme që operatori të jetë anëtar i përhershëm i Grupit.
Gjithashtu, përbërja e Grupit nuk pengon bashkëpunimin me AKSHI-n. Përkundrazi, në rastet kur informacioni apo ekspertiza teknike e AKSHI-t është e nevojshme për vlerësimin e një kërcënimi ose incidenti që prek infrastrukturat qeveritare, bashkëpunimi mund të realizohet në kuadër të kompetencave dhe mekanizmave ekzistues të bashkëpunimit ndërinstitucional. Kjo qasje shmang zgjerimin e panevojshëm të përbërjes së një strukture me funksion të posaçëm dhe ruan fleksibilitetin për përfshirjen e institucioneve të tjera sipas natyrës së çështjes që trajtohet.
Për sa i përket propozimit për parashikimin e një mundësie të përgjithshme për ftesën e institucioneve të tjera, vlerësohet se mekanizmat e bashkëpunimit dhe koordinimit mund të realizohen në funksion të çështjeve konkrete që shqyrton Grupi, pa qenë e nevojshme zgjerimi i përbërjes së tij në mënyrë të përhershme. Nëse për trajtimin e

një kërcënimi të caktuar kërkohet ekspertiza ose informacioni i një institucioni tjetër, ai mund të përfshihet në procesin përkatës të bashkëpunimit.

11. Detyrimi për përdorimin e produkteve, shërbimeve dhe proceseve të certifikuara sipas listës së miratuar me VKM (neni 15 i projektligjit; neni 41 i ligjit)

Ndryshimi i pikës 1 të nenit 41, ku Autoriteti "inkurajon" përdorimin e produkteve të certifikuara, është në drejtimin e duhur, sepse sjell dispozitën në përputhje me parimin e vullnetarizmit të certifikimit në BE. Megjithatë, pikat 3 deri në 6 të propozuara e përmbysin menjëherë këtë qasje. Ato i detyrojnë operatorët e përfshirë në një listë të miratuar me VKM të përdorin produkte, shërbime dhe procese TIK të certifikuara, ose të pajisen me certifikatë për to. Lista përditësohet "në rastet kur identifikohen nivele të pamjaftueshme të sigurisë kibernetike". Vlerësojmë se këto pika duhet të hiqen, për arsyet e mëposhtme.

11.1. Direktiva NIS2 e lejon detyrimin vetëm në mënyrë të synuar

Për korrektësi, pranojmë se Direktiva NIS2 u lejon shteteve anëtare t'u kërkojnë subjekteve të përdorin produkte, shërbime dhe procese TIK të certifikuara. Megjithatë, kjo mundësi ka kufij të qartë. Së pari, detyrimi lidhet me "produkte… të veçanta" dhe synon të demonstrojë përmbushjen e "kërkesave të veçanta" të masave të menaxhimit të riskut. Pra, ai përcaktohet sipas **kategorisë së produktit dhe kërkesës së sigurisë** që duhet plotësuar. Së dyti, certifikimi duhet të jetë sipas skemave evropiane të miratuara në zbatim të nenit 49 të Aktit të Sigurisë Kibernetike. Së treti, kur detyrimi vendoset në nivel evropian, ai përcaktohet sipas **kategorive të subjekteve**, me akt të deleguar të Komisionit. Asnjëherë nuk përcaktohet me listë individuale operatorësh të emërtuar.

Praktika e shteteve anëtare e konfirmon këtë qasje. Në rastet kur është vendosur detyrim, ai zbatohet për kategori të ngushta produktesh ose funksionesh, me akt normativ të përgjithshëm dhe me periudha transitore. Në Gjermani, për shembull, certifikimi është i detyrueshëm për pajisjet e matjes inteligjente (*smart meter gateways*). Në Francë, operatorët e rëndësisë jetike janë të detyruar të përdorin sisteme dhe ofrues të kualifikuar të detektimit të incidenteve, me afate të përcaktuara sipas sektorit. Asnjë nga këto regjime nuk e kthen certifikimin në masë ndaj operatorëve të veçantë në bazë të performancës së tyre.

11.2. Detyrimi është objektivisht i pazbatueshëm për shërbimet dhe proceset

Skema e vetme kombëtare e certifikimit, e miratuar me VKM-në nr. 813/2025 dhe e përafruar me skemën evropiane EUCC, zbatohet **vetëm për produktet TIK dhe për profilet e mbrojtjes**. Nuk ekziston asnjë skemë kombëtare për certifikimin e shërbimeve ose të proceseve TIK. Për rrjedhojë, detyrimi për të përdorur "shërbime dhe procese TIK të certifikuara" nuk mund të përmbushet nga asnjë operator. Megjithatë, mospërmbushja e tij do të sanksionohej.

11.3. Lista me VKM bazuar në "nivele të pamjaftueshme" është sanksion i fshehur, jo proporcional dhe diskriminues

Kriteri i përditësimit të listës, "kur identifikohen nivele të pamjaftueshme të sigurisë kibernetike", e kthen përfshirjen në listë në masë ndëshkuese. Për mangësitë në zbatimin e masave të sigurisë, ligji parashikon tashmë një procedurë të plotë: masa korrigjuese me afat të arsyeshëm, kundërvajtje administrative dhe sanksione. Kjo procedurë zbatohet me të gjitha garancitë procedurale, përfshirë të drejtën e dëgjimit dhe të ankimit. Lista e propozuar e anashkalon këtë procedurë dhe vendos një barrë financiare shumë më të rëndë, pa garanci procedurale. Për më tepër, dy operatorë të të njëjtit sektor, me të njëjtin profil risku, do t'u nënshtroheshin regjimeve të ndryshme vetëm sepse njëri është përfshirë në listë. Ky trajtim i pabarabartë bie ndesh me parimin e barazisë para ligjit dhe me kërkesën që kufizimet e të drejtave të jenë proporcionale. Për operatorët privatë, ai shtrembëron konkurrencën.

Detyrimi bie ndesh edhe me parimin e neutralitetit teknologjik, të cilin vetë ligji e shpall parim të përgjithshëm. Sipas këtij parimi, subjektet janë të lira të zgjedhin teknologjinë më të përshtatshme për nevojat e tyre, pa imponim dhe pa diskriminim të një lloji të veçantë teknologjie.

11.4. Kostot jashtëzakonisht të larta dhe mungesa e tregut

Detyrimi, siç është formuluar, nuk dallon ndërmjet blerjeve të reja dhe infrastrukturës ekzistuese. Kështu, ai mund të imponojë zëvendësimin e pajisjeve dhe sistemeve në përdorim, me kosto që i përballon operatori. Për operatorët e administratës publike, këto kosto bien mbi buxhetin e shtetit. Për operatorët privatë, ato rëndojnë mbi bizneset dhe, në fund, mbi konsumatorët. Tregu i produkteve të certifikuara sipas EUCC është ende në zhvillim edhe në BE. Në Shqipëri, VKM-ja nr. 813/2025 sapo ka hyrë në fuqi, organet e vlerësimit duhet të akreditohen dhe, për nivelin e lartë, të autorizohen, ndërsa marrëveshja e njohjes reciproke me BE-në nuk është lidhur ende. Relacioni pohon se dispozitat e tjera, përveç CSIRT-eve, "nuk sjellin efekte financiare shtesë të drejtpërdrejta". Ky pohim nuk qëndron për nenin 41 dhe tregon se ndikimi i tij nuk është vlerësuar fare.

11.5. Drejtimi i së drejtës së BE-së: detyrimet vendosen mbi prodhuesit, jo mbi përdoruesit

Akti i Qëndrueshmërisë Kibernetike (CRA) vendos kërkesat thelbësore të sigurisë për produktet me elemente digjitale, si siguria që në projektim, trajtimi i vulnerabiliteteve dhe vlerësimi i konformitetit, **mbi prodhuesit, para vendosjes së produktit në treg**. Certifikimi i detyrueshëm mbetet i rezervuar vetëm për kategori produktesh kritike, të përcaktuara me akt të deleguar të Komisionit. Rregullorja DORA, nga ana e saj, nuk vendos asnjë detyrim për përdorimin e produkteve të certifikuara nga subjektet financiare. Ajo mbështetet te korniza e menaxhimit të riskut TIK, testimi dhe menaxhimi i riskut të palëve të treta. Pra, qasja evropiane synon ta garantojë sigurinë e produkteve në nivel tregu. Ajo nuk i detyron operatorët individualë të zëvendësojnë infrastrukturat ekzistuese.

11.6. Propozimi

Kërkesa jonë parësore është **ruajtja e ndryshimit të pikës 1 dhe heqja e pikave 3, 4, 5 dhe 6 të nenit 41**, si dhe e pikës 1 të nenit 20 të projektligjit, që lidhet me to. Si **propozim alternativ**, nëse Këshilli i Ministrave gjykon të nevojshme një bazë ligjore për certifikimin e detyrueshëm në përputhje me nenin 24 të Direktivës NIS2, propozojmë këtë formulim:

"3. Këshilli i Ministrave, me propozimin e Autoritetit, bazuar në një vlerësim të ndikimit rregullator dhe pas konsultimit publik, mund të përcaktojë kategori të veçanta produktesh TIK për të cilat operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, në blerjet e reja, përdorin produkte të certifikuara sipas një skeme evropiane të certifikimit të sigurisë kibernetike ose sipas skemës kombëtare të përafruar me të, me qëllim demonstrimin e përmbushjes së kërkesave të veçanta të nenit 21 të këtij ligji.

4. Vendimi i Këshillit të Ministrave sipas pikës 3 të këtij neni përcakton kategoritë e produkteve, kërkesat e sigurisë që synohen dhe një periudhë tranzitore jo më të shkurtër se 24 muaj. Vendimi miratohet vetëm kur në treg ka produkte të certifikuara dhe organe të vlerësimit të konformitetit në numër të mjaftueshëm. Detyrimi nuk zbatohet për produktet dhe sistemet në përdorim para hyrjes në fuqi të vendimit."

Përgjigje: Nuk është marrë në konsideratë. Neni 24 i Direktivës (BE) 2022/2555 (NIS2) nuk e kufizon përdorimin e detyrueshëm të produkteve, shërbimeve dhe proceseve TIK të certifikuara vetëm në raste të përcaktuara individualisht apo vetëm për kategori të ngushta produktesh. Përkundrazi, neni 24(1) u jep shprehimisht

shteteve anëtare mundësinë t'u kërkojnë subjekteve thelbësore dhe të rëndësishme të përdorin produkte, shërbime dhe procese të veçanta TIK të certifikuara sipas skemave evropiane të certifikimit, me qëllim demonstrimin e përmbushjes së kërkesave të veçanta të masave të menaxhimit të riskut të përcaktuara në nenin 21.
Në këtë kuptim, pretendimi se qasja e projektligjit bie ndesh me parimin e vullnetarizmit të certifikimit nuk qëndron. Neni 56(2) i Rregullores (BE) 2019/881 përcakton se certifikimi është vullnetar, përveç rasteve kur e drejta e Bashkimit ose e një shteti anëtar parashikon ndryshe. Pra, vetë kuadri evropian njeh mundësinë e vendosjes së detyrimeve për përdorimin e produkteve, shërbimeve ose proceseve të certifikuara.
Për më tepër, neni 24(2) i NIS2 parashikon shprehimisht se, kur identifikohen nivele të pamjaftueshme të sigurisë kibernetike, Komisioni mund të përcaktojë, me akte të deleguara, kategoritë e subjekteve që do të detyrohen të përdorin produkte, shërbime ose procese të caktuara të certifikuara ose të pajisen me certifikatë, duke përfshirë edhe një periudhë zbatimi. Për rrjedhojë, përdorimi i identifikimit të niveleve të pamjaftueshme të sigurisë si bazë për ndërmarrjen e masave të certifikimit nuk përbën, në vetvete, një mekanizëm ndëshkues, por është një qasje e parashikuar shprehimisht nga NIS2.
Në këtë kuadër, dispozitat e propozuara në nenin 41 nuk synojnë të vendosin një sanksion të ri për operatorët, por të krijojnë një mekanizëm parandalues për rritjen e nivelit të sigurisë kibernetike në ato raste kur vlerësohet se përdorimi i produkteve, shërbimeve ose proceseve të certifikuara është i nevojshëm për përmbushjen e kërkesave të sigurisë. Detyrimi për përdorimin e produkteve apo shërbimeve të certifikuara duhet dalluar nga sanksioni administrativ: i pari është një masë rregullatore dhe parandaluese, ndërsa sanksioni aplikohet në rast të mosrespektimit të detyrimit ligjor.
Gjithashtu, nuk qëndron pretendimi se përcaktimi i operatorëve me vendim të Këshillit të Ministrave është në kundërshtim me NIS2. Neni 24(1) i drejtohet subjekteve thelbësore dhe të rëndësishme, ndërsa neni 24(2) i referohet kategorive të subjekteve që mund t'i nënshtrohen këtij detyrimi. Për rrjedhojë, përcaktimi në nivel kombëtar i subjekteve ose kategorive të operatorëve që, në funksion të profilit të tyre të riskut dhe nevojave të sigurisë, duhet të përdorin produkte të certifikuara, është një mënyrë e lejueshme për zbatimin e këtij mekanizmi në kuadrin kombëtar.
Sa i përket pretendimit se detyrimi shtrihet edhe mbi shërbimet dhe proceset TIK, ky argument nuk mund të përdoret si bazë për heqjen e dispozitës. Rregullorja (BE)

2019/881 nuk e kufizon konceptin e certifikimit vetëm te produktet TIK, por parashikon shprehimisht skema që mund të mbulojnë produkte, shërbime dhe procese TIK. Për rrjedhojë, ekzistenca ose jo e një skeme konkrete kombëtare në një moment të caktuar nuk e bën të pavlefshme bazën ligjore për përdorimin e ardhshëm të skemave të certifikimit për kategoritë përkatëse. Zbatimi konkret i detyrimit do të kushtëzohet nga ekzistenca dhe zbatueshmëria e skemës përkatëse të certifikimit.
Nuk qëndron as pretendimi se dispozita cenon parimin e neutralitetit teknologjik. Detyrimi nuk përcakton një prodhues, markë, teknologji apo zgjidhje specifike, por lidhet me përmbushjen e kërkesave të sigurisë përmes përdorimit të produkteve, shërbimeve ose proceseve që plotësojnë kërkesat e një skeme të përcaktuar certifikimi. Kjo e vendos kërkesën në funksion të rezultatit të sigurisë dhe jo të favorizimit të një teknologjie apo operatori ekonomik të caktuar.
Për sa i përket kostove, pretendimi se dispozita sjell automatikisht zëvendësimin e të gjitha produkteve dhe sistemeve ekzistuese është më i gjerë se përmbajtja e saj. Detyrimi duhet të zbatohet në përputhje me përcaktimet konkrete të aktit që miraton listën dhe me kushtet e zbatimit të tij. Në çdo rast, fakti që një masë rregullatore mund të sjellë kosto për operatorët nuk e bën atë të papajtueshme me NIS2, veçanërisht kur synimi është përmbushja e kërkesave të sigurisë kibernetike dhe reduktimi i riskut.
Në këtë drejtim, duhet theksuar edhe se vetë Rregullorja (BE) 2019/881 parashikon që skemat evropiane të certifikimit të përcaktojnë kategoritë e produkteve, shërbimeve ose proceseve që mbulohen, kërkesat e sigurisë, kriteret e vlerësimit dhe mekanizmat për ruajtjen e pajtueshmërisë. Pra, detyrimi i përdorimit të produkteve ose shërbimeve të certifikuara nuk funksionon në mënyrë abstrakte, por lidhet me një skemë konkrete certifikimi dhe me kërkesa të përcaktuara të sigurisë.
Për rrjedhojë, propozimi i AKSHI-t për heqjen e pikave 3, 4, 5 dhe 6 të nenit 41 nuk pranohet. Dispozitat e propozuara synojnë të krijojnë bazën ligjore për zbatimin në nivel kombëtar të mekanizmit të parashikuar në nenin 24 të NIS2, duke mundësuar që, në funksion të nivelit të sigurisë kibernetike dhe kërkesave konkrete të riskut, të përcaktohen rastet kur përdorimi i produkteve, shërbimeve ose proceseve të certifikuara bëhet i detyrueshëm.
Gjithashtu, nuk pranohet propozimi alternativ, pasi kufizimi paraprak i mekanizmit vetëm në “blerjet e reja”, vetëm në produktet TIK dhe vetëm në skemat evropiane do të ngushtonte pa nevojë hapësirën që neni 24 i NIS2 u njeh shteteve anëtare për të vendosur kërkesa të përshtatshme për subjektet thelbësore dhe të rëndësishme.

Përgjigje: Nuk është marrë në konsideratë. Parashikimet e projektligjit lidhur me përdorimin e produkteve, shërbimeve dhe proceseve TIK të certifikuara mbështeten drejtpërdrejt në nenin 24 të Direktivës (BE) 2022/2555 (NIS2), i cili u jep shteteve anëtare mundësinë që, për qëllime të demonstrimit të përputhshmërisë me kërkesat e masave të menaxhimit të rrezikut të parashikuara në nenin 21 të saj, t'u kërkojnë subjekteve thelbësore dhe të rëndësishme të përdorin produkte, shërbime dhe procese TIK të certifikuara sipas skemave evropiane të certifikimit të sigurisë kibernetike. Po kështu, neni 24 parashikon mundësinë e kërkimit të pajisjes me certifikatë, ndërsa paragrafi 2 parashikon përcaktimin e kategorive të subjekteve për të cilat mund të zbatohet ky detyrim.
Në këtë kuadër, projektligji e konkretizon këtë mundësi në nivel kombëtar, duke parashikuar fillimisht, në pikën 1 të nenit 15 të tij, i cili ndryshon nenin 41 të ligjit 25/2024, inkurajimin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit për përdorimin e produkteve, shërbimeve dhe proceseve TIK të certifikuara, ndërsa në pikat 3–6 përcakton rastet në të cilat ky përdorim bëhet i detyrueshëm. Pra, projektligji nuk vendos një detyrim të përgjithshëm dhe automatik për të gjithë operatorët, por ndërton një mekanizëm të diferencuar, sipas të cilit detyrimi zbatohet vetëm ndaj operatorëve të përcaktuar në mënyrë të posaçme.
Kriteret e propozuara për përcaktimin e operatorëve, vlerësimi i ndikimit, niveli i rrezikut, rezultatet e vlerësimeve të sigurisë kibernetike dhe konsultimi me operatorët, synojnë pikërisht që detyrimi të zbatohet në mënyrë proporcionale dhe të bazuar në rrezik. Për rrjedhojë, lista e miratuar me vendim të Këshillit të Ministrave nuk përbën një masë ndëshkuese apo një "sanksion të fshehtë", por një instrument zbatues për identifikimin e kategorive/operatorëve ndaj të cilëve, për shkak të nivelit të rrezikut dhe nevojave konkrete të sigurisë kibernetike, kërkohet një nivel më i lartë sigurie përmes certifikimit.
Gjithashtu, parashikimi i pikës 5 të projektligjit, sipas të cilit vendimi i Këshillit të Ministrave përcakton edhe periudhën e zbatimit të detyrimit, shërben si garanci për një zbatim gradual dhe të parashikueshëm të kërkesës së re. Kjo shmang aplikimin e menjëhershëm të detyrimit dhe mundëson që operatorët të kenë një periudhë të përshtatshme për përmbushjen e tij.
Pretendimi se kjo skemë bie ndesh me parimin e neutralitetit teknologjik nuk qëndron. Projektligji nuk përcakton produkte, prodhues apo ofrues të caktuar, por vendos si kriter certifikimin sipas një skeme kombëtare ose evropiane të certifikimit

të sigurisë kibernetike. Për rrjedhojë, kërkesa lidhet me nivelin dhe kërkesat e sigurisë që duhet të përmbushë produkti, shërbimi ose procesi TIK dhe jo me zgjedhjen e një teknologjie, marke apo ofruesi të caktuar.
Në këtë drejtim, duhet mbajtur parasysh edhe Rregullorja (BE) 2019/881, e cila parashikon se certifikimi i sigurisë kibernetike është, në parim, vullnetar, përveç rasteve kur e drejta e Bashkimit Evropian ose e një shteti anëtar parashikon ndryshe. Për rrjedhojë, legjislacioni kombëtar mund të përcaktojë raste në të cilat certifikimi ose përdorimi i produkteve, shërbimeve apo proceseve të certifikuara bëhet i detyrueshëm.
Për sa i përket pretendimit se skema e propozuar nuk mund të zbatohet për shërbime dhe procese TIK, ky argument nuk qëndron. VKM nr. 813, datë 30.12.2025, "Për miratimin e Skemës Kombëtare të Certifikimit të Sigurisë Kibernetike, si dhe të niveleve të sigurisë së skemës", përcakton se certifikimi i sigurisë kibernetike kryhet për produkte TIK, shërbime TIK dhe procese TIK, në përputhje me kërkesat dhe fushën e zbatimit të skemës. Për rrjedhojë, pretendimi se kuadri kombëtar i certifikimit nuk parashikon certifikimin e shërbimeve dhe proceseve TIK nuk është i bazuar, pasi këto kategori janë të përfshira shprehimisht në Skemën Kombëtare të Certifikimit të miratuar me VKM nr. 813/2025.
Në këtë kuptim, projektligji nuk synon të imponojë në mënyrë të menjëhershme certifikimin e çdo produkti, shërbimi ose procesi TIK, por krijon bazën ligjore për aktivizimin e një detyrimi të tillë vetëm në rastet e përcaktuara në mënyrë të posaçme, në varësi të nivelit të rrezikut, rezultateve të vlerësimeve të sigurisë kibernetike, skemave të certifikimit në fuqi dhe periudhës së përcaktuar për zbatim. Për më tepër, detyrimi për përdorimin e produkteve, shërbimeve ose proceseve të certifikuara nuk përbën masë administrative ndëshkuese në vetvete. Ai është një kërkesë e sigurisë kibernetike, e cila synon të sigurojë përmbushjen e një niveli të përshtatshëm sigurie nga operatorët me ekspozim të lartë ndaj rrezikut. Pasoja administrative mund të lidhet vetëm me mospërmbushjen e një detyrimi ligjor të zbatueshëm dhe jo me faktin se një operator është përfshirë në listë.
Sa i përket pretendimit se përfshirja në listë do të krijonte diskriminim ndërmjet operatorëve, vetë mekanizmi i parashikuar në projektligj e kushtëzon përfshirjen me kritere objektive të lidhura me rrezikun dhe ndikimin, ndërsa lista miratohet me vendim të Këshillit të Ministrave, me propozimin e Autoritetit. Përditësimi i saj në rast të identifikimit të niveleve të pamjaftueshme të sigurisë kibernetike siguron që

detyrimi të jetë i lidhur me gjendjen faktike të rrezikut dhe të mund të përshtatet me ndryshimin e saj.
Për rrjedhojë, parashikimet e projektligjit përbëjnë një mekanizëm kombëtar për zbatimin e mundësisë së parashikuar në nenin 24 të Direktivës (BE) 2022/2555 dhe janë të ndërlidhura me kuadrin e certifikimit të përcaktuar në Rregulloren (BE) 2019/881 dhe në VKM nr. 813, datë 30.12.2025.

12. Kundërvajtjet administrative dhe masa e gjobave (nenet 17 dhe 18 të projektligjit; nenet 44 dhe 45 të ligjit)

Projektligji i rrit gjobat për kundërvajtjet ekzistuese të shkronjave "b", "c", "ç" dhe "e" të nenit 44 **dhjetë herë**, nga 200 000–400 000 lekë në 2 000 000–4 000 000 lekë. Po ashtu, ai i rrit dhjetë herë edhe gjobat për shkronjën "dh", nga 400 000–1 000 000 lekë në 4 000 000–10 000 000 lekë. Këto kundërvajtje përfshijnë shkelje formale, si mosraportimi i pikës së kontaktit. Relacioni nuk jep asnjë të dhënë mbi zbatimin e deritanishëm të sanksioneve, mbi mosrespektimin e detyrimeve apo mbi arsyet për një rritje të tillë. Parimi i proporcionalitetit të sanksioneve, i kërkuar edhe nga Direktiva NIS268, nuk mund të vlerësohet pa një argumentim të tillë. Për operatorët e administratës publike, gjoba paguhet nga buxheti i shtetit dhe derdhet në buxhetin e shtetit, pa efekt real parandalues. Propozojmë ruajtjen e masave në fuqi për këto kundërvajtje, ose argumentimin e plotë të rritjes në relacion. Kundërvajtjet e reja (shkronjat "f", "g", "gj" dhe "h") duhet të rishikohen në përputhje me vërejtjet e pikave 7 dhe 9 më sipër.

Përgjigje: Nuk është marrë në konsideratë. Pretendimi se rritja e masës së gjobave përbën një rritje të pajustifikuar dhe të pambështetur në parimin e proporcionalitetit nuk qëndron. Në përputhje me nenin 34 të Direktivës (BE) 2022/2555 (NIS2), sanksionet administrative për shkeljet e detyrimeve të sigurisë kibernetike duhet të jenë efektive, proporcionale dhe bindëse, duke marrë në konsideratë rrethanat e çdo rasti konkret. Për shkeljet e neneve 21 dhe 23 të Direktivës, NIS2 përcakton gjithashtu nivele minimale të kufirit maksimal të gjobave, përkatësisht të paktën 10 000 000 euro ose 2% të xhiros vjetore globale për subjektet thelbësore dhe të paktën 7 000 000 euro ose 1,4% të xhiros vjetore globale për subjektet e rëndësishme, sipas shumës më të lartë.

Në këtë kuadër, masat e parashikuara në projektligj nuk mund të konsiderohen të ekzagjeruara vetëm për faktin se përfaqësojnë një rritje në raport me masat aktualisht në fuqi. Përkundrazi, rritja synon të sigurojë që sanksionet të kenë karakter realisht *parandalues dhe bindës*, duke marrë në konsideratë natyrën dhe rëndësinë e detyrimeve që synojnë të garantojnë vazhdimësinë dhe sigurinë e shërbimeve të mbështetura në infrastrukturat kritike dhe të rëndësishme të informacionit.
Gjithashtu, duhet evidentuar se kufijtë e përcaktuar në projektligj nuk nënkuptojnë aplikimin automatik të masës maksimale të gjobës. Përkundrazi, intervali midis kufirit minimal dhe maksimal i jep mundësi Autoritetit që, në zbatimin e legjislacionit për kundërvajtjet administrative, dhe metodologjisë për përcaktimin e masës së dënimit administrativ gjobë të përcaktojë masën konkrete në funksion të rrethanave të shkeljes, rëndësisë së saj, pasojave, shkallës së përgjegjësisë dhe rrethanave të tjera të parashikuara nga legjislacioni në fuqi. Vetë neni 34, pika 3 e direktivës NIS2 kërkon që, në përcaktimin e ekzistencës dhe masës së gjobës në çdo rast konkret, të merren në konsideratë rrethanat përkatëse.
Nuk qëndron as argumenti se kundërvajtja që lidhet me mosraportimin e pikës së kontaktit është thjesht një shkelje formale. Përcaktimi dhe komunikimi i pikës së kontaktit përbën një element të rëndësishëm të mekanizmit të koordinimit ndërmjet operatorit dhe Autoritetit, veçanërisht në rast incidenti kibernetik. Mungesa e një pike kontakti të identifikuar dhe funksionale mund të pengojë komunikimin në kohë reale, koordinimin e masave dhe reagimin ndaj incidenteve. Për këtë arsye, detyrimi nuk mund të vlerësohet vetëm në funksion të karakterit formal të veprimit të kërkuar, por në raport me funksionin që ai përmbush në kuadrin e sigurisë kibernetike.
Për sa i përket operatorëve të administratës publike, neni 34 pika 7 e direktivës NIS2 parashikon shprehimisht se çdo shtet anëtar mund të përcaktojë nëse dhe në çfarë mase mund të vendosen gjoba administrative ndaj subjekteve të administratës publike. Në këtë drejtim, ligjvënësi shqiptar ka zgjedhur që edhe këto subjekte t'i nënshtrojë mekanizmit të përgjegjësisë administrative, në funksion të garantimit të zbatimit efektiv të detyrimeve të sigurisë kibernetike. Fakti që për subjektet publike pagesa kryhet brenda sistemit buxhetor nuk e eliminon funksionin juridik dhe institucional të sanksionit, pasi përgjegjësia për përmbushjen e detyrimeve lidhet me subjektin dhe strukturat përgjegjëse për administrimin e tij.
Për rrjedhojë, rritja e masave të gjobave duhet parë në kontekstin e forcimit të mekanizmit të zbatimit të ligjit dhe të nevojës për sanksione efektive, proporcionale dhe bindëse, dhe jo vetëm në raport me vlerën nominale të gjobës sipas legjislacionit

aktual. Diferencimi ndërmjet kufirit minimal dhe maksimal të gjobës mundëson individualizimin e sanksionit sipas rrethanave konkrete dhe, në këtë mënyrë, respekton kërkesën për proporcionalitet.
Sa i përket kundërvajtjeve të reja të parashikuara në shkronjat "f", "g", "gj" dhe "h" të pikes 2, të nenit 17 të projektligjit i cili ndryshon nenin 44 të ligjit 25/2024, ato lidhen me detyrime të reja ose të konsoliduara në projektligj dhe janë pjesë e mekanizmit të mbikëqyrjes dhe zbatimit të kërkesave të sigurisë kibernetike.

13. Përfshirja e pushtetit vendor në sektorët me kritikalitet të lartë (neni 19 i projektligjit; aneksi I i ligjit)

Projektligji shton në aneksin I, sektori "Administrata publike", subjektet e vetëqeverisjes vendore. Direktiva NIS2 ua lë këtë zgjedhje shteteve anëtare, pra nuk e bën të detyrueshme. Përfshirja në aneksin I ka pasoja të drejtpërdrejta dhe të rëndësishme. Detyrimet e nenit 32 të ligjit zbatohen për operatorët e administratës publike "sipas aneksit 1". Kjo do të thotë që të gjitha bashkitë do të detyroheshin të hostojnë nyjën primare të infrastrukturës së tyre pranë Qendrës së të Dhënave Qeveritare dhe nyjën sekondare pranë Qendrës së Vazhdueshmërisë së Punës, dhe do të monitoroheshin nga Qendra Kombëtare Operacionale. Kjo sjell nevojë për kapacitete të reja hostimi, rrjeti dhe monitorimi, si dhe kosto për njësitë e vetëqeverisjes vendore dhe për institucionet qendrore. Relacioni nuk i vlerëson fare këto kosto. Propozojmë që ky ndryshim të pezullohet deri në hartimin e një vlerësimi ndikimi, në bashkëpunim me AKSHI-n dhe me ministrinë përgjegjëse për pushtetin vendor. Nëse ruhet, duhet të shoqërohet me dispozitë kalimtare që parashikon një periudhë zbatimi të arsyeshme.

Përgjigje: Nuk është marrë në konsideratë. Përfshirja e njësive të vetëqeverisjes vendore në sektorin "Administrata publike" është një zgjedhje legjislative e lejuar shprehimisht nga Direktiva (BE) 2022/2555 (NIS2). Neni 2, pika 5, shkronja "a", e Direktivës u jep shteteve anëtare mundësinë të përfshijnë në fushën e zbatimit edhe subjektet e administratës publike në nivel rajonal dhe vendor. Për rrjedhojë, përfshirja e tyre në Aneksin I të ligjit është në përputhje me kuadrin e NIS2.
Gjithsesi, duhet bërë dallimi ndërmjet përfshirjes së sektorit në Aneksin I dhe identifikimit të një subjekti si operator i infrastrukturës kritike ose të rëndësishme të informacionit. Përfshirja e njësive të vetëqeverisjes vendore në Aneksin I nuk

nënkupton që çdo bashki bëhet automatikisht operator dhe nuk sjell, për këtë arsye, zbatimin automatik të të gjitha detyrimeve të parashikuara për operatorët. Subjektet konkrete identifikohen në përputhje me nenin 12 të ligjit dhe përfshihen në listën e miratuar me vendim të Këshillit të Ministrave, mbi bazën e kritereve të përcaktuara nga kuadri ligjor dhe nënligjor.
Për më tepër njësitë e vetëqeverisjes vendore nuk përfshihen për herë të parë në kuadrin e operatorëve të infrastrukturave të informacionit. Ato janë identifikuar tashmë si operatorë nëpërmjet VKM nr. 364, datë 30.6.2025, "Për miratimin e listës së infrastrukturave kritike dhe të rëndësishme të informacionit", e ndryshuar me VKM nr. 688, datë 11.09.2026, "Për miratimin e listës së infrastrukturave kritike dhe të rëndësishme të informacionit". Për rrjedhojë, njësitë e vetëqeverisjes vendore të përfshira në listën aktuale kanë tashmë statusin e operatorëve dhe, si të tilla, u nënshtrohen kërkesave dhe masave të sigurisë kibernetike të parashikuara në ligjin nr. 25/2024, "Për sigurinë kibernetike".

14. Aktet nënligjore (neni 20 i projektligjit)
Neni 20 i projektligjit ngarkon drejtorin e përgjithshëm të Autoritetit me nxjerrjen e akteve nënligjore për simulimet (neni 13, shkronja "ll"), për regjistrimin e organeve të vlerësimit (neni 20, pika 7) dhe për vetëdeklarimet (nenet 20/1 dhe 20/2). Për arsyet e parashtruara në pikat 6, 8 dhe 9 më sipër, këto akte vlerësojmë se duhet të miratohen me vendim të Këshillit të Ministrave. Pika 1 e nenit 20 të projektligjit, që lidhet me listën sipas nenit 41, pika 4, duhet të hiqet ose të përshtatet me propozimin alternativ të pikës 11. Vërejmë gjithashtu se neni 20 i projektligjit ka dy pika të numërtuara "2", si rrjedhojë sugjerojmë të korrigjohet.

Përgjigje: Nuk është marrë në konsideratë. Përcaktimi i Drejtorit të Përgjithshëm të Autoritetit si organ kompetent për miratimin e akteve nënligjore të parashikuara në nenin 20 të projektligjit është në përputhje me natyrën dhe objektin e rregullimeve që do të përcaktohen prej tyre. Këto akte kanë karakter kryesisht teknik dhe procedural dhe synojnë të përcaktojnë mënyrën e zbatimit të detyrimeve të parashikuara shprehimisht në ligj, pa krijuar detyrime të reja për subjektet përtej kufijve të përcaktuar nga ligji.
Sa i përket akteve për simulimet, vetëdeklarimet dhe regjistrimin e organeve të vlerësimit të konformitetit, ligji përcakton objektin e rregullimit dhe kompetencën përkatëse, ndërsa akti i Drejtorit të Përgjithshëm përcakton elementet teknike dhe

procedurale të zbatimit. Kjo mënyrë rregullimi është e përshtatshme për fusha me natyrë teknike dhe dinamike, ku kërkesat dhe procedurat mund të kërkojnë përshtatje më të shpeshtë në funksion të zhvillimeve teknologjike dhe të praktikës së sigurisë kibernetike.

VII. Agjencia e Prokurimit Publik është shprehur me komente dhe sugjerime si vijon:

Agjencia e Prokurimit Publik (në vijim "APP") mori në shqyrtim projektligjin e ridërguar për mendim, së bashku me relacionin shoqërues të tij, nëpërmjet platformës e-akte, me objekt: "Për disa shtesa dhe ndryshime në ligjin nr. 25/2024 "Për sigurinë kibernetike".

Nga shqyrtimi i relacionit shoqërues, qëllimi i këtij projektligji është përmirësimi dhe plotësimi i kuadrit ligjor ekzistues në fushën e sigurisë kibernetike, me qëllim rritjen e nivelit të mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit, forcimin e kapaciteteve institucionale për reagimin ndaj incidenteve të sigurisë kibernetike.

Lidhur me sa kërkohet sqarojmë se, APP i ushtron detyrat e saj në bazë dhe për zbatim të Ligjit Nr. 162/2020 "Për prokurimin publik", të ndryshuar (në vijim "LPP"), si dhe akteve nënligjore të dala në zbatim të tij.

Sa i takon projektligjit të dërguar për mendim, konstatojmë se, në nenin 1, pika 3 e projektaktit parashikohet: "Pas pikës 58 shtohen pikat 59 dhe 60, me këtë përmbajtje:

"59. "Organi i blerjes së përqendruar për trajnimet në fushën e sigurisë kibernetike" është autoriteti publik, i cili organizon, kryen prokurimet e qendërzuara për trajnimet në fushën e sigurisë kibernetike, për operatorët e infrastrukturave të informacionit të administratës shtetërore, sipas përcaktimeve të këtij ligji dhe legjislacionit të posaçëm".

Gjithashtu, në nenin 2, pika 3 parashikohet se: "*Në nenin 9 bëhen ndryshimi dhe shtesat e mëposhtme:*

1. Pas shkronjës "j", shtohen shkronjat "k" , "l", dhe "ll" me këtë përmbajtje:

“k) organizon, kryen prokurimet e përqendruara për trajnimet në fushën e sigurisë kibernetike, me vlerë mbi kufirin monetar të prokurimeve me vlera të vogla për operatorët e infrastrukturave të informacionit të administratës shtetërore në përputhje me legjislacionin në fuqi të prokurimeve” të cilat jo më vonë se data 30 prill i dërgojnë kërkesë me shkrim pranë AKSK- së për nevojat e tyre për trajnime, sipas buxhetit të miratuar;”.

Nga shqyrtimi i relacionit shoqërues të projektaktit, konstatojmë se, nuk janë dhënë argumente ligjore sa i takon caktimit të AKSK si organ qendror blerës për kryerjen e prokurimeve për trajnimet në fushën e sigurisë kibernetike.

APP sqaron se, në shkronjat “h” dhe “i” të nenit 9, të Ligjit Nr. 25/2024 “Për sigurinë kibernetike” parashikohet se: *“Autoriteti, në përputhje me përcaktimet e bëra në këtë ligj, ushtron kompetencat e mëposhtme:*

h) kryen aktivitete ndërgjegjësimi në fushën e sigurisë kibernetike për të gjitha grupet e shoqërisë; i) Autoriteti, me urdhër të drejtorit të përgjithshëm dhe në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, zhvillon dhe nxit, sa herë vlerësohet e nevojshme, ***trajnime për personelin e këtyre operatorëve****, në kuadër të përmbushjes me efektivitet të lartë të detyrave”.*

Gjithashtu, në VKM Nr. 783, datë 18.12.2024 “Për organizimin dhe funksionimin e Autoritetit Kombëtar për Sigurinë Kibernetike”, parashikohet se, ndër përgjegjësitë e AKSK, është edhe organizimi i punës për edukimin dhe rritjen e ndërgjegjësimit në fushën e sigurisë kibernetike.

Referuar sa më sipër, AKSK ka si detyrë funksionale zhvillimin dhe nxitjen e trajnimeve, si dhe kryerjen e aktiviteteve të edukimit dhe ndërgjegjësimit në fushën e sigurisë kibernetike për operatorët përkatës. Në këtë kuptim, trajnimet në fushën e sigurisë kibernetike përbëjnë pjesë të funksioneve dhe përgjegjësive, që i janë ngarkuar vetë AKSK nga legjislacioni i posaçëm.

Ndërkohë, sa i takon parashikimeve të propozuara në nenet e sipërcituara të këtij projektakti, ku synohet që AKSK të ushtrojë funksionin e organit qendror blerës për kryerjen e prokurimeve të përqendruara për trajnimet në fushën e sigurisë kibernetike, për operatorët e infrastrukturave të informacionit të administratës

shtetërore, APP sjell në vëmendje qëllimin dhe funksionin e organit qendror blerës, sipas përcaktimeve në legjislacionin e prokurimit publik.

Konkretisht, sipas parashikimeve në nenin 53/2 të LPP, Këshilli i Ministrave mund të ngarkojë për procedura të veçanta prokurimi një autoritet ose ent tjetër kontraktor, si organ qendror blerës, që do të zhvillojë procedurën e prokurimit për objekte të caktuara.

Referuar parashikimeve në nenin 67/1 të VKM Nr. 285/2021 "Për miratimin e rregullave të prokurimit publik", të ndryshuar, prokurimi i përqendruar mund të përdoret kur blerja e përqendruar mundëson përfitime ekonomike për shkak të rritjes së sasisë së mallrave, punëve ose shërbimeve homogjene dhe që ofrohen në treg me kushte të ngjashme, si dhe kur autoriteti kontraktor, që luan rolin e organit qendror blerës, ka njohuri të mjaftueshme për zhvillimin e procedurave të prokurimit për mallrat, punët ose shërbimet, që do të prokurohen.

Në këtë kuptim, nisur nga fakti se, në relacion nuk jepen argumente ligjore, vlerësojmë së është i paqartë ngarkimi i AKSK, si organ qendror blerës në kuptim të parashikimeve ligjore të prokurimit publik.

Përsa më sipër, projektakti dhe relacioni shoqërues kanë nevojë të rishikohen, duke u plotësuar me argumentimin përkatës ligjor lidhur me këtë çështje.

Përgjigje: Parashikimi i pikës 3 të projektligjit, që synon ngarkimin e AKSK-së me funksionin e organit qendror blerës për prokurimin e përqendruar të trajnimeve të specializuara në fushën e sigurisë kibernetike, nuk bie ndesh me përcaktimet e ligjit nr. 25/2024 "Për sigurinë kibernetike", të ndryshuar, dhe as me legjislacionin në fuqi për prokurimin publik.

Në mbështetje të nenit 9, shkronjat "h" dhe "i", të ligjit nr. 25/2024, AKSK ka përgjegjësinë të zhvillojë aktivitete ndërgjegjësimi në fushën e sigurisë kibernetike, si dhe të zhvillojë dhe nxisë trajnime për personelin e operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit. Këto kompetenca, së bashku me përgjegjësitë e përcaktuara në VKM-në nr. 783, datë 18.12.2024, "Për organizimin dhe funksionimin e AKSK-së", përbëjnë bazën funksionale për identifikimin e nevojave dhe koordinimin e masave për ngritjen e kapaciteteve profesionale në këtë fushë.

Parashikimi i propozuar nuk synon që AKSK-ja të marrë përsipër zhvillimin e drejtpërdrejtë të të gjitha trajnimeve, por të organizojë dhe të kryejë procedurat e prokurimit të përqendruar për shërbime trajnimi të specializuara, të cilat do të ofrohen nga subjekte profesionale me ekspertizën, programet dhe certifikimet përkatëse. Këto shërbime synojnë të adresojnë nevoja konkrete për aftësi dhe njohuri teknike, të identifikuara në bazë të vlerësimit të kapaciteteve dhe të nevojave të operatorëve të infrastrukturave të informacionit të administratës shtetërore, si dhe të prioriteteve të sigurisë kibernetike në nivel sektorial dhe kombëtar.

Në këtë kuptim, duhet bërë dallimi ndërmjet kompetencës së AKSK-së për zhvillimin dhe nxitjen e trajnimeve, nga njëra anë, dhe mekanizmit të prokurimit të shërbimeve të specializuara të trajnimit, nga ana tjetër. Fakti që trajnimi përbën pjesë të përgjegjësive funksionale të AKSK-së nuk nënkupton se çdo trajnim duhet të zhvillohet drejtpërdrejt nga Autoriteti. Përkundrazi, për trajnimet që kërkojnë ekspertizë të posaçme teknike, programe të strukturuara profesionale dhe certifikime të njohura në fushën e sigurisë kibernetike, përzgjedhja e ofruesve të specializuar nëpërmjet procedurave të prokurimit publik përbën mekanizmin e përshtatshëm për realizimin e tyre.

Gjithashtu, parashikimi i propozuar nuk synon të zëvendësojë përgjegjësinë e operatorëve për ngritjen dhe përditësimin e vazhdueshëm të kapaciteteve të personelit të tyre, por të mundësojë adresimin e nevojave të përbashkëta dhe të boshllëqeve të identifikuara, për të cilat kërkohet një qasje e koordinuar në nivel qendror. Në këtë kuadër, prokurimi i përqendruar krijon mundësinë e unifikimit të kërkesave teknike dhe profesionale për trajnimet, të koordinimit të nevojave të operatorëve dhe të përdorimit më efikas të fondeve publike.

Sa i përket përputhshmërisë me legjislacionin e prokurimit publik, neni 53/2 i ligjit nr. 162/2020 “Për prokurimin publik”, të ndryshuar, parashikon mundësinë që Këshilli i Ministrave të ngarkojë, për procedura të veçanta prokurimi, një autoritet ose ent tjetër kontraktor si organ qendror blerës. Ndërkohë, neni 67/1 i VKM-së nr. 285, datë 19.05.2021, “Për miratimin e rregullave të prokurimit publik”, të ndryshuar, përcakton kushtet për përdorimin e prokurimit të përqendruar. Për këtë arsye, parashikimi i propozuar duhet të vlerësohet në funksion të specifikës së shërbimeve që do të prokurohen, mundësisë së agregimit të nevojave të operatorëve

dhe përfitimeve që mund të sigurohen nga zhvillimi i procedurave të përbashkëta, duke garantuar njëkohësisht respektimin e kërkesave të legjislacionit në fuqi.

Për sa më sipër, AKSK vlerëson se caktimi i AKSK-së si organ qendror blerës për prokurimin e përqendruar të trajnimeve të specializuara në fushën e sigurisë kibernetike mbështetet në natyrën e funksioneve të tij dhe në nevojën për një qasje të koordinuar për ngritjen e kapaciteteve profesionale. Për rrjedhojë, sugjerimi i APP-së për mosparashikimin e këtij funksioni për AKSK-në nuk pranohet.

VIII. Banka e Shqipërisë është shprehur me komente dhe sugjerime si vijon:

1. Neni 1 i projektit që ndryshon nenin 5, pika 5, të ligjit (CSIRT sektorial). Banka e Shqipërisë vlerëson se përcaktimi i institucionit përgjegjës për licencimin dhe mbikëqyrjen e bankave si CSIRT sektorial nuk përputhet me praktikën më të përhapur evropiane dhe nuk përbën kërkesë të detyrueshme të NIS2. Funksioni i CSIRT-it është në thelb operacional dhe teknik, ndërsa mandati i Bankës së Shqipërisë është rregullator, mbikëqyrës dhe makroprudencial. Për rrjedhojë, konsiderojmë më të përshtatshëm ruajtjen e një ndarjeje të qartë ndërmjet funksioneve operacionale të reagimit ndaj incidenteve dhe funksioneve mbikëqyrëse e koordinuese të autoriteteve sektoriale.

Propozim për riformulim: "CSIRT sektorial" është ekipi i përgjigjes ndaj incidenteve të sigurisë kibernetike për sektorin përkatës, i ngritur pranë ose i përcaktuar nga Autoriteti Kombëtar për Sigurinë Kibernetike, sipas fushës së përgjegjësisë dhe nevojave sektoriale. Autoritetet sektoriale kompetente bashkëpunojnë me CSIRT-in sektorial në funksion të shkëmbimit të informacionit, koordinimit institucional, mbikëqyrjes dhe menaxhimit të rrezikut kibernetik, sipas kompetencave të tyre ligjore. Bashkëpunimi ndërmjet Autoritetit Kombëtar për Sigurinë Kibernetike, CSIRT-eve dhe autoriteteve sektoriale kompetente realizohet nëpërmjet mekanizmave formalë të koordinimit, shkëmbimit të informacionit dhe procedurave të raportimit të incidenteve, në përputhje me kompetencat e secilit institucion.

Përgjigje: Pranuar pjesërisht dhe reflektuar.

2. Neni 3 i projektligjit, i cili ndryshon nenin 12 të ligjit.

Pika 4 – Sugjerojmë që detyrimi për dhënien e informacionit të lidhet shprehimisht me parimin e proporcionalitetit.

Propozim për riformulim: “Subjektet e identifikuara si infrastruktura kritike ose të rëndësishme të informacionit kanë detyrimin të raportojnë pranë Autoritetit informacionin e mëposhtëm, në mënyrë të saktë dhe të plotë, për aq sa ky informacion është i nevojshëm dhe proporcional për identifikimin, regjistrimin dhe ushtrimin e funksioneve mbikëqyrëse të Autoritetit sipas këtij ligji.”

Pika 5 – Sugjerojmë ruajtjen e karakterit konfidencial të listës ose përcaktimin e një regjimi të posaçëm administrimi për të.

Përgjigje: Pika 4 komenti nuk pranohet. Ligji nr. 25/2024 “Për sigurinë kibernetike”, në nenin 12, pika 4, ka përcaktuar në mënyrë shteruese informacionin që subjektet e identifikuara si infrastruktura kritike ose të rëndësishme të informacionit kanë detyrimin të raportojnë pranë Autoritetit, konkretisht emrin e subjektit, adresën, sektorin dhe nënsektorin përkatës, si dhe listën e shteteve ku ofrojnë shërbime, kur është e aplikueshme. Për rrjedhojë, detyrimi ligjor është i kufizuar në informacionin e përcaktuar shprehimisht nga ligjvënësi dhe nuk parashikon një kërkesë të pakufizuar për dhënien e të dhënave. Në këto kushte, shtimi i një përcaktimi të veçantë mbi proporcionalitetin nuk vlerësohet i nevojshëm.

Pika 5 komenti pranohet dhe është reflektua.

3. Neni 4 i projektligjit, i cili ndryshon nenin 13 të ligjit.

Pika g – Termi “vulnerabilitete të shfrytëzueshme” kërkon qartësim, pasi nuk përcaktohen kriteret mbi të cilat një vulnerabilitet konsiderohet i tillë.

Pika ll – Përveç njoftimit paraprak, konsiderojmë të nevojshme që ligji të përcaktojë kërkesat minimale lidhur me: përmbajtjen e njoftimit; afatin minimal të njoftimit; rastet e shtyrjes ose pezullimit të simulimit; përgjegjësinë për dëmet eventuale; trajtimin dhe ruajtjen e rezultateve të simulimit. Duke marrë parasysh ndikimin që simulimet mund të kenë në funksionimin e sistemeve dhe shërbimeve të operatorëve, konsiderojmë se kërkesat minimale procedurale dhe kushtet e ushtrimit të kësaj kompetence duhet të përcaktohen në nivel ligjor dhe jo të lihen tërësisht për rregullim me akt nënligjor.

Përgjigje: Pika “g” – Komenti nuk pranohet. Shtimi i termit “të shfrytëzueshme” synon të qartësojë se skanimet proaktive dhe veprimet e mëtejshme të CSIRT-it

Kombëtar lidhen me vulnerabilitete që mund të shfrytëzohen për realizimin e sulmeve kibernetike, duke mundësuar një vlerësim më të orientuar drejt rrezikut dhe identifikimin e pikave të dobëta që mund të cenojnë sigurinë e infrastrukturave kritike dhe të rëndësishme të informacionit. Vlerësimi i shfrytëzueshmërisë së një vulnerabiliteti lidhet me karakteristikat e tij teknike dhe kontekstin e sistemit ku është evidentuar, ndaj përcaktimi shterues i kritereve në ligj nuk vlerësohet i nevojshëm.

Pika "ll" – Komenti nuk pranohet. Projektligji parashikon që simulimet të kryhen duke shfrytëzuar vulnerabilitetet e evidentuara nëpërmjet skanimeve proaktive, si dhe përcakton detyrimin për njoftimin dhe dakordësimin paraprak me operatorët për fashat orare të kryerjes së tyre. Këto parashikime synojnë të sigurojnë koordinimin me operatorët dhe të marrin në konsideratë vijueshmërinë e funksionimit të sistemeve dhe shërbimeve gjatë realizimit të simulimeve. Gjithashtu, projektligji parashikon miratimin e procedurës së simulimit me urdhër të drejtorit të përgjithshëm të Autoritetit, duke mundësuar përcaktimin e kërkesave procedurale dhe teknike të nevojshme për zbatimin e kësaj kompetence. Për rrjedhojë, nuk vlerësohet e nevojshme që të gjitha elementet e propozuara të parashikohen në mënyrë të detajuar në ligj, pasi përmbajtja e njoftimit, procedurat e koordinimit dhe aspektet e tjera të zbatimit mund të rregullohen në procedurën përkatëse, në përputhje me natyrën teknike të simulimeve dhe nevojën për të garantuar sigurinë e sistemeve dhe rrjeteve të operatorëve.

4. Neni 5 i projektligjit, i cili ndryshon nenin 15 të ligjit.

Sugjerojmë që dispozita të riformulohet duke konsideruar komentin e paraqitur për nenin 5 të ligjit, që reflekton ndarjen ndërmjet funksioneve operacionale të CSIRT-it dhe rolin mbikëqyrës të autoriteteve sektoriale.

Propozim për riformulim: "CSIRT-et sektoriale ngrihen ose përcaktohen në përputhje me fushën përkatëse të veprimtarisë dhe nevojat sektoriale, në koordinim me Autoritetin Kombëtar për Sigurinë Kibernetike. Autoritetet sektoriale kompetente bashkëpunojnë me CSIRT-et sektoriale në funksion të shkëmbimit të informacionit, koordinimit institucional, mbikëqyrjes dhe menaxhimit të rrezikut kibernetik sipas kompetencave të tyre ligjore."

Përgjigje: Pranuar pjesërisht reflektuar.

5. Neni 6 i projektligjit, i cili riformulon nenin 16 të ligjit.

Përdorimi i termave "menjëherë" dhe "zgjidhje e shpejtë e incidentit" mund të krijojë paqartësi në interpretimin dhe zbatimin praktik të dispozitës, pasi nuk përcaktojnë kritere objektive ose afate të matshme. Për këtë arsye, sugjerojmë zëvendësimin e termit "menjëherë" me një formulim juridikisht më të qartë, si: "pa vonesë të pajustifikuar" ose "brenda afateve të përcaktuara në procedurat e raportimit të incidenteve". Ndërsa togfjalëshi "në rast të zgjidhjes së shpejtë të incidentit" mund të zëvendësohej me "pas përfundimit të trajtimit të incidentit".

Përgjigje: Komenti nuk pranohet. Përdorimi i termit "menjëherë" në lidhje me detyrimin e CSIRT-it sektorial për të njoftuar CSIRT-in Kombëtar synon të garantojë shkëmbimin në kohë të informacionit mbi incidentet e identifikuara, duke mundësuar koordinimin e menjëhershëm ndërmjet strukturave përgjegjëse, vlerësimin e situatës dhe marrjen e masave të nevojshme për kufizimin e përhapjes dhe parandalimin e pasojave të mëtejshme. Duke qenë se incidentet kibernetike ndryshojnë për nga natyra, shkalla dhe ndikimi i tyre, përcaktimi i një afati të përgjithshëm ose referimi te procedura të tjera nuk vlerësohet i nevojshëm, pasi mund të kufizojë reagimin në kohë ndaj incidenteve.

Gjithashtu, shprehja "në rast të zgjidhjes së shpejtë të incidentit" synon të sigurojë njoftimin e CSIRT-it Kombëtar edhe kur incidenti trajtohet dhe zgjidhet brenda një periudhe të shkurtër, me qëllim garantimin e një pasqyre të plotë të incidenteve të evidentuara në nivel sektorial dhe mundësimin e vlerësimit të tyre nga CSIRT-i Kombëtar, pavarësisht kohëzgjatjes ose zgjidhjes së shpejtë të tyre. Për rrjedhojë, vlerësohet e nevojshme ruajtja e formulimit të parashikuar në projektligj.

6. Neni 7 i projektligjit, i cili ndryshon nenin 17 të ligjit.

Shkronja "f" – Sugjerojmë të vlerësohet mundësia e harmonizimit të kësaj dispozite me qasjen e NIS2 (i cili fokusohet kryesisht në raportimin e incidenteve me ndikim të rëndësishëm), duke ruajtur një ekuilibër ndërmjet nevojës për raportim efektiv dhe barrës administrative për operatorët.

Shkronja "g" – Duke qenë se zbatimi i masave të propozuara mund të ketë ndikim në disponueshmërinë, performancën ose vijueshmërinë e shërbimeve të operatorëve,

konsiderojmë se dispozita duhet të marrë në konsideratë edhe realizueshmërinë teknike dhe vlerësimin e ndikimit operacional. Për këtë arsye, sugjerojmë që detyrimi për zbatimin e IOC-ve, IOA-ve dhe masave të tjera të komunikuara nga Autoriteti të kushtëzohet me: vlerësimin e ndikimit operacional; mundësinë e aplikimit të masave alternative të mitigimit të rrezikut.

Propozim për riformulim: "Operatorët zbatojnë, në masën që është teknikisht e realizueshme dhe proporcionalisht e justifikuar, masat për bllokimin, filtrimin, kufizimin, detektimin ose neutralizimin e treguesve të kompromet imit (IOC), treguesve të sulmeve dhe vulnerabiliteteve të komunikuara nga Autoriteti. Në rast pamundësie objektive për zbatimin e tyre, operatori dokumenton arsyet dhe merr masa alternative për mitigimin e rrezikut."

Përgjigje: Shkronja "f" – Komenti nuk pranohet. Dispozita synon të garantojë raportimin efektiv të informacionit të nevojshëm për identifikimin dhe trajtimin e kërcënimeve kibernetike, në funksion të reagimit në kohë dhe mbrojtjes së infrastrukturave kritike dhe të rëndësishme të informacionit. Harmonizimi me qasjen e NIS2 nuk nënkupton domosdoshmërisht kufizimin e raportimit vetëm te incidentet me ndikim të rëndësishëm, pasi shkëmbimi i informacionit për treguesit e kompromet imit, sulmet dhe vulnerabilitetet mundëson identifikimin dhe parandalimin në kohë të kërcënimeve, përpara se ato të shkaktojnë pasoja të konsiderueshme. Për rrjedhojë, ruajtja e detyrimit të parashikuar në dispozitë është e nevojshme për përmbushjen efektive të funksioneve të Autoritetit dhe forcimin e sigurisë kibernetike.

Shkronja "g" – Komenti nuk pranohet. Projektligji i adreson çështjet e ngritura në koment lidhur me realizueshmërinë teknike të zbatimit të masave, duke parashikuar forma të ndryshme ndërhyrjeje, si bllokimi, filtrimi, kufizimi, detektimi ose neutralizimi i treguesve të kompromet imit (IOC), treguesve të sulmeve dhe vulnerabiliteteve të komunikuara nga Autoriteti. Këto masa ofrojnë mundësi për zgjedhjen e ndërhyrjes së përshtatshme, në varësi të natyrës së kërcënimit, karakteristikave të sistemeve dhe kushteve teknike të zbatimit. Për rrjedhojë, dispozita krijon hapësirën e nevojshme për përshtatjen e masave me situatën konkrete, pa cenuar efektivitetin e detyrimit për marrjen e masave mbrojtëse dhe parandalimin e pasojave të mundshme të kërcënimeve kibernetike.

7. Neni 9 i projektligjit, i cili shton nenet 20/1 dhe 20/2 të ligjit.

Në parim, mbështesim futjen e mekanizmave të vetëdeklarimit. Duke qenë se këto dispozita krijojnë për herë të parë një mekanizëm sistematik mbledhjeje të informacionit mbi nivelin e përputhshmërisë dhe organizimin e infrastrukturave teknologjike të operatorëve, konsiderojmë të nevojshme vendosjen e kërkesave të qarta ligjore mbi administrimin dhe mbrojtjen e këtij informacioni. Prandaj, sugjerojmë që ligji duhet të përcaktojë: kategoritë bazë të informacionit që mund të kërkohet; kufijtë materialë të vetëdeklarimit; kërkesat për informacionin sensitiv (përdorimin e informacionit, kufizimet e aksesit, ruajtjen e informacionit, shkëmbimin dhe gjurmueshmërinë e tij); detyrimet për përditësim; afatet e ruajtjes së informacionit.

Ndërsa aktet nënligjore, siç e kemi përmendur edhe në paragrafin 1.2, duhet të kufizohen në aspektet procedurale dhe teknike të zbatimit, si p.sh.: modelin e formularëve; procedurat e paraqitjes; aspektet teknike të administrimit të procesit.

Përgjigje: Komenti nuk pranohet. Dispozitat e propozuara synojnë të krijojnë një mekanizëm vetëdeklarimi që i mundëson Autoritetit mbledhjen e informacionit të nevojshëm për identifikimin e infrastrukturave teknologjike të operatorëve dhe vlerësimin e nivelit të përmbushjes së kërkesave të sigurisë kibernetike. Përcaktimi i elementeve konkrete të informacionit që kërkohet, formati i deklarimit dhe mënyra e administrimit të tij lidhen me natyrën dhe specifikat teknike të sistemeve dhe rrjeteve të operatorëve, të cilat mund të ndryshojnë në varësi të sektorit dhe zhvillimeve teknologjike. Për këtë arsye, rregullimi i këtyre elementeve përmes akteve nënligjore vlerësohet i përshtatshëm, pasi mundëson fleksibilitetin e nevojshëm për zbatimin efektiv të mekanizmit dhe përshtatjen e tij me nevojat konkrete. Njëkohësisht, kërkesa për ruajtjen e konfidencialitetit të informacionit të siguruar gjen pasqyrim në nenin 11 të projektligjit, i cili parashikon që në shkronjën "dh" të pikës 2 të nenit 30 të ligjit, pas fjalës "mbrojtjen", të shtohen fjalët "dhe konfidencialitetin". Për rrjedhojë, vlerësohet se çështja e ruajtjes së konfidencialitetit të informacionit është adresuar në projektligj dhe nuk është e nevojshme të përsëritet në mënyrë të posaçme në nenet 20/1 dhe 20/2.

8. Neni 13 i projektligjit, sipas të cilit shtohet neni 33/1 në ligj.

Grupi Ndërinstitucional i Inteligjencës Kibernetike përpunon potencialisht informacion me nivel të lartë sensitiviteti. Për këtë arsye, në vijim të komenteve të

paraqitura për nenet 20/1 dhe 20/2 mbi administrimin e informacionit sensitiv, sugjerojmë që këto kërkesa të shtrihen edhe ndaj Grupit Ndërinstitucional të Inteligjencës Kibernetike.

Përgjigje: Komenti nuk pranohet. Grupi i Bashkëpunimit për Inteligjencën Kibernetike ka si qëllim shkëmbimin e informacionit paralajmërues për evidentimin e kërcënimeve potenciale kibernetike dhe vlerësimin e ndikimit të tyre të mundshëm, në kuadër të bashkëpunimit ndërinstitucional. Duke qenë se pika 3 e nenit 33/1 të propozuar parashikon që rregullat e organizimit dhe funksionimit të Grupit, procedurat e shkëmbimit të informacionit dhe mënyra e koordinimit ndërinstitucional të miratohen me urdhër të Kryeministrit, vlerësohet se këto çështje mund të trajtohen në kuadër të këtij akti, duke marrë në konsideratë natyrën e informacionit që shkëmbehet dhe kërkesat përkatëse për ruajtjen e konfidencialitetit të tij. Për rrjedhojë, nuk vlerësohet e nevojshme që këto kërkesa të detajohen në mënyrë të posaçme në vetë dispozitën ligjore.

IX. **Shkolla Shqiptare e Administratës Publike** është shprehur me komente dhe sugjerime si vijon:

Lidhur me pikën 59 të nenit 5 të projektligjit, e cila parashikon shtimin e përkufizimit të "Organit të blerjes së përqendruar për trajnimet në fushën e sigurisë kibernetike", sugjerojme që në dispozitën përkatëse të specifikohet qartë natyra dhe lloji i trajnimeve që d9o të zhvillohen në kuadër të kësaj kompetence.

Ky saktësim vlerësohet i nevojshëm për të garantuar qartësi në zbatimin e dispozitës dhe për të shmangur mbivendosje të mundëshme me fushat e përgjegjësisë së Shkollës Shqiptare të Administratës Publike (ASPA), e cila ushtron funksione në fushën e zhvillimit profesional dhe ngritjes se kapaciteteve të administratës publike. Në këtë kuadër, vlerësojmë së dispozita duhet të përcaktojë qartë se kjo kompetencë kufizohet në trajnime spacifike në fushën e sigurisë kibernetike, te cilat nuk ofrohen nga institucione të spacializuara në vend.

Përgjigje: Pranuar reflektuar.

X. **Ministria e Infrastrukturës dhe Energjisë** është shprehur me komente dhe sugjerime si vijon:

1. Në nenin 1 të projektligjit, lidhur me përkufizimin e “CSIRT sektorial”, sugjerojmë që përkufizimi dhe roli i CSIRT-ve sektoriale të qartësohen në përputhje me nenin 10 të Direktivës NIS2, duke shmangur mbivendosjen me CSIRT-et ekzistuese. Në këtë kuadër, sugjerojmë që të rishikohen në mënyrë konsistente edhe dispozitat e lidhura në nenet 5 dhe 6 të projektligjit, që kanë të bëjnë me pikën 1 të nenit 15 dhe shkronjën “dh)” të nenit 16 të ligjit.

Përgjigje: Komenti nuk pranohet. Rikonceptimi i CSIRT-eve sektoriale në projektligj vlerësohet se është në përputhje me parashikimet e nenit 10 të Direktivës (BE) 2022/2555 (NIS2), pasi synon organizimin e kapaciteteve të reagimit ndaj incidenteve të sigurisë kibernetike në nivel sektorial, në përputhje me specifikat dhe përgjegjësitë e sektorëve përkatës.

Përkufizimi i propozuar përcakton se CSIRT-i sektorial është ekipi i përgjigjes ndaj incidenteve të sigurisë kibernetike për sektorin përkatës, i ngritur nga Autoriteti Kombëtar për Sigurinë Kibernetike ose operatori qeveritar që menaxhon infrastrukturat qeveritare, sipas përcaktimeve të anekseve të ligjit. Ky organizim synon të sigurojë mbulimin sektorial dhe forcimin e kapaciteteve të reagimit ndaj incidenteve, duke marrë parasysh përgjegjësitë institucionale përkatëse.

Gjithashtu, nuk krijohet mbivendosje kompetencash as me CSIRT-in Kombëtar dhe as me CSIRT-et pranë operatorëve, pasi funksionet dhe përgjegjësitë e këtyre strukturave përcaktohen nga ligji nr. 25/2024, “Për sigurinë kibernetike”. CSIRT-i Kombëtar ushtron funksionet e koordinimit në nivel kombëtar, ndërsa CSIRT-et sektoriale mbulojnë reagimin ndaj incidenteve në nivel sektorial dhe CSIRT-et pranë operatorëve veprojnë në nivelin e sistemeve dhe rrjeteve të operatorëve përkatës. Këto struktura kanë role plotësuese dhe bashkëpunojnë ndërmjet tyre, në përputhje me detyrat dhe përgjegjësitë e përcaktuara në ligj.

Për rrjedhojë, rikonceptimi i propozuar synon të qartësojë organizimin dhe mbulimin sektorial të CSIRT-eve, pa cenuar kompetencat e CSIRT-it Kombëtar dhe të strukturave ekzistuese, si dhe pa krijuar mbivendosje funksionale ndërmjet tyre.

2. Në nenin 1 të projektligjit, në formulimin e nenit 5, sugjerojmë të shtohet edhe ministri përgjegjës për komunikimet elektronike, për sa i përket propozimit të akteve nënligjore që lidhen me këtë fushë.

Përgjigje: Komenti nuk pranohet. VKM-ja nr. 508, datë 25.09.2025, "Për përcaktimin e fushës së përgjegjësisë shtetërore të Ministrisë së Infrastrukturës dhe Energjisë", përcakton fushën e përgjegjësisë shtetërore të Ministrisë së Infrastrukturës dhe Energjisë, e cila përfshin, ndër të tjera, komunikimet elektronike dhe digjitalizimin. Megjithatë, këto fusha nuk lidhen automatikisht me sigurinë kibernetike, e cila përbën një fushë të veçantë, me specifika dhe kuadër rregullator të posaçëm. Për rrjedhojë, përfshirja e komunikimeve elektronike dhe digjitalizimit në fushën e përgjegjësisë së ministrisë nuk përbën, në vetvete, bazë për t'i atribuar asaj kompetencën për propozimin e akteve nënligjore që rregullojnë sigurinë kibernetike.

3. Lidhur me pikën 3 të nenit 1 dhe shtimin e shkronjës "k" në pikën 3 të nenit 2 të projektligjit, sugjerojmë që dispozitat për prokurimin e përqendruar të trajnimeve të koordinohen me institucionet përgjegjëse për prokurimin publik dhe financat publike.

Përgjigje: Komenti nuk pranohet. Parashikimi i prokurimit të përqendruar të trajnimeve në fushën e sigurisë kibernetike synon të sigurojë koordinimin e nevojave dhe zhvillimin e kapaciteteve të specializuara në këtë fushë, në përputhje me kompetencat e AKSK-së sipas ligjit nr. 25/2024. Ky parashikim nuk përjashton zbatimin e legjislacionit në fuqi për prokurimin publik dhe financat publike, të cilat mbeten të detyrueshme për procedurat përkatëse. Për rrjedhojë, nuk vlerësohet e nevojshme të shtohet një parashikim i veçantë për koordinimin me institucionet përgjegjëse, pasi zbatimi i kuadrit ligjor përkatës garantohet nga vetë legjislacioni në fuqi.

4. Lidhur me propozimin në pikën 3 të nenit 2 të projektligjit, për shtimin e shkronjës "ll", që lidhet me rolin e AKSK-së si autorizues për organet e vlerësimit të konformitetit sipas skemës kombëtare të certifikimit, vlerësojmë se formulimi ka nevojë për qartësime dhe plotësime, duke marrë në konsideratë praktikën e Bashkimit Evropian në fushën e certifikimit të sigurisë kibernetike. Në formulimin e propozuar nuk përcaktohet instrumenti përmes të cilit do të specifikohen kategoritë e produkteve TIK, si dhe profilet e mbrojtjes në të cilat shtrihet autorizimi. Duke marrë në konsideratë faktin se skemat e certifikimit në këtë fushë kanë elemente të bazuara në vullnetaritet, shtrirjen gjithnjë e më të gjerë të produkteve TIK, si dhe proceset në vijim të rishikimit të kuadrit rregullator të BE-së për këtë çështje, sugjerojmë që specifikimi i kategorive të produkteve TIK dhe i profileve të mbrojtjes të përcaktohet me vendim të Këshillit të Ministrave, me propozim të ministrit

përgjegjës për komunikimet elektronike, në bashkërendim me institucionet përgjegjëse për fushën digjitale dhe në konsultim me AKSHI-n dhe autoritetet e tjera rregullatore të lidhura me këtë fushë.

Përgjigje: Komenti nuk pranohet. Çështjet e ngritura në koment lidhur me specifikimin e kategorive të produkteve TIK dhe profileve të mbrojtjes janë tashmë të parashikuara në VKM nr. 813, datë 30.12.2025, "Për miratimin e Skemës Kombëtare të Certifikimit të Sigurisë Kibernetike, si dhe të niveleve të sigurisë së skemës", e cila përcakton kuadrin e zbatimit të skemës kombëtare të certifikimit dhe nivelet e sigurisë.
Për rrjedhojë, dispozita e propozuar synon të përcaktojë kompetencën e AKSK-së për autorizimin e organeve të vlerësimit të konformitetit, ndërsa specifikimet teknike dhe kategoritë përkatëse rregullohen në kuadrin e skemës kombëtare të miratuar me VKM nr. 813/2025. Për këtë arsye, nuk vlerësohet e nevojshme ndërhyrja e propozuar.

5. Në pikën 2 të nenit 4 të projektligjit, në vijim të ndryshimeve të propozuara për shkronjën "ll", sugjerojmë që të shtohet një përcaktim i qartë se simulimet e parashikuara nuk duhet të cenojnë funksionimin normal të sistemeve dhe/ose ofrimin e shërbimeve nëpërmjet tyre. Në fjalinë e fundit, ku parashikohet procedura e simulimit e miratuar me urdhër të drejtorit të Përgjithshëm, sugjerojmë të shtohet përcaktimi: "pas konsultimit me autoritetet e tjera kompetente të lidhura me sektorët dhe/ose infrastrukturat kritike", sipas përcaktimeve të nenit 11 të ligjit.

Përgjigje: Komenti nuk pranohet. Dispozita e propozuar e ka adresuar tashmë çështjen e ngritur në koment, pasi parashikon shprehimisht që simulimet kryhen *"duke njoftuar dhe dakordësuar paraprakisht me operatorët për fashat orare të kryerjes së simulimeve"*. Ky parashikim garanton koordinimin paraprak me operatorët dhe marrjen në konsideratë të funksionimit të sistemeve gjatë përcaktimit të kohës së simulimeve.
Për sa i përket konsultimit me autoritetet e tjera, kjo nuk vlerësohet e nevojshme të përcaktohet si kusht procedural në dispozitë, pasi bashkëpunimi ndërinstitucional realizohet sipas kompetencave dhe kuadrit ligjor në fuqi.

6. Referuar propozimit për riformulimin e shkronjës "ë" të nenit 17 të ligjit, sugjerojmë që të vlerësohet nevoja për raportim në dy drejtime dhe të shmanget, sa

është e mundur, mbivendosja e procedurave të raportimit, me qëllim që të mos rëndohen operatorët e infrastrukturave kritike, përfshirë ata në sektorët e energjisë dhe të transportit.

Përgjigje: Komenti nuk pranohet. Përcaktimi që CSIRT-i pranë operatorëve të raportojë si pranë CSIRT-it Kombëtar, ashtu edhe pranë CSIRT-it sektorial, është i nevojshëm për të garantuar informimin e strukturave përgjegjëse dhe koordinimin efektiv të reagimit ndaj incidenteve. Shtimi i detyrimit për bashkëpunim, shkëmbim informacioni, koordinim të veprimeve dhe zbatim të masave të nevojshme synon të qartësojë mënyrën e bashkëveprimit ndërmjet këtyre strukturave dhe të forcojë procesin e parandalimit, reagimit dhe rikuperimit.
Për rrjedhojë, formulimi i propozuar nuk krijon një raportim të panevojshëm, por përcakton qartë përgjegjësitë dhe mekanizmat e koordinimit ndërmjet CSIRT-it pranë operatorit, CSIRT-it Kombëtar dhe CSIRT-it sektorial.

7. Në nenin 7 të projektligjit, lidhur me shkronjat "g" dhe "gj" që propozohet të shtohen, në veçanti për shkronjën "g", sugjerojmë që të formulohet duke u harmonizuar me parashikimet e nenit 9 të rregullores DSA, të parashikuara në projektligjin për shërbimet digjitale, për aq sa është e zbatueshme.

Përgjigje: Komenti nuk pranohet. Parashikimet e shkronjave "g" dhe "gj" lidhen drejtpërdrejt me masat teknike dhe operative për mbrojtjen e rrjeteve dhe sistemeve nga kërcënimet dhe incidentet e sigurisë kibernetike, në kuadër të kompetencave të parashikuara nga legjislacioni për sigurinë kibernetike.
Përmbajtja e këtyre dispozitave nuk lidhet me parashikimin e nenit 9 të Rregullores së DSA-së, pasi ky i fundit rregullon një çështje me objekt dhe qëllim të ndryshëm. Për rrjedhojë, nuk vlerësohet e nevojshme harmonizimi i shkronjave "g" dhe "gj" me këtë dispozitë të DSA-së.

8. Në pikën 2 të nenit 8 të projektligjit, për formulimin e pikës 7, si dhe në pikën 2 të nenit 16 të projektligjit, për propozimin e pikës 3 të nenit 42, sugjerojmë që formulimet të konsultohen me institucionin përgjegjës për vlerësimin e konformitetit dhe akreditimin, me qëllim zbatimin e harmonizuar të legjislacionit në fuqi për këtë proces.

Përgjigje: Komenti nuk pranohet. Dispozitat e propozuara rregullojnë tarifat e regjistrimit dhe autorizimit, si dhe procedurat dhe kriteret për regjistrimin e organeve

të vlerësimit të konformitetit në fushën e sigurisë kibernetike. Ato nuk ndërhyjnë në procedurat e akreditimit dhe vlerësimit të konformitetit, të cilat vijojnë të rregullohen nga legjislacioni përkatës. Për rrjedhojë, nuk vlerësohet e nevojshme rishikimi i formulimeve të propozuara, pasi ato synojnë të përcaktojnë kërkesat që lidhen me ushtrimin e kompetencave të AKSK-së në fushën e sigurisë kibernetike, pa cenuar kompetencat e institucioneve përgjegjëse për akreditimin. Megjithatë ky projektligj është bashkërenduar me ministrinë përgjegjëse.

9. Në nenin 9 të projektligjit, lidhur me propozimin për shtimin e neneve 20/1 dhe 20/2, për vetëdeklarimin e masave të sigurisë kibernetike dhe vetëdeklarimin e hostimit, vërejmë se këto rregullime nuk parashikohen shprehimisht në Direktivën NIS2. Nëse vlerësohet se kjo masë është e nevojshme, sugjerojmë që dispozitat të plotësohen për të qartësuar kur lind detyrimi dhe cili është afati për paraqitjen e vetëdeklarimit, si për operatorët e infrastrukturave kritike, ashtu edhe për vetëdeklarimin e hostimit, me qëllim sigurinë juridike të operatorëve që i nënshtrohen ligjit.

Përgjigje: Komenti nuk pranohet. Parashikimet për vetëdeklarimin janë masa që synojnë të lehtësojnë monitorimin dhe mbikëqyrjen e zbatimit të masave të sigurisë kibernetike nga operatorët dhe nuk bien ndesh me NIS2. Fakti që këto rregullime nuk parashikohen shprehimisht në NIS2 nuk pengon përcaktimin e tyre në legjislacionin kombëtar.
Gjithashtu, dispozitat e propozuara përcaktojnë tashmë kuadrin e nevojshëm procedural. Në mënyrë të veçantë, neni 20/1, pika 3 parashikon që forma, përmbajtja, mënyra e paraqitjes, afatet dhe procedurat e administrimit të vetëdeklarimit përcaktohen me urdhër të drejtorit të Përgjithshëm të Autoritetit. E njëjta qasje parashikohet edhe në nenin 20/2 për vetëdeklarimin e hostimit dhe administrimit të sistemeve, rrjeteve dhe infrastrukturës së informacionit

10. Në nenin 13 të projektligjit, sugjerojmë që të shtohet një pikë ku të parashikohet që Autoriteti bashkëpunon dhe nënshkruan memorandum bashkëpunimi me autoritetet kompetente, në veçanti me AKEP-in, si dhe me autoritete të tjera sipas rastit, për zbatimin e harmonizuar të legjislacionit për sigurinë e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike. Kjo do të shmangte mbivendosjen dhe ngarkesën e sektorit privat me kërkesa të dubluara për masat e sigurisë për subjektet që i nënshtrohen njëkohësisht ligjit nr. 54/2024 dhe ligjit nr. 25/2024, si dhe do të ishte në frymën e rregullimit të harmonizuar dhe të qasjes “omnibus” që BE-ja ka

ndërmarrë në fushën e rregullimit digjital. Ky propozim mban parasysh edhe bashkëpunimin MIE–AKEP–AKSK në kuadër të projektit IPA 2022 për sigurinë e rrjeteve 5G.

Përgjigje: Komenti nuk pranohet. Ligji nr. 25/2024 "Për sigurinë kibernetike" e ka rregulluar shprehimisht bashkëpunimin ndërinstitucional, duke parashikuar në nenin 33, pika 1, se AKSK-ja koordinon veprimtarinë e saj me institucionet e sigurisë dhe të mbrojtjes, si dhe bashkëpunon me subjektet e tjera përgjegjëse për sigurinë kibernetike. Për rrjedhojë, nuk vlerësohet e nevojshme të shtohet një dispozitë e veçantë që parashikon nënshkrimin e memorandumeve të bashkëpunimit me AKEP-in apo autoritete të tjera, pasi bashkëpunimi ndërinstitucional është tashmë i parashikuar në ligj dhe mund të realizohet në funksion të nevojave konkrete.

Gjithashtu, përcaktimi i AKSK-së si autoritet përgjegjës për zbatimin dhe mbikëqyrjen e legjislacionit për sigurinë kibernetike nuk mund të kushtëzohet nga koordinimi paraprak me një autoritet tjetër. Bashkëpunimi ndërmjet institucioneve synon harmonizimin e veprimtarisë dhe shmangien e mbivendosjeve, por nuk mund të kufizojë ushtrimin e kompetencave që ligji nr. 25/2024 i njeh drejtpërdrejt AKSK-së.

Direktiva NIS 2 e ka përfshirë sigurinë e rrjeteve publike të komunikimeve elektronike dhe të shërbimeve të komunikimeve elektronike në kuadrin e posaçëm të sigurisë kibernetike, duke përcaktuar detyrimet për masat teknike, operacionale dhe organizative të sigurisë, si dhe mbikëqyrjen e tyre nga autoritetet kompetente për sigurinë kibernetike. neni 43 i NIS 2 shfuqizoi nenet 40 dhe 41 të Direktivës (BE) 2018/1972, që rregullonin më parë sigurinë e rrjeteve dhe shërbimeve të komunikimeve elektronike, me efekt nga data 18 tetor 2024.

11. Në pikën 2 të nenit 15 të projektligjit, sugjerojmë që propozimi për VKM të bëhet nga ministri përgjegjës për komunikimet elektronike, mbi bazën e sugjerimeve të Autoritetit dhe pas konsultimit me autoritetet e lidhura, sipas përcaktimeve të nenit 11 të ligjit.

Përgjigje: Komenti nuk pranohet. VKM-ja nr. 508, datë 25.09.2025, "Për përcaktimin e fushës së përgjegjësisë shtetërore të Ministrisë së Infrastrukturës dhe Energjisë", përfshin ndër të tjera komunikimet elektronike dhe digjitalizimin në fushën e përgjegjësisë së kësaj ministrie. Megjithatë, këto fusha nuk lidhen automatikisht me sigurinë kibernetike, e cila përbën një fushë të veçantë, me specifika dhe kuadër rregullator të posaçëm.

12. Në nenin 17 të projektligjit, lidhur me propozimin për ndryshimet në nenin 44, mendojmë se ky nen duhet riparë pas rishikimit të neneve përkatëse të cilave u referohet, në veçanti të neneve 20/1 dhe 20/2, sipas sugjerimit në pikën 9 më sipër.

Përgjigje: Komenti nuk pranohet. Duke qenë se nenet 20/1 dhe 20/2 të projektligjit nuk do të ndryshohen, nuk lind nevoja për rishikimin e nenit 44 të ligjit nr. 25/2024, i cili mbetet i pandryshuar.

13. Gjithashtu, sugjerojmë parashikimin e një periudhe transitore për zbatimin e rregullimeve të reja dhe të detyrimeve që shtohen për operatorët e infrastrukturave kritike, përfshirë ata në sektorët e energjisë dhe të transportit, me qëllim që t'u jepet kohë e mjaftueshme për zbatim.

Përgjigje: Komenti nuk pranohet. Detyrimet e parashikuara në projektligj për operatorët e infrastrukturave kritike të informacionit janë kryesisht të natyrës së zbatimit të menjëhershëm ose periodik dhe nuk sjellin një ngarkesë të tillë për operatorët që të justifikojnë parashikimin e një periudhe të përgjithshme transitore. Përjashtim bën detyrimi për përdorimin e produkteve, shërbimeve dhe proceseve TIK të certifikuara të sigurisë kibernetike, për zbatimin e të cilit mund të nevojitet një periudhë transitore, përfshirë rastet kur kërkohet certifikimi i produkteve ekzistuese. Periudha dhe kushtet për zbatimin e këtij detyrimi do të përcaktohen me vendim të Këshillit të Ministrave, duke mundësuar një zbatim të përshtatshëm dhe të koordinuar të kërkesave përkatëse.

IX. RAPORTI I VLERËSIMIT TË TË ARDHURAVE DHE SHPENZIMEVE BUXHETORE

Projektligji nuk parashikon krijimin e institucioneve të reja me personalitet juridik, por përmirëson kuadrin ligjor për organizimin dhe funksionimin e strukturave ekzistuese në fushën e sigurisë kibernetike, si dhe zgjeron kompetencat e Autoritetit Kombëtar për Sigurinë Kibernetike në përputhje me zhvillimet e kuadrit evropian dhe nevojat e sigurisë kombëtare.

Efektet financiare të projektligjit lidhen kryesisht me zbatimin e dispozitave që kërkojnë:

- organizimin dhe funksionimin e CSIRT-eve sektoriale nga institucionet përgjegjëse;

- administrimin e proceseve të vetëdeklarimit të masave të sigurisë kibernetike dhe të vetëdeklarimit të hostimit dhe administrimit të sistemeve të informacionit;
- ushtrimin e funksioneve të Autoritetit si organ kombëtar i certifikimit të sigurisë kibernetike dhe autorizimin e organeve të vlerësimit të konformitetit;
- organizimin dhe koordinimin e Grupit të Bashkëpunimit për Inteligjencën Kibernetike;
- organizimin e procedurave të prokurimeve të përqendruara për trajnimet në fushën e sigurisë kibernetike për operatorët e infrastrukturave të informacionit të administratës shtetërore.

Nga analiza e dispozitave të projektligjit rezulton se pjesa më e madhe e detyrimeve të reja do të realizohen nga strukturat ekzistuese të institucioneve përgjegjëse dhe nuk kërkojnë krijimin e institucioneve të reja apo shtimin e menjëhershëm të strukturave organizative.

Efektet financiare lidhen kryesisht me funksionimin e CSIRT-eve sektoriale, të cilat, sipas parashikimeve të projektligjit, ngrihen pranë Autoritetit Kombëtar për Sigurinë Kibernetike dhe operatorit qeveritar që menaxhon infrastrukturat qeveritare. Përllogaritja e kostove është bazuar në strukturën minimale të nevojshme të personelit për këto njësi, duke përfshirë fondin e pagave dhe kontributet për sigurimet shoqërore dhe shëndetësore.

Efekti financiar vjetor i përllogaritur për funksionimin e këtyre strukturave është **111,123,252.43 lekë**, sipas analizës financiare të kryer.

Për dispozitat e tjera të projektligjit, zbatimi i tyre nuk sjell efekte financiare shtesë të drejtpërdrejta për buxhetin e shtetit, pasi ato lidhen me riorganizimin e procedurave administrative, zgjerimin e kompetencave të institucioneve ekzistuese dhe miratimin e akteve nënligjore përkatëse.

Efektet financiare do të përballohen në përputhje me legjislacionin për menaxhimin e sistemit buxhetor dhe planifikimin buxhetor afatmesëm, nëpërmjet fondeve të miratuara për institucionet përgjegjëse ose fondeve që do të planifikohen sipas procedurave të zakonshme buxhetore.

PROPOZUESI

K R Y E M I N I S T R I

EDI RAMA