**Raporti individual i konsultimit publik**

1. **Titulli i projekt aktit**

Projektligji “Për sigurinë kibernetike”.

1. **Kohëzgjatja e konsultimeve**

*Specifikoni kohëzgjatjen e përgjithshme të konsultimeve publike sa i përket ditëve të punës, përfshirë datën e hapjes dhe mbylljes së konsultimeve publike; nëse kohëzgjatja ishte më e shkurtër se 20 ditë pune e paraparë me ligj, jepni arsye për shkurtimin e kohëzgjatjes.*

Kohëzgjatja e konsultimit publik për këtë akt ishte 20 ditë pune nga data e shpalljes së njoftimit në Regjistrin Elektronik për Njoftimet dhe Konsultimet Publike, bazuar në ligjin 146/2014 “Për njoftimin dhe konsultimin publik.

Publikimi u bë në datë 26.4.2023 dhe nëpërmjet një njoftimi të publikuar online në RENJK, të gjitha palët e interesuara: 1) organet publike; 2) shtetasit e Republikës së Shqipërisë dhe grupet e interesit; 3) personat fizikë të huaj me vendqëndrim të përhershëm në Republikën e Shqipërisë, si dhe personat juridikë të huaj, të regjistruar në Republikën e Shqipërisë) ishin të ftuar për të paraqitur komentet dhe rekomandimet e tyre për projektaktin, në adresën e koordinatorit për njoftimin dhe konsultimin publik: [merita.bundo@kryeministria.al](mailto:merita.bundo@kryeministria.al).

Data e mbylljes së procesit të konsultimit ishte 24.5.2023.

Projektligji “Për sigurinë kibernetike”, relacioni përkatës si dhe njoftimi për pjesëmarrje në takimet konsultative, në datat 9, 10, 11 Maj u publikuan në linkun, [www.konsultimipublik.gov.al](http://www.konsultimipublik.gov.al).

1. **Metoda e konsultimit**

*Listoni të gjitha metodat e konsultimit të përdorura, të tilla si konsultimet elektronike (Regjistri Elektronik, posta elektronike, faqet e internetit, etj.), Takimet publike, seancat e organeve këshilluese…, dhe siguroni informacione për afatin kohor, kohëzgjatjen dhe afatet e tyre. Shpjegoni se si u shpërnda informacioni mbi konsultimet e hapura, si u ftuan palët e interesuara të kontribuojnë. Përfshini gjithashtu aktivitete nga konsultimet paraprake nëse janë organizuar të tilla).*

Projektligji, në zbatim të ligjit 146/2014, i është nënshtruar procesit të konsultimit publik, në portalin “Regjistri elektronik për Njoftimet dhe Konsultimet Publike”, nga data 26.4.2023 deri në datën 24.5.2023.

Paralelisht, Auoriteti ka zhvilluar edhe takime konsultative më datat 9, 10 dhe 11 Maj, njoftim i publikuar edhe në RENJKP, ku u ftuan të gjithë grupet e interesit të marrnin pjesë në këto takime.

Gjithashtu u njoftuan me shkresë dhe email infrastrukturat kritike dhe të rëndësishme të informacionit, për pjesëmarrjen në takimet konsultative për projektligjin.

Në datën 9 Maj u zhvilluan takime konsultative me grupin I ku u përfshi sektori bankar, financiar (shkresa i është dërguar Bankës së Shqipërisë, Shoqatës Shqiptare të Bankave, Shoqatës Mikrofinanciare Shqiptare, MFE, AMF, si dhe janë njoftuar me e-mail të gjitha pikat e tyre të kontaktit).

Në datën 10 Maj u zhvilluan takime konsultative me grupin II ku u përfshi: Presidenca, Kuvendi, AKSHI, SHISH, AKSIK, ILDKPKI, PSH.

Në datën 11 Maj u zhvilluan takime konsultative me grupin III ku u përfshi sektori i transportit, shëndetësor, furnizimit me ujë, energjia, AKEP.

Në këto takime morën pjesë të gjitha infrastrukturat e informacionit si edhe subjekte të tjera të interesuara të cilët shfaqën interesin e tyre për pjesëmarrje nga njoftimi në regjistrin e konsultimeve publike.

Në këto takime u paraqitën risitë e projektligjit si dhe u diskutua lidhur me komentet dhe sugjerimet e pjesëmarrësve lidhur me projektligjin.

1. **Palët e interesit të përfshira**

*Listoni të gjithë palët e interesuara, qoftë organizata apo individë, të cilët kanë dhënë komente/kontribut në konsultimet publike përmes metodave të ndryshme të konsultimit, gjatë gjithë procesit të hartimit.*

*Përmendni gjithashtu numrin dhe strukturën e palëve të interesuara që morën pjesë në takime publike ose seanca të organeve këshilluese.*

*Specifikoni palët e interesuara që morën pjesë në grupin e punës për hartimin e aktit.*

Nëpërmjet platformës së konsultimit publik institucionet të cilat kanë përcjellë komente dhe sugjerime janë:

* Ministri i Shtetit dhe Kryenegociatori,
* Departamenti i Administratës Publike,
* Ministria e Drejtësisë,
* Agjencia Kombëtare e Shoqërisë së Informacionit,
* Ministria e Infrastrukturës dhe Energjisë,
* Komisioneri për të Drejtën e Informimit dhe Mbrojtjen e të Dhënave Personale,
* Autoriteti Kombëtar i Sigurisë së Informacionit të Klasifikuar,
* Ambasada Amerikane,
* Shoqata Shqiptare e Bankave,
* Banka e Shqipërisë,
* Ministria e Brendshme.

Projektligji është propozuar nga Kryeministri dhe është hartuar me kontributin e Autoritetit Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK), si dhe është bashkëpunuar me Agjencinë Kombëtare të Shoqërisë së Informacionit (AKSHI).

* Në datat 20 - 22 korrik, Autoriteti zhvilloi një workshop me ekspertët e TAIEX për shpjegimin e Direktivës 2016/1148 (NIS Directive). Ekspertët u njohën edhe me projekt ligjin e përgatitur nga ana e Autoritetit lidhur me qasjen ndaj Direktivës NIS 1 ku u shprehën se:

1. AKCESK ka treguar një përkushtim të fortë në arritjen e një shkalle të lartw pjekurie lidhur me kuadrin ligjor të sigurisë kibernetike në përputhje me legjislacionin e BE-së.

2. Ndërtimi dhe rregullimi i kuadrit normativ për mbrojtjen e infrastrukturës kritike të informacionit (hartimi dhe nxjerrja e ligjeve dhe akteve nënligjore) instituconi përgjegjës– Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike (AKCESK) e ka marrë shumë seriozisht dhe ka punuar me përkushtim deri më tani për të.

3. Projektligji “Për sigurinë kibernetike” përmban të giitha parashikimet e nevojshme për transpozimin e direktivës, nevojiten vetëm disa detaje të vogla për t’u përfshirë.

Rekomandimet e dhëna i referoheshin mbrojtjes së infrastrukturave kritike të informacionit, përkatësisht:

a) Për zhvillimin e mëtejshëm të kësaj fushe shihet e nevojshme njohja dhe shkëmbimi i njohurive dhe praktikave më të mira midis Republikës së Shqipërisë dhe autortiteteve të Bashkimit Evropian, të vendeve anëtare dhe vendeve të rajonit.

b) Procesi i përvetësimit të njohurive është një aktivitet afatgjatë dhe për këtë është e nevojshme të zbulohet se cilat njohuri dhe fusha kyçe duhet të përvetësohen, në mënyrë që ndërtimi i një sistemi të fuqishëm të mbrojtjes së infrastrukturës kritike të informacionit të jetë një aktivitet i planifikuar. Prandaj, është i nevojshëm zgjerimi i bashkëpunimit me komunitetin akademik, i cili mund të ofrojë njohuri dhe qasje që ndonjëherë mungojnë në këtë fazë për institucionet dhe individët.

c) Pjesëmarrja aktive e të gjitha ministrive që janë kompetente për politikat dhe planet sektoriale.

d) Konkretisht lidhur me këtë proces, por edhe ndërtimin e sistemit, është e nevojshme të ketë dialog dhe bashkëpunim sa më të gjerë të mundshëm me të gjithë aktorët përkatës brenda çdo sektori. Kjo duhet të përfshijë ministritë, agjencitë rregullatore, operatorët e infrastrukturës së informacionit kritik, organizatat profesionale dhe deri te shërbimet e inspektimit.

* Në datat 14-15 Dhjetor 2022 stafi i Autoritetit mori pjesë edhe në një trajnim të zhvilluar nga eGA lidhur me “Implementation of EU Cybersecurity Law”, trajnim në të cilin u shpjegua rreth Direktivës NIS 1 dhe NIS 2 duke bërë të mundur analizimin e elementëve të përfshirë në projektligj si dhe reflektimin e rekomandimeve të dhëna lidhur me të dy Direktivat. Në këtë trajnim u sqaruan të dy direktivat duke përfshirë pika kryesore lidhur me autortietit mbikëqyrëse kompetente, CSIRT, infrastrukturat e informacionit, raportimi dhe reagimi ndaj incidenteve kibernetike. Gjithashtu në fokus ishin edhe skemat e certifikimit të sigurisë kibernetike, risi e Direktivës NIS 2, e përfshirë edhe në projektligj. Shpjegimet u shoqëruan edhe me shembuj të modeleve të vendeve të Bashkimit Europian.

1. **Pasqyra e komenteve të pranuara me arsyetimin e komenteve të pranuara/ refuzuara**

*Gruponi komentet/ propozimet e pranuara sipas çështjes që ato ngritën;*

*Gruponi komente të ngjashme së bashku dhe renditni palët e interesuara që i ngritën ato;*

*Shpjegoni cili ishte vendimi i marrë dhe sqaroni shkurtimisht arsyet për të.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Çështja e adresuar** | **Komenti** | **Palët e interesuara** | **Vendimi** | **Justifikimi** |
| 1. **Mbi përmbajtjen e nenit 4**   **Përkufizimet** | Në nenin 4, pika 7, ku përkufizohet “Certifikatë e sigurisë kibernetike”, sugjerojmë të përcaktohet se cili është organi konkret që lëshon këtë certifikatë. | MB | Pranuar | Neni 4 pika 8 është riformuluar: Certifikatë e sigurisë kibernetike është një dokument i lëshuar nga një organ i vlerësimit të konformitetit për sigurinë kibernetike , që vërteton se një produkt, shërbim ose proces TIK, është vlerësuar për pajtueshmërinë me kërkesat specifike të sigurisë të përcaktuara në skemën e certifikimit të sigurisë kibernetike. |
| Në pikën 7, të sqarohet se cili është organi që lëshon certifikatën e sigurisë kibernetike. | MD | Pranuar | Reflektuar |
| Në nenin 4, pika 9, ku përkufizohet “*Emergjencë e sigurisë kibernetike”,* sugjerojmë saktësimin e nivelit të cenimit të sigurisë së informacionit në sistemet e informacionit, ose sigurisë së rrjeteve të komunikimeve elektronike, për të qenë në kushtet e emergjencës së sigurisë kibernetike. | MB | Refuzohet | Përkufizimi është i përgjithshëm. Nuk mund të bëhet saktësimi I nivelit të cënimit të sigurisë së rrjeteve dhe sistemeve.  Përkufizimi: është situata gjatë së cilës siguria e informacionit në sistemet e informacionit, ose siguria e rrjeteve të komunikimeve elektronike është cenuar duke vënë në rrezik interesin publik të Republikës së Shqipërisë. |
| Në nenin 4, pika 30, ku përkufizohet “Siguria kibernetike”, sugjerojmë riformulimin e kësaj pike, duke patur në vëmendje që siguria kibernetike është një grupim teknologjish, procesesh dhe praktikash të hartuara për të mbrojtur rrjetet, pajisjet, programet dhe të dhënat nga sulmet, vjedhjet, dëmtimet, modifikimet ose aksesi i paautorizuar | MB | Pranuar | Është bërë riformulimi i kësaj pike në përputhje me Direktivën NIS 2.  Neni 4 pika 28: “Siguria kibernetike”, është tërësia e veprimeve të nevojshme për të mbrojtur rrjetet dhe sistemet e informacionit, përdoruesit e këtyre rrjeteve dhe sistemeve si dhe personat e tjerë të prekur nga kërcënimet kibernetike. |
| Lidhur me nenin 4 “Përkufizime”, vlerësojmë se:  Në pikën 1 është e nevojshme të sqarohet nëse bëhet fjalë për një institucion të ri apo për Autoritetin Kombëtar për Çertifikimin Elektronik dhe Sigurinë Kibernetike | MIE | Refuzuar | Bëhet fjalë për të njëjtin institucion. Ka ndryshuar vetëm emërtimi.  Në nenin 39 pika 2 përcaktohet: Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike vazhdon të ushtrojë veprimtarinë e tij si institucioni përgjegjës në fushën e sigurisë kibernetike, deri në riorganizimin e tij në përputhje me dispozitat e këtij ligji. |
| Në përputhje me nenin 6, pika 1 të Direktivës NIS2 dhe me qëllim harmonizimin me ligjin për komunikimet elektronike, propozojmë riformulimin e pikës 26 të nenit 4, si më poshtë vijon:  “26. Rrjet dhe sistem informacioni është:  a ) një rrjet i komunikimeve elektronike sipas përcaktimeve në nenin 3 të ligjit për komunikimet elektronike në fuqi...” | MIE | Pranuar | Reflektuar |
| Përkufizimi i termit “shërbimi digjital” në pikën 37, duhet të rishikohet/riformulohet pasi është pothuajse i njëjtë me përkufizimin e shërbimit të shoqërisë se informacionit sipas ligjit nr.10 128 datë 11.05.2009 “Për tregtinë elektronike” si dhe nenit 3 pika 50 e ligjit nr. 9918/2008 “Për komunikimet elektronike”. | MIE | Pranuar | Reflektuar |
| Neni 4 pika 17 përcakton:“Motor kërkimi në internet” – vërejmë se ky togfjalësh nuk përdoret më tej ne tekst për rrjedhojë mendojmë se përcaktimi i tij është i panevojshëm. | Banka e Shqipërisë | Refuzuar | Gjen zbatim në anekset e këtij ligji |
| Të njëjtin koment si më lart kemi dhe për togfjalëshat e përcaktuar në pikat 22, 23, 24, 25 të nenit 4. | Banka e Shqipërisë | Refuzuar. | Perkufizimet janë perfshire ne lidhje me përdorimin e tyre ne ligj ( anekset) |
| Në pikën 10 të nenit 4 të Direktivës është dhënë përkufizimi i përfaqësuesit të një ofruesi të shërbimeve digjitale. Ky përkufizim nuk është përafruar në projektligjit me arsyetimin se ky përkufizim zbatohet vetëm për shtetet anëtare. Ky arsyetim nuk duket i drejtë duke pasur parasysh se pika 10 e nenit 4 të Direktivës flet për një përfaqësues të regjistruar në një shtet anëtar të Bashkimit Evropian që përfaqëson një ofrues të shërbimeve digjitale që nuk është regjistruar si entitet në Bashkimin Evropian. Në rastin e Shqipërisë, përfaqësuesi do të përfaqësonte një ofrues të shërbimeve digjitale që nuk është i regjistruar në Shqipëri, por në një vend të tretë. | Ministri i Shtetit dhe Kryenegociatori | Refuzuar | Marrë në konsideratë faktin që ofrues i shërbimit digjital është përfshirë vetëm si koncept. |
| Në pikën 11 të nenit 4 të Direktivës është dhënë përkufizimi i standardit duke iu referuar një akti tjetër të Bashkimit Evropian. Në këtë rast duhet pasur parasysh se përkufizimi i standardit në legjislacionin shqiptar është bërë tashmë në nenin 3 të Ligjit Nr. 9870, datë 4.2.2008 “Për standardizimin”, të ndryshuar. Në këtë rast duhet të vlerësohet nëse mund të bëhet referencë tek ky ligj. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Reflektuar |
| Në pikën 5 të nenit 4 të Direktivës është dhënë përkufizimi i shërbimit digjital. Kjo pikë është përafruar plotësisht në pikën 37 të nenit 4 të projektligjit. Në këtë rast sjellim në vëmendjen tuaj se një përkufizim i ngjashëm është dhënë në nenin 3 të Ligjit Nr. 10128, datë 11.5.2009 “Për tregtinë elektronike”, të ndryshuar. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Reflektuar |
| Në pikën 17 të nenit 4 të Direktivës është dhënë përkufizimi i tregtisë në internet si një shërbim digjital. Ndërkohë, përkufizimi i bërë në pikën 40 të nenit 4 të projektligjit e përkufizon tregun online si një ose disa platforma. Për këtë arsye lutemi rishikimin e këtij përkufizimi për ta bërë atë sa më të saktë. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Reflektuar |
| Në lidhje me pikën 3 të nenit 6, përkufizimi i termit “siguri kibernetike”, Direktiva bën referencë tek Rregullorja (BE) 2019/881. Në këtë rast vërejmë se përkufizimi i dhënë në pikën 29, neni 4 i projektligjit nuk është në përputhje me përkufizimin e Rregullores (BE) 2019/881. Përkufizimet duhet të jepen sa më shumë që të jetë e mundur *verbatim et literatim*. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Reflektuar |
| Lidhur me nenin 4 të projektligjit, sugjerohet si vijon:  Referuar pikave 22, 26, 33, 37, të kësaj dispozite, sjellim në vëmendje se përkufizimet synojnë të japin kuptimin e termave kryesorë, pa u ndalur në sanksionimin e rregullimeve ligjore të cilat duhet të gjejnë vend në krerë të tjerë të projektligjit (shih nenin 9, shkronja “e” të udhëzimit nr. 6/2022 të sipërcituar). Në këto kushte, të ripunohen këto paragrafë, duke shmangur përdorimin e tyre për të shprehur rregullimet ligjore përkatëse. | MD | Pranuar | Përkufizimet janë parë dhe janë riformuluar në përputhje me NIS 2 dhe janë reflektuar ne projektligj. |
| Të mbahet në konsideratë fakti që përkufizimet hartohen në funksion të shpjegimit të disa termave që gjejnë përdorim në projektligj. Në këtë drejtim, konstatohet që termi “specifikim teknik” nuk gjen përdorim, duke u sanksionuar vetëm në përkufizime. Të rishikohen të gjitha termat e përkufizuara në këtë linjë. | MD | Pranuar | Jane ripare përkufizimet. Specifikimi teknik gjen përdorim. |
| 1. **Shtim përkufizimesh** | Në nenin 4, “Përkufizime”, sugjerojmë shtimin e një pike në të cilën të përcaktohet “Hetimi digjital”, duke saktësuar se çfarë është dhe cilat veprime kryen gjatë këtij procesi. | MB | Refuzuar | Nuk konsiderohet e nevojshme. Pika përkatëse përcakton: ë) “Mbledh dhe analizon të dhënat nëpërmjet hetimit digjital dhe ofron analizë dinamike të riskut dhe të incidentit, si dhe kryen ndërgjegjësimin për situatën aktuale të sigurisë kibernetike.” |
| 1. **Mbi teknikën legjislative** | Referuar nenit 9, shkronja “c” të udhëzimit nr. 6, datë 29.4.2022, të Ministrit të Drejtësisë, “Për përcaktimin e metodologjisë së unifikuar për hartimin e akteve normative”, sipas së cilit baza ligjore e një akti ligjor duhet të përmbajë ndër të tjera edhe informacionin mbi propozuesin e projektligjit, sugjerohet që në bazë ligjore të shtohet edhe neni 81, pika 1 e Kushtetutës. | MD | Pranuar | Reflektuar |
| Në drejtim të strukturimit të projektligjit, dispozita e qëllimit të vijë në renditje pas dispozitës së objektit, duke ndjekur strukturën sipas nenit 9 të udhëzimit nr. 6/2022 të sipërcituar. Nga ana tjetër, për shkak të rëndësisë që paraqesin këto dy dispozita në një akt ligjor, sidomos në kuadër të zhvillimit të interpretimit të normave të caktuara juridike në përmbajtje të tij, sugjerohet rishikimi i tyre në drejtim të formulimit sa më qartë në raport me natyrën që këto dispozita kanë. | MD | Pranuar | Reflektuar |
| Konkretisht, lidhur me dispozitën e qëllimit, vlerësojmë se projektligji nuk mund të ketë si qëllim vetë atë, pra ligjin, referuar togfjalëshit “...përcaktimi i kornizës së nevojshme ligjore...”, por duhet të nxjerrë në pah qëllimin që synon të arrijë ligjvënësi nëpërmjet këtij projektligji dhe rregullave në përmbajtje të tij.  Ndërkohë, dispozita e objektit të rifomulohet qartë dhe të jetë koncize, pa specifikuar në mënyrë të hollësishme disa prej dispozitave, në një paragraf me disa nënparagrafë të renditur sipas rregullave në udhëzimin e sipërcituar, duke shmangur parashikimin e pikës 3, pasi ligjet prezumohen se janë në harmoni dhe koherencë me njëra tjetrën, duke kryer të gjitha përpjekjet për shmangien e kontradiktave gjatë fazës së hartimit të tij. Nga ana tjetër, pika 4 të përfshihet në një dispozitë që rregullon fushën e zbatimit të këtij projektligji. | MD | Pranuar | Reflektuar |
| Të mbahet në konsideratë gjatë ripunimit të projektligjit neni 20 i udhëzimit nr. 6/2022 të Ministrit të Drejtësisë, të sipërcituar lidhur me shënimin e numrave. | MD | Pranuar | Reflektuar |
| Në pikën 2, të vendoset në fund të përkufizimit termi “pranë Autoritetit”, në kushtet kur referuar nenit 8, pika 1, shkronja “c”, Autoriteti vepron në cilësinë e CERT-it, në funksion të qartësisë. | MD | Pranuar | Reflektuar |
| Fjalët e huaja, për të cilat nuk është gjetur një fjalë e përshtatshme në gjuhën shqipe, të shkruhen me shkronja kursive. | MD | Pranuar | Reflektuar |
| Në pikën 25, të jepet sqarimi për shkurtesën në kllapa “TLD”. Në të kundërt, të hiqet nga përmbajtja si i panevojshëm. | MD | Pranuar | Reflektuar |
| Në nenin 7, pika 1, lidhëza “ose” të zëvëndësohet me lidhëzën “dhe”. | MD | Pranuar | Reflektuar |
| Në nenin 8, pika 1, të shmanget përdorimi i togfjalëshit “në funksion të përmbushjes së qëllimit të këtij ligji”, pasi nuk ka funksion ligjor, por sqarues dhe mund të gjejë vend në relacionin shpjegues. Ky koment të mbahet në konsideratë edhe për dispozita të tjera të projektligjit ku gjejnë vend togfjalësha të tilla. | MD | Pranuar | Reflektuar |
| Të hiqet numërtimi i paragrafit (1) në kushtet kur dispozita përmban një paragraf të vetëm. Ky koment vlen edhe për dispozita të tjera të projektligjit ku vihet re gjithashtu identifikimi i nën paragrafëve me numra si vijon: “1.1, 1.2...”. Në këtë drejtim, lutemi unifikimin e tekstit të projektligjit sipas rregullave të teknikës legjislative (shih nenin 10 të udhëzimit nr. 6/2022 të sipërcituar lidhur me identifikimin e paragrafëve dhe nënparagrafëve). | MD | Pranuar | Reflektuar |
| Në nenin 11, në shkronjat “ë” dhe “j” të përcaktohet që rregulloret miratohen me urdhër të Drejtorit të Përgjithshëm të Autoritetit. Ky koment të mbahet në konsideratë edhe për nenet 13-14 të projektligjit. Gjithashtu, në shkronjën “k” të rishikohet referenca e brendshme e përdorur. | MD | Pranuar | Reflektuar |
| 1. **Mbi tabelën e përputhshmërisë** | Së fundmi, në lidhje me tabelat e përputhshmërisë, mënyra e paraqitjes së tyre krijon konfuzion dhe paqartësi në nivelin e transpozuar të direktivës së re, pasi direktiva e vjetër NIS është shfuqizuar. | MIE | Pranuar | Është përgatitur tabela e përputhshmërisë cila synon përafrimin e pjesshëm me Direktivën NIS 2. |
| Në tërësi për përkufizimet e bëra në nenin 4 të projektligjit duhet të kontrollohet përputhshmëria e tyre me tabelën e përputhshmërisë. Për shembull, përkufizimi i sigurisë së rrjetit dhe sistemeve të informacionit është bërë në pikën 29 të nenit 4 të projektligjit. Por, në tabelën e përputhshmërisë rezulton që të jetë vendosur si pika 28. Po ashtu, përkufizimi i operatorit të infrastrukturës kritike dhe të rëndësishme është bërë në pikat 18 dhe 19 të nenit 4 të projektligjit. Ndërsa në tabelën e përputhshmërisë është thënë se është bërë në pikat 16 dhe 17 të nenit 4 të projektligjit. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Reflektuar |
| Përkufizimi i rrjetit dhe sistemit të informacionit i bërë në pikën 1 të nenit 4 të Direktivës rezulton i përafruar në pikën 26 të nenit 4 të projektligjit. Kjo duhet të plotësohet në tabelën e përputhshmërisë. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Reflektuar |
| Në lidhje me nenin 5 të Direktivës, vërejmë se teksti i vendosur në tabelën e përputhshmërisë nuk përputhet plotësisht me tekstin e Direktivës sikurse publikuar në Fletoren Zyrtare të Bashkimit Evropian. Ky nen është synuar të përafrohet plotësisht në nenin 10 të projektligjit. Por, në këtë rast, vërejmë se nuk është përafruar pika 2 e nenit 5 të Direktivës e cila tregon kriteret për identifikimin e operatorëve të shërbimeve thelbësore. Në pikën 2 të nenit 10 të projektligjit thuhet se metodologjia e identifikimit të infrastrukturave kritike dhe të rëndësishme do të kryhet mbi bazën e një metodologjie të miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit. Po ashtu, edhe pika 7 e nenit 5 të Direktivës nuk është e përafruar plotësisht në nenin 10 të projektligjit. Pika 7 e nenit 5 të Direktivës tregon se cilat informacione do t’i dërgohen Komisionit nga shtetet anëtare. Pika 3 e nenit 10 të projektligjit nuk i përcakton këto informacione. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Reflektuar |
| Në shënimin në lidhje me nenet 1 dhe 2 të Direktivës, thuhet se “Shkronja (e), neni 2, kushtëzohet me anëtarësimin e Republikës së Shqipërisë në BE”. Në lidhje me këtë vërejmë se germa “e” e pikës 2 të nenit 1 të Direktivës përcakton detyrimin që shteti anëtar (në këtë rast edhe Shqipëria si shtet kandidat që e përafron këtë Direktivë) duhet të caktojë autoritetet kompetente, pikën e vetme të kontaktit dhe CSIRT me detyra në lidhje me sigurinë e rrjeteve dhe sistemeve të informacionit. Në vlerësimin tonë, kjo germë është e përafruar në nenin 2 të projektligjit, në të cilin caktohet autoriteti përgjegjës për sigurinë kibernetike, i cili kryen edhe rolin e pikës së vetme të kontaktit, dhe ekipeve përgjegjëse ndaj incidenteve të sigurisë kibernetike, si CSIRT kombëtar, etj. Në vlerësimin tonë, nuk është përafruar si një mundësi dhe detyrim vetëm për shtetet anëtare, germa “b” dhe “c” e pikës 2 të nenit 1 të Direktivës. Kjo sepse germa “b” përcakton ngritjen e një grupi bashkëpunimi mes institucioneve të shteteve anëtare, ndërsa germa “c” përcakton ngritjen e një rrjeti të ekipeve të shteteve anëtare, të reagimit nga incidenteve. Në këtë dy këto forma bashkëpunimi, Shqipëria si shtet kandidat nuk merr pjesë për momentin. Germa “b” dhe “c” mund të shtohen në një moment të mëvonshëm si pjesë e integrimit të përshpejtuar pas marrëveshjes eventuale me Komisionin Evropian. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Marrë në konsideratë. Është riparë direktiva duke përfshirë në projektligj edhe nenet lidhur me Grupin e Bashkepunimit, rrjeti CSIRT-ve etje. |
| Në lidhje me nenin 3 të Direktivës është vendosur një shënim se ky nen aplikohet për shtetet anëtare. Kjo nuk është e saktë. Ky nen u jep mundësinë shteteve anëtare dhe atyre kandidate që të miratojnë ose të mbajnë në fuqi dispozita që synojnë një nivel më të lartë sigurie se ato të përcaktuara në Direktivë. Edhe shteti shqiptar mund të vendosë rregulla të tilla nëse e shikon këtë të nevojshme dhe të realizueshme. Në këtë aspekt, Direktiva përcakton rregullat minimale për sigurinë kibernetike. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Marrë në konsideratë. |
| Neni 6 i Direktivës nuk është i përafruar plotësisht në nenin 19 të projektligjit. Konkretisht, kriteret mbi të cilat bazohet vlerësimi i pasojave të padëshirueshme sipas Direktivës nuk janë përafruar plotësisht në pikën 4 të nenit 19 të projektligjit. Pika 2 e nenit 6 të Direktivës nuk është e përafruar në nenin 19 të projektligjit. Në tabelën e përputhshmërisë, neni 19 është vendosur gabimisht si neni 18. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Marrë në konsideratë. |
| Në lidhje me nenin 8 të Direktivës, vërejmë se ai kërkon që çdo shtet anëtar të caktojë një ose disa institucione kompetente të sigurisë kibernetike që të mbulojnë të paktën sektorët e përmendur në Shtojcën II dhe shërbimet e përmendura në Shtojcën III. Projektligji në nenet 6, 8, 9 dhe 15 të tij nuk përmban një dispozitë të qartë që të ngarkojë AKCESK-un me detyrën për mbuluar sektorët e përfshirë në Shtojcën II dhe shërbimet e përmendura në Shtojcën III të Direktivës. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Projektligji përcakton AKCESK si autoritetin përgjegjës për sigurinë kibernetike si dhe subjektet e tjera përgjegjëse për sigurinë kibernetike.Ne projektligj eshte bere edhe referenca përkatëse tek anekset e projektligjit. |
| Në lidhje me nenin 9 të Direktivës vërejmë se ai përcakton ngritjen e CSIRT-eve në përputhje me kërkesat e pikës 1 të Shtojcës 1 të Direktivës. Pika 1 e Shtojcës 1 të Direktivës kërkon që CSIRT-et të kenë disa sisteme komunikimi me të tjerët në çdo kohë. Kjo dispozitë nuk duket e përafruar qartë në projektligjin shqiptar. Direktiva kërkon që mjediset e CSIRT dhe sistemet mbështetëse të informacionit të jenë në vende të sigurta. Ndërkohë projektligji, në germën “l” të pikës 1 të nenit 11, flet vetëm për sistemet e informacionit të CSIRT që duhet të jenë në vende të sigurta. | Ministri i Shtetit dhe Kryenegociatori | Refuzuar | Në projektligj janë dhënë parashikimet e përgjithshme. Ne përputhje me NIS 2 Direktiven dispozita eshte ripare dhe janë perfshire përcaktime lidhur me kërkesat e përgjithshme qe duhet te permbushen. |
| Në lidhje me nenin 10 të Direktivës, vërejmë se teksti i vendosur në tabelën e përputhshmërisë nuk përputhet plotësisht me tekstin e Direktivës sikurse publikuar në Fletoren Zyrtare të Bashkimit Evropian. | Ministri i Shtetit dhe Kryenegociatori | Pranuar |  |
| Në lidhje me nenin 11 të Direktivës, vërejmë se teksti i vendosur në tabelën e përputhshmërisë nuk përputhet plotësisht me tekstin e Direktivës sikurse publikuar në Fletoren Zyrtare të Bashkimit Evropian. | Ministri i Shtetit dhe Kryenegociatori | Pranuar |  |
| Në lidhje me pikën 3 të nenit 28 të projektligjit (që synon përafrimin e plotë të nenit 11 të Direktivës) vërejmë se shënimi në tabelën e përputhshmërisë i referohet nenit 27 të projektligjit dhe jo nenit 28. | Ministri i Shtetit dhe Kryenegociatori | Pranuar |  |
| Në lidhje me nenin 12 të Direktivës, vërejmë se teksti i vendosur në tabelën e përputhshmërisë nuk përputhet plotësisht me tekstin e Direktivës sikurse publikuar në Fletoren Zyrtare të Bashkimit Evropian. | Ministri i Shtetit dhe Kryenegociatori | Pranuar |  |
| Pika 3 e nenit 14 të Direktivës përcakton se njoftimet për CSIRT nga operatorët e shërbimeve thelbësore do të përmbajnë informacion që mundëson AKCESK-un në rastin tonë, që të vlerësojë ndikimin ndërkufitar të incidentit. Kjo kërkesë e pikës 3 të nenit 14 të Direktivës nuk duket e përafruar në nenet 16, 17, 19 dhe 21 të projektligjit. Pika 5 e nenit 14 të Direktivës kërkon më tej se kur informohen shtetet e tjera mbi ndikimin e një incidenti mbi shërbimet thelbësore në këto shtete, kjo bëhet duke ruajtur sigurinë dhe interesat tregtare të operatorit të shërbimeve thelbësore. Kur e lejojnë rrethanat, autoriteti kombëtar i jep operatorit informacion relevant mbi ecurinë e njoftimit të tij për të mbështetur trajtimin efektiv të incidentit. Këto rregulla nuk janë përafruar në legjislacionin shqiptar. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Marrë në konsideratë. |
| Në lidhje me përafrimin e neneve 14 dhe 16 të Direktivës, AKCESK si hartues i projektligjit ka shpjeguar se janë përafruar në të njëjtat nene të projektligjit sepse ofrojnë rregulla të njëjta si për operatorët e shërbimeve thelbësore ashtu edhe për ofruesit e shërbimeve digjitale. Në këtë rast vërejmë se bëhet fjalë për dy kategori të ndryshme subjektesh të rregullimit ligjor. Rregullimi ligjor që Direktiva ofron për ta është e ndryshme dhe kjo duhet të reflektohet edhe në projektligjin shqiptar. Në pikën 49 të preambulës së Direktivës thuhet se “Në praktikë, shkalla e riskut për operatorët e shërbimeve thelbësore, të cilat shpesh janë thelbësore për kryerjen e aktiviteteve kritike shoqërore dhe ekonomike, është më e lartë se për ofruesit e shërbimeve digjitale. Prandaj, kërkesat e sigurisë për ofruesit e shërbimeve digjitale duhet të jenë më të lehta. Ofruesit e shërbimeve digjitale duhet të mbeten të lirë për të marrë masat që ata i konsiderojnë të përshtatshme për të menaxhuar risqet që vijnë për sigurinë e rrjetit të tyre dhe sistemeve të informacionit”. Për shembull, sipas pikës 11 të nenit 16 të Direktivës, rregullat për ofruesit e shërbimeve digjitale të Kapitullit V të Direktivës nuk do të zbatohen për ndërmarrjet mikro dhe të vogla (Shiko edhe pikën 53 të preambulës). Ndërkohë neni 14 nuk e bën një përjashtim të tillë për ndërmarrjet mikro dhe të vogla në rolin e operatorit të shërbimeve thelbësore. Po ashtu, fjalia e fundit e pikës 4 të nenit 16 të projektligjit përcakton se ofruesi i shërbimit digjital ka detyrimin që të njoftojë një incident nëse ai ka akses në informacionin e duhur për të vlerësuar ndikimin e incidentit krahasuar me parametrat e përcaktuar në pikën 4 të nenit 16. Ky rregull nuk vlen për ofruesit e shërbimeve thelbësore sipas nenit 14. | Ministri i Shtetit dhe Kryenegociatori | Refuzuar | Projektligji jep parashikime të përgjithshme lidhur me kërkesat e sigurisë për operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit. Detyrimet përkatëse lidhur me zbatimin e masave të sigurisë do te përcaktohen me akte nenligjore.  Gjithashtu proejktligji eshte ripare ne perputhjeme përcaktimet e NIS 2. |
| Në lidhje me përafrimin e nenit 15 të Direktivës, vërejmë se fjalia e fundit e pikës 2 të nenit 15 të Direktivës, përcakton se kur autoriteti (AKCESK) kërkon informacion ose dëshmi, ai duhet të deklarojë qëllimin e kërkesës dhe të specifikojë informacionin që kërkon. Kjo dispozitë nuk është përafruar në nenin 25 të projektligjit. Më tej, pika 4 e nenit 15 të Direktivës përcakton se autoriteti do të bashkëpunojë ngushtësisht në marrjen e informacionit dhe dëshmive me autoritetet e mbrojtjes së të dhënave personale. As kjo pikë nuk është përafruar në nenin 25 të projektligjit. | Ministri i Shtetit dhe Kryenegociatori | Refuzuar | Këto parashikime janë bërë në tërësi të përmbajtjes së projektligjit. Parimi i mbrojtjes së të dhënave personale është një nga parimet bazë. |
| Në lidhje me nenin 17 të Direktivës, AKCESK ka zgjedhur që ta përafrojë në ato nene me të cilat ka përafruar edhe nenin 15. Do të ishte më oportune që përafrimi të bëhej në nene të ndryshme për të ruajtur dallimet mes operatorit të shërbimeve thelbësore dhe ofruesit të shërbimeve digjitale. Në këtë rast vërejmë se pika 60 e preambulës thotë “Ofruesit e shërbimeve digjitale duhet t'i nënshtrohen aktiviteteve mbikëqyrëse më të lehta dhe reaktive ex post të justifikuara nga natyra e shërbimeve dhe operacioneve të tyre. Prandaj, autoriteti kompetent në fjalë duhet të ndërmarrë veprime vetëm kur i ofrohen prova, për shembull nga vetë ofruesi i shërbimit digjital, nga një autoritet tjetër kompetent, duke përfshirë një autoritet kompetent të një shteti tjetër anëtar, ose nga një përdorues i shërbimit, se një ofrues i shërbimit digjital nuk është në përputhje me kërkesat e kësaj Direktive, veçanërisht pas ndodhjes së një incidenti. Prandaj, autoriteti kompetent nuk duhet të ketë asnjë detyrim të përgjithshëm për të mbikëqyrur ofruesit e shërbimeve digjitale. | Ministri i Shtetit dhe Kryenegociatori | Refuzuar | Projektligji i referohet operatorëve kritikë dhe të rëndësishëm të informacionit. Jane reflektuar përcaktimet qe ben direktiva NIS 2.  Gjithashtu ne projektlgji janed përcaktuar detyrimet e përgjithshëm te operatoreve te infrastruktruave te informacionit, ndërsa përcaktimet e tjera sic janë masat e sigurisë kibernetike, ndarja se kush do zbatoje çfarë do te përcaktohet me akt neneligjor. |
| Në lidhje me nenin 18 “Juridiksioni dhe territorialiteti”, është vendosur një shënim se ky nen është relevant vetëm për shtetet anëtare. Në këtë rast vërejmë se rregullat e këtij neni përcaktojnë se kur një ofrues i shërbimeve digjitale është në juridiksionin e një shteti të caktuar. Në mungesë të një norme juridike të ngjashme shtrohet pyetja se kur dhe cilët ofrues të shërbimeve digjitale janë nën juridiksionin e shtetit shqiptar. Për këtë sjellim në vëmendjen tuaj, shpjegimet e dhëna në pikat 64 dhe 65 të preambulës së Direktivës. | Ministri i Shtetit dhe Kryenegociatori | Refuzuar | Projektligji i referohet operatorëve kritikë dhe të rëndësishëm të informacionit duke ndjekur NIS 2 Direktiven. Ofruesit e shërbimeve digjitale janë përmendur si koncept por jo rregullime te detajuara. |
| Në lidhje me përafrimin e nenit 21 të Direktivës, vërejmë se neni rregullon ndëshkimin dhe jo masat korrigjuese. Për këtë arsye, ky nen nuk është i përafruar në nenin 31, por vetëm në nenin 32, 33, 34 dhe 35. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Riparë |
| Në lidhje me nenet 21, 23, 24 dhe 25 të Direktivës, vërejmë se teksti i vendosur në tabelën e përputhshmërisë nuk përputhet plotësisht me tekstin e Direktivës sikurse publikuar në Fletoren Zyrtare të Bashkimit Evropian. | Ministri i Shtetit dhe Kryenegociatori | Pranuar |  |
| Nenet 39 dhe 40 të projektligjit duhet të vendosen saktë në tabelën e përputhshmërisë. | Ministri i Shtetit dhe Kryenegociatori | Pranuar |  |
| Shtojca I e Direktivës është e përafruar edhe në nenin 11 të projektligjit, i cili duhet të vendoset në tabelën e përputhshmërisë. | Ministri i Shtetit dhe Kryenegociatori | Pranuar |  |
| Shtojca II e Direktivës është e përafruar në nenin 9 të projektligjit. Por, në këtë rast do të sugjeronim që të ndiqej e njëjta mënyrë përcaktimi e subjekteve të infrastrukturave kritike sikurse vepruar në Shtojcën II, duke bërë referencë në aktet ligjore shqiptare përkatëse. Për shembull, në rastin e ndërmarrjeve në sektorin e energjisë, nënsektori i elektricitetit, të përcaktohet se bëhet fjalë për ndërmarrjet e furnizimit, shpërndarjes dhe transmetimit të energjisë elektrike, sipas përcaktimeve të Ligjit Nr. 43/2015 “Për sektorin e energjisë”, i ndryshuar. | Ministri i Shtetit dhe Kryenegociatori | Refuzuar | Nuk mund të bëhet një përcaktim i tillë , kjo pasi ky nen bën përcaktimin e subjekteve të tjera përgjegjëse të sigurisë kibernetike ( subjektet dhe sektorët) . ( referenca ne projektin aktual neni 11) |
| Në tabelën e përputhshmërisë thuhet se Shtojca III është përafruar në pikën 37 të nenit 4 dhe në germën “dh” të pikës 2 të nenit 9. Në këtë rast vërejmë se pika 37 e nenit 4 jep përkufizimin e shërbimit digjital duke mos pasur asnjë lidhje me kategoritë e shërbimeve digjitale të Shtojcës III. Neni 9 nga ana tjetër, nuk ka pikë 2. Germat “dh” të pikës 1.1 dhe pikës 1.2 të nenit 9, flasin respektivisht për ministrinë përgjegjëse për mbrojtjen dhe subjektet që ofrojnë shërbime në sektorët e mjedisit dhe mbrojtjes së territorit dhe autoritetet territoriale përgjegjëse për furnizimin dhe shpërndarjen e ujit të pijshëm. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Marrë në konsideratë. |
| Në tabelën e përputhshmërisë duhet të vendoset i plotë teksti i Direktivës (BE) 2022/2555 sikurse kërkuar nga Vendimi i Këshillit të Ministrave nr. 584, datë 28.8.2003, “Për miratimin e rregullores së Këshillit të Ministrave”, i ndryshuar. Kjo do të lehtësojë vlerësimin tërësor të përputhshmërisë në lidhje me projektligjin e propozuar. Për shembull, neni 1 i Direktivës i cili nuk është i përfshirë në tabelën e përputhshmërisë është plotësisht i përafruar në projektligj. Pjesë të tjera të Direktivës mund të jenë përafruar ose synohen të përafrohen në akte të tjera ligjore. Për shembull, germa “a” e pikës 1 të nenit 6 të Direktivës synohet të përafrohet plotësisht në projektligjin “Për komunikimet elektronike në Republikën e Shqipërisë”. Vendosja e tekstit të plotë në tabelën e përputhshmërisë do të ndihmojë në perspektivë procesin e përafrimit të mëtejshëm të Direktivës. | Ministri i Shtetit dhe Kryenegociatori | Pranuar |  |
| Në tabelën e përputhshmërisë duhet të synohet zbërthimi në një nivel sa më detajuar i aktit të Bashkimit Evropian që synohet të përafrohet. Në çdo rast duhet të evitohet që në një rresht të tabelës të mblidhen bashkë dy ose më shumë nene të aktit të Bashkimit Evropian. | Ministri i Shtetit dhe Kryenegociatori | Pranuar |  |
| Neni 9 i Direktivës nuk është i përafruar plotësisht në projektligj. Për  shembull, pika 4 e nenit 9 të Direktivës, përcakton se duhet të miratohet një plan kombëtar për incidentet e sigurisë kibernetike dhe reagimit ndaj krizave në shkallë të gjerë. Në këtë pikë jepen edhe elementet që duhet të ketë ky plan. Ndërkohë në projektligj nuk gjejmë një dispozitë ekuivalente. | Ministri i Shtetit dhe Kryenegociatori | Pranuar | Marre ne konsiderate dhe reflektuar tek neni 28 lidhur me krizën kibernetike ( pika 8) |
| **V. Terminologjia juridike** | Në pikën 4 të nenit 4 të Direktivës është dhënë përkufizimi i operatorit të shërbimeve thelbësore. Duhet të kontrollohet nëse ky përkufizim është i përafruar plotësisht në projektligj, ku flitet për operator të infrastrukturës kritike. Në këtë rast do të sugjeronim që të përdorej një terminologji e krahasueshme me atë të përdorur në vetë Direktivën. | Ministri i Shtetit dhe Kryenegociatori | Refuzuar | Terminologjia e përdorur eshte ajo kritike dhe e rendesishme. |
| Në pikën 6 të nenit 4 të Direktivës është dhënë përkufizimi i ofruesit të shërbimit digjital. Por, projektligji flet për operator të infrastrukturës së rëndësishme të informacionit. Përsëri do të sugjeronim që të përdorej një terminologji e krahasueshme me atë të përdorur në vetë Direktivën | Ministri i Shtetit dhe Kryenegociatori | Refuzuar | Terminologjia e përdorur operator i infrastrukturës kritike dhe te rëndësishme te informacionit. Sherbimi digjital eshte përdorur si koncept dhe eshte bere pjese e anekseve te projektligjit. |
| Në pikën 1, termi “institucion publik” të zëvendësohet me termin “organ publik”, në përputhje me terminologjinë e Kodit të Procedurave Administrative. Ky koment të mbahet në konsideratë kudo që është i aplikueshëm në përmbajtje të projektligjit. | MD | Pranuar |  |
| Referuar pikave 3, 4, 5 dhe 6, të unifikohet terminologjia e përdorur duke përcaktuar qartë nëse CSIRT është ekip apo person i vetëm. Nga ana tjetër, të rishikohen këto formulime në funksion të qartësisë ligjore, pasi në thelb CSIRT sektorial nënkupton atë kombëtar, ndërsa CSIRT pranë operatorëve nënkupton CSIRT qeveritar | MD | Refuzuar | Përkufizimet janë në përputhje me funksionet që kryen secili. |
| Referuar pikave 18, 19 dhe 20, sugjerohet zëvendësimi i termave “subjekt publik”, “subjekt privat” me termat “person fizik” ose “person juridik”, sipas rastit, në përputhje me terminologjinë e përdorur në dispozitat e Kodit Civil, sikurse parashikohet nga ligji në fuqi. Ky koment të mbahet në konsideratë gjatë ripunimit në tërësi të projekt aktit. | MD | Pranuar | Reflektuar |
| Në nenin 6, të bëhet unifikimi i termave të përdorura lidhur me statusin juridik të Autoritetit Kombëtar për Sigurinë Kibernetike, pasi vihet re përdorimi i termave të ndryshëm si: “organ rregullator”, “institucion përgjegjës” dhe “institucion juridik publik”, ndërkohë në përkufizim është cilësuar si “institucion publik përgjegjës për...”. | MD | Pranuar | Reflektuar |
| Në nenin 14, pika 1, togfjalëshi “ekipi përgjegjës (CSIRT) për operatorin” të riformulohet në përputhje me termin e përkufizuar (CSIRT pranë operatorëve), në funksion të unifikimit të termave të përdorura në këtë projektligj. | MD | Pranuar | Reflektuar |
| Në nenin 23, pika 2, togfjalëshi “institucionet e tjera përgjegjëse” të zëvëndësohet me togfjalëshin “subjektet e tjera përgjegjëse”, sipas terminologjisë së përdorur në nenin 9 të këtij projektligji. | MD | Pranuar | Reflektuar |
| Neni 8 i projektligjit parashikon kompetencat e Autoritetit Kombëtar përgjegjës për Sigurinë Kibernetike. Në lidhje me shkronjën “g” të këtij neni sipas së cilës parashikohet “...regjistron organizmat e testimit dhe vlerësimit të konformitetit për masat e sigurisë kibernetike” sugjerojmë të rishikohen termat e përdorur duke i njehsuar me nenet paraardhëse, konkretisht nenin 4, pika 21 ku përdoret termi “Organizmi i Vlerësimit të Konformitetit”. Ky koment vlen edhe për terminologjinë e përdorur në nenin 26 pika 4. | BSH | Pranuar | Terminologjia eshte unifikuar (organe te vlerësimit te konformitetit per sigurinë kibernetike) |
| Neni 16 pika 2 :“...të certifikuara...” – Sugjerojmë zëvendësimin e fjalës të certifikuara me të licencuara. Nëse do ti qëndroni shprehjes të certifikuara mendojmë se duhet të shpreheni se nga cili autoritet certifikohen. | BSH | Refuzuar | Terminologjia e përdorur është e certifikuar, në kuadër të skemës së certifikimit te sigurisë kibernetike. Cerifikimi bëhet nga një organ i vlerësimit të konformitetit për sigurinë kibernetike. |
| **VI. Mbi përmbajtjen e nenit 2** | Në përputhje me nenin 2 pika 12 dhe 14 të Direktivës NIS2, sugjerojmë që në nenin 2 pas pikës 4, të shtohen pikat si më poshtë:  “5. Ky ligj nuk cënon/paragjykon zbatimin e legjislacionit në fuqi për komunikimet elektronike në veçanti lidhur me dispozitat për privatësinë në komunikimet elektronike.  6. Përpunimi i të dhënave personale sipas këtij ligji nga ofruesit e rrjeteve të komunikimeve elektronike ose ofruesit e sherbimeve të komunikimeve elektronike të disponueshme për publikun do të kryhet në përputhje me legjislacionin në fuqi për mbrojtjen e të dhënave personale në veçanti me dispozitat për mbrojtjen e të dhënave personale në komunikimet elektronike sipas ligjit për komunikimet elektronike.” | MIE | Refuzuar | Referuar objektit të ligjit është riformuluar marrë konsideratë komentet e ardhura. Shtimi i pikave të propozuara nuk është pranuar pasi ligji ka përcaktuar rregullimet e nevojshme referuar direktives si dhe parimet e pergjithshme. |
| **VII. Mbi përmbajtjen e nenit 5** | Në nenin 5, pika 3: të sqarohet që plani i veprimit i cili i bashkëlidhet Strategjisë Kombëtare të Sigurisë Kibernetike dhe që rishikohet të paktën çdo dy vjet, miratohet me vendim të Këshillit të Ministrave. | MD | Pranuar | Reflektuar |
| Në nenin 5 “Strategjia Kombëtare për Sigurinë Kibernetike”, sugjerojmë që pika e 2-të e këtij neni të kalojë si pikë e parë. Gjithashtu, në pikën 3 të këtij neni, nuk del e qartë nëse plani i veprimit është pjesë integrale e strategjisë dhe nëse miratohet me vendim të Këshillit të Ministrave. | MIE | Pranuar | Reflektuar |
| Neni 7 i Direktivës nuk është i përafruar plotësisht në nenin 5 të projektligjit. Neni 7 tregon elementët kryesorë që duhet të përmbajë strategjia e sigurisë kibernetike. Ndërkohë nenin 5 i projektligjit nuk bën asnjë përcaktim të tillë. | Ministri I Shtetit dhe Kryenegociatori | Pranuar | Reflektuar |
| **VIII. Mbi përmbajtjen e nenit 6** | Neni 6: Në pikën 4 parashikohet se marrëdhëniet e punës së Drejtorit të Përgjithshëm dhe nëpunësve të Autoritetit rregullohen në bazë të dispozitave të Kodit të Punës të Republikës së Shqipërisë, i ndryshuar. Në këtë drejtim, duke mbajtur në konsideratë nenin 2 të ligjit nr. 152/2013, “Për nëpunësin civil”, i ndryshuar dhe përcaktimet e ligjit nr. 90/2012, “Për organizimin dhe funksionimin e administratës shtetërore”, të jepen sqarime mbi rregullimin e marrëdhënieve të punës sipas Kodit të Punës dhe jo sipas legjislacionit të shërbimit civil, sikurse parashikohet aktualisht. | MD | Pranuar | Reflektuar |
| Të hiqet parashikimi i pikës 5 si i papërshtatshëm për t’u vendosur në një akt ligjor, duke vlerësuar përfshirjen e tij në vendimin e Këshillit të Ministrave që rregullon çështjet e strukturave dhe të niveleve të pagave të nëpunësve në institucionet e administratës publike ose në një vendim tjetër të Këshillit të Ministrave sipas vlerësimit tuaj. | MD | Refuzuar | Përcaktimi i bërë në projektligj rrjedh nga akti normativ nr.18, datë 9.12.2022 “Për disa ndryshime dhe shtesa në ligjin nr.9880, datë 25.2.2008,“Për nënshkrimin elektronik”, të ndryshuar. Referuar tipologjisë së veçantë të institucionit, mjaft pozicione kane nevojë për ekspertizë specifike të veçantë (p.sh. kontrolli i masave të sigurisë, certifikimi dhe verifikimi i proceseve dhe pajisjeve te informacionit, siguria e sistemeve dhe rrjeteve të informacionit, sulmet kibernetike, siguria kibernetike, infrastrukturat etj) që kanë domosdoshmëri për kualifikime dhe certifikime mjaft specifike sektoriale të vazhdueshme. Në këtë kontekst kategorizimi i shtesës së pagës për kushte të veçanta pune, është hartuar në përputhje me veprimtarinë e çdo njësie sipas imaktit që shkakton puna në këtë njësi. Kompleksiteti i fushës, imponon trajtime financiare te ndryshme për role të ndryshme. Në këtë frymë është konsideruar lënia e këtij parashikimi referuar vetë rëndësisë që paraqet. |
| Gjithashtu, në nenin 6, të projektligjit duhet të përfshihet një dispozitë me përmbajtjen si vijon:  “Pjesë e strukturës dhe organikës së Autoritetit Kombëtar për Sigurinë Kibernetike është qendra operacionale kombëtare e monitorimit të sigurisë kiberenetike përgjegjëse për ” . | DAP | Pranuar | Reflektuar |
| Në lidhje me përcaktimin e shtesës për natyrë të veçantë pune dhe masës së saj në pikën 5, të  nenit 6, sugjerojmë që kjo pikë të riformulohet si vijon:  “5. Drejtori i Përgjithshëm dhe nëpunësit e njësive organizative të përmbajtjes së Autoritetit, përveç pagës bruto mujore të përcaktuar me vendim të Këshillit të Ministrave, përfitojnë edhe një shtesë të veçantë të kushtëzuar, sipas përcaktimit në legjislacionin në fuqi.”  Sugjerimi për riformulimin e kësaj pike bëhet duke marrë shkas nga inicimi i projektligjit të veçantë që përcakton kompetencat për caktimin e pagave, të trajtimeve të tjera financiare dhe të përfitimeve për të punësuarit në institucionet e administratës publike, projektligj që tashmë pas miratimit nga Këshilli i Ministrave është dërguar në Kuvend për shqyrtim dhe miratim. | DAP | Refuzuar | Përcaktimi i bërë në projektligj rrjedh nga akti normativ nr.18, datë 9.12.2022 “Për disa ndryshime dhe shtesa në ligjin nr.9880, datë 25.2.2008,“Për nënshkrimin elektronik”, të ndryshuar. Referuar tipologjisë së veçantë të institucionit, mjaft pozicione kane nevojë për ekspertizë specifike të veçantë (p.sh. kontrolli i masave te sigurise, certifikimi dhe verifikimi i proceseve dhe pajisjeve te informacionit, siguria e sistemeve dhe rrjeteve të informacionit, sulmet kibernetike, siguria kibernetike, infrastrukturat etj) që kanë domosdoshmëri për kualifikime dhe certifikime mjaft specifike sektoriale të vazhdueshme. Në këtë kontekst kategorizimi i shteses se pages per kushte te vecanta pune, eshte hartuar ne perputhje me veprimtarine e cdo njesie sipas imaktit qe shkakton puna ne kete njesi. Kompleksiteti i fushes, imponon trajtime financiare te ndryshme per role te ndryshme. Ne kete fryme eshte konsideruar lënia e këtij parashikimi referuar vetë rëndësisë që paraqet. |
| Në pikën 5 të nenit 6, të projektligjit parashikohet se: “Drejtori i Përgjithshëm dhe nëpunësit e njësive teknike të përmbajtjes së Autoritetit, përveç pagës sipas kategorive të pagës së përcaktuar me vendim të Këshillit të Ministrave, përfitojnë një shtesë për natyrë të veçantë pune, në masën deri në 800 000 (tetëqind mijë) lekë në muaj. Masa e shtesës për natyrë të veçantë pune për secilën kategori përcaktohet me vendim të Këshillit të Ministrave”.  Në kushtet ku, masa shtesë për natyrë të veçantë pune ka qenë e parashikuar dhe në pikën 5, të nenit 12, të projektligjit “Për identifikimin elektronik dhe shërbimet e besuara” vlerësojmë se i njëjti parashikim nuk mund të jetë në dy projektakte të ndryshme.  Verësojmë se ky parashikim bie në kundërshtim dhe me Vendimin e miratuar nga Këshilli i Ministrave për propozimin e projektligjit “Për përcaktimin e pagave, trajtimeve të tjera financiare dhe përfitimeve të të punësuarve në institucionet e administratës publike si dhe të pagës bazë  minimale në shkallë vendi”. Referuar këtij projektligji, qeveria synon të mos vendosë trajtime financiare nëpër ligje sektoriale por ti vendosë ato në një ligj të veçantë.  Gjithashtu, sjellim në vëmendjen tuaj se trajtimi financiar i punonjësve të AKSHI-t u hoq nga projektligji “Për qeverisjen elektronike” me argumentimin e mësipërm, gjatë mbledhjes së qeverisë ku u mor vendimi për të dërguar në parlament këtë projektligj. | AKSHI | Refuzuar | Referuar tipologjisë së veçantë të institucionit, mjaft pozicione kane nevojë për ekspertizë specifike të veçantë (p.sh. kontrolli i masave te sigurise, certifikimi dhe verifikimi i proceseve dhe pajisjeve te infrastrukturave te celesave publike dhe atyre te infrastrukturave te informacionit, siguria e sistemeve dhe rrjeteve të informacionit, sulmet kibernetike, siguria kibernetike, infrastrukturat etj) që kanë domosdoshmëri për kualifikime dhe certifikime mjaft specifike sektoriale të vazhdueshme. Në këtë kontekst kategorizimi i shteses se pages per kushte te vecanta pune, eshte hartuar ne perputhje me veprimtarine e cdo njesie sipas imaktit qe shkakton puna ne kete njesi. Kompleksiteti i fushes, imponon trajtime financiare te ndryshme per role te ndryshme. Ne kete fryme eshte konsideruar lënia e këtij parashikimi referuar vetë rëndësisë që paraqet. |
| **IX. Mbi përmbajtjen e nenit 7** | Neni 7: Lidhur me pikën 2, shkronja “d”, të jepen sqarime mbi mënyrën e verifikimit të plotësimit të kriterit përkatës, pasi formulimi është i përgjithshëm. | MD | Pranuar | Kjo pikë është riformuluar dhe është bërë shpjegimi përkatës në relacion. Shquarja për aftësi në fushën e sigurisë kibernetike dhe qenia i certifikuar ndërkombëtarsht përfshin: certifikatë ndërkombëtare në analizë kibernetike, në shfrytëzim sisitemesh, për implementimin e standardeve të saigurisë së informacionit, pjesë e një numri projektesh ndërkombëtare ( më shumë se 4 projekte ndërkombëtare) |
| Lidhur me kriterin e parashikuar në pikën 2, shkronja “ë”, të parashikohen se cilat janë rastet e konfliktit të interesit në ushtrimin e detyrës. Në të kundërt, të bëhet referimi në legjislacionin përkatës që rregullon çështjet e konfliktit të interesave në ushtrimin e funksioneve publike. | MD | Prannuar | Reflektuar duke bërë referencë tek ligji përkatës. |
| Në pikën 4, shkronja “c”, të sqarohen se cilat do të konsiderohen shkelje të rënda në detyrë, të cilat përbëjnë shkak për shkarkimin e Drejtorit të Përgjithshëm të Autoritetit nga detyra. Nga ana tjetër, të parashikohen rregulla lidhur me procedurën e shkarkimit nga detyra të Drejtorit, duke garantuar në çdo rast një proces të rregullt ligjor përgjatë zhvillimit të kësaj procedure. | MD | Pranuar pjesërisht | Reflektuar rastet të cilat do të koniderohen si shkelje të rënda në detyrë.  Lidhur me procedurën e shkarkimit nuk shihet e nevojshme të përcaktohet pasi në çdo rast garantohet procesi i rregullt ligjor. |
| **X. Mbi përmbajtjen e nenit 8** | Në shkronjën “dh”, të pikës 1, të nenit 8, të projektligjit, është përfshirë, si një ndër kompetencat e Autoritetit Kombëtar për Sigurinë Kibernetike, “ngritja dhe administrimi i qendrës operacionale kombëtare të monitorimit të sigurisë kibernetike”.  Meqënëse në tekstin e projektligjit dhe në relacionin shoqërues nuk jepen sqarime në lidhje me qendrën, e si rrjedhim statusi institucional dhe detyrat e përgjegjësitë e saj, mbeten të paqarta, sqarojmë sa vijon:  a. Nëse qendra do të jetë një institucion i administratës shtetërore me personalitet juridik publik të ndryshëm nga ai i autoritetit, atëherë në bazë të ligjit nr. 90/2012, “Për organizimin dhe funksionimin e administratës shtetërore” dhe të ligjit nr. 9000/2003, “Për organizimin dhe funksionimin e Këshillit të Ministrave”, ajo nuk mund të ngrihet dhe administrohet nga Autoriteti Kombëtar i Sigurisë Kibernetike. Nëse ky është rasti, duhet të bëhen ndryshimet e nevojshme në projektligj, duke parashikuar krijimin e qendrës nga Këshilli i Ministrave dhe të jepen përgjegjësitë kryesore të saj.  b. Nëse qendra do të jetë pjesë e strukturës dhe organikës së autoritetit, atëherë përcaktimi i shkronjës “dh”, të pikës 1, të nenit 8, të projektligjit duhet të hiqet. | DAP | Pranuar | Marrë në konsideratë komenti. Është hequr “ngre”. |
| Neni 8: Në pikën 1, shkronja “ë”, të jepet sqarimi për termat e përdorura “monitorim aktiv” dhe “instalim të agjentëve”, pasi janë të paqartë. Nëse vlerësohet e nevojshme me qëllim qartësimin e kësaj kompetence që i jepet Autoritetit, sugjerohet të jepet përkufizimi i tyre. | MD | Refuzuar | Kjo pike është riforuluar. Instalim i agjentëve - është hequr.  Lidhur me sqarimin e termit “monitorim aktiv”-nuk është e nevojshme sqarimi në dispozitë  (kompetencë e SOC+ respektimi i parimit të mbrotjejs së të dhënave personale, parimi I neutralitetit të teknologjisë) |
| Në nenin 8, të Kreut II, të projektaktit, sugjerojmë që: shkronja “ë” të riformulohet sipas përmbajtjes: *“ë)kryen monitorim aktiv të infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet aksesit në platformat e brendshme sektoriale të monitorimit me qëllim evidentimin dhe parandalimin e veprimeve keqdashëse;”* | AKSHI | Pranuar pjesërisht | Eshtë bërë riformulim i pikës: e) kryen monitorim aktiv të infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet informacioneve të marra nga platformat e jashtme të ngritura nga Autoriteti si dhe nga platformat e brendshme me kërkesë nga operatorët e infrastrukturave të informacionit qëllim evidentimin dhe parandalimin e veprimeve keqdashëse; ( referenca ne projektin aktual pika “e” neni 9 |
| Shkronja f) të riformulohet sipas përmbajtjes: “f) vlerëson dhe analizon nivelin e sigurisë së sistemeve për infrastrukturat kritike dhe të rëndësishme të informacionit, nëpërmjet kontrolleve dhe testimeve simuluese. Metodologjia e përdorur për qëllim vlerësimin dhe analizimin e sigurisë miratohet me vendim të Këshillit të Ministrave;”. | AKSHI | Pranuar | Reflektuar |
| Me synim shmangien e ndonjë impakti të padëshiruar në sistemet dhe shërbimet e operatorëve, propozojmë që pika e mësipërme të riformulohet si vijon:*f) vlerëson dhe analizon nivelin e sigurisë së sistemeve për infrastrukturat kritike dhe të rëndësishme të informacionit, nëpërmjet kontrolleve dhe testimeve simuluese në dakordësim paraprak me operatoret e infrastrukturave kritike dhe të rëndësishme”* | Shoqata Shqiptare e Bankave | Refuzuar | Kjo pike është riformuluar”  f) vlerëson dhe analizon nivelin e sigurisë së sistemeve për infrastrukturat kritike dhe të rëndësishme të informacionit, nëpërmjet kontrolleve dhe testimeve simuluese; Metodologjia e përdorur për qëllim vlerësimin dhe analizimin e sigurisë kibernetike miratohet me vendim të Këshillit të Ministrave. |
| Neni 8 shkronja d): *“...me të dhënat në sisteme...”* i projektligjit - Ky togfjalësh sugjerojmë të zëvendësohet me: “... *mbi masat mbrojtëse*...”, pasi nuk mendojmë qe do shkëmbehen të dhënat në sisteme. Ose dispozita siç është parashikuar ne projektligj të jetë më e qarte pasi mund të krijoje keqkuptime. | BSH | Refuzuar | Nuk ka lidhje me masat mbrojtëse. |
| Neni 8 shkronja ë): *“kryen monitorim aktiv të infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet instalimit të agjenteve...”* i projektligjit mendojmë se është i paqartë kryesisht shprehjet “monitorim aktiv” dhe “nëpërmjet instalimit të agjentëve”. | BSH | Pranuar | Është riformuluar: “e) kryen monitorim aktiv të infrastrukturave kritike dhe të rëndësishme të informacionit nëpërmjet informacioneve të marra nga platformat e jashtme të ngritura nga Autoriteti si dhe nga platformat e brendshme me kërkesë nga operatorët e infrastrukturave të informacionit qëllim evidentimin dhe parandalimin e veprimeve keqdashëse; |
| Neni 8 shkronja g*): “regjistron organizmat e vlerësimit të konformitetit për masat e sigurisë kibernetike”* është e paqartë për ne. | BSH | Refuzuar | Eshte kompetence e Autoritetit. “regjistron organizmat e vlerësimit të konformitetit për sigurinë kibernetike për vlerësimin e masave të sigurisë kibernetike.”  Neni 26 pika 4 “Për impelementimin efektiv të masave të sigurisë kibernetike, operatorët paraqesin pranë Autoritetit raportin e vleresimit të konformitetit, nga një Organ i Vlerësimit të Konformitetit për Sigurinë Kibernetike , të paktën një herë në 2 vjet.”  Gjithashtu nenin 5 pika 23 “Organ i Vlerësimit të Konformitetit për sigurinë kibernetike”, është një person fizik ose juridik, kombëtar ose ndërkombëtar, i akredituar nga institucioni përgjegjës për akreditim, për të kryer vlerësimet dhe konformitetin e produkteve, shërbimeve dhe proceseve që lidhen me sigurinë kibernetike TIK, si dhe vlerësimin e masave të sigurisë kibernetike të implementuara nga infrastrukturat kritike dhe të rëndësishme të informacionit.” |
| Neni 8, pika 1, shkronja ë:  Nevojitet të përcaktohet qartë, se çfarë lloj informacioni do monitorohet nëpërmjet “agjenteve”. Agjentët nuk duket te monitorojnë të dhëna personale, të dhëna klientësh, apo të dhëna konfidenciale, të cilat përbejnë sekret bankar. Ky monitorim duhet të kryhet vetëm nëse dakordësohet procesi mes operatoreve dhe Autoritetit. Në çdo rast kjo duhet të arrihet pasi SOC kombëtar të arrijë pjekurinë e duhur dhe të ketë demonstruar masa të larta sigurie.  Nevojitet të përcaktohet me definicion se çfarë kuptohet me” agjent”. Instalimi i agjenteve rrit riskun kibernetik kundrejt sistemeve të infrastrukturave kritike dhe rrit riskun operacional (konflikt mes teknologjive të ndryshme, mirëmbajtje, suport); bie ndesh me parimin e sigurisë së informacionit mbi ndarjen e minimumit të nevojshëm të informacionit dhe rrit në mënyrë të panevojshme volumin e të dhënave pa u shoqëruar me kontekst.  Mendojmë se mbledhja e informacionit në një pikë të vetme ka rrezikshmëri, pasi mund të funksionojë si “single point of failure”. Në rast kompromentimi të SOC sektorial, rrezikon i gjithë sektori financiar. Për këtë arsye është e rëndësishme që legjislacioni të parashikoje dhe masa të larta sigurie të cilat zhvillohen dhe përditësohen në përputhje me “best practices” ndërkombëtar. Gjithashtu informacioni që autoriteti përpunon dhe ruan, nuk duhet të ketë të dhëna konfidenciale mbi infrastrukturat kritike si p.sh teknologjitë e përdorura. Në rast nevoje specifike për të pasur këtë informacion, informacioni duhet të fshihet menjëherë pas përfundimit të procesit.  Zgjidhja teknike sugjerohet të mos jetë pjesë e ligjit pasi është subjekt e ndryshimeve të shpeshta që ndodhin të teknologji si edhe ligji duhet të jetë me gjithë përfshirës dhe të akomodojë si i sektorin publik edhe atë privat, ambiente të ndryshme dhe teknologji të ndryshme si edhe nivele të ndryshme maturiteti që kanë operatorët e infrastrukturave kritike dhe të rëndësishme në shërbimet e sigurisë kibernetike.  Kjo pikë nuk është pjesë e Direktivës (BE) 2016/1148 dhe nuk gjendet në asnjë rregullore/ligj të BE ose US si praktikë ose si kompetencë e organeve shtetërore ndaj infrastrukturave financiare. Gjithashtu bie ndesh me kompetencat e OIKR për te garantuar monitorimin dhe implementimin e masave sipas objektit te këtij ligji duke krijuar konflikt kompetencash midis funksioneve te sigurisë se OIKR dhe funksioneve/nën funksioneve monitoruese të Autoritetit. Duhet theksuar që asetet informatike janë ne pronësi të OIKR, të dhënat që ruhen/përpunohen në to i janë dhënë me konsent OIKR nga pronarët e këtyre të dhënave. Në bazë të këtyre argumentimeve aksesi direkt për të monitoruar këto asete mundet ti jepet palëve të treta (në këtë rast AKCESK) vetëm me dakordësi paraprake me OIKR, autorizim nga bordet drejtuese dhe njoftim paraprak tek Komisioneri për Mbrojtjen e të Dhënave Personale. | Shoqata Shqiptare e Bankave | Refuzuar  Refuzuar | Projektligji jep parashikime të përgjithshme. Agjentët janë hequr. Gjithashtu në çdo moment ligji synon mbrojtjen e të dhënave personale, konfidencialitetin si dhe bashkëpunimin midis subjekteve te këtij ligji. Gjithashtu masat e sigurisë te përcaktuara janë dhene te përgjithshme (detajimi i tyre me VKM) duke synuar nje nivel te larte te sighurise kibernetike ne vend. |
| Në nenin 8, pika 1, shkronja “j”, ku përcaktohet se Autoriteti Kombëtar për Sigurinë Kibernetike vepron si qendër kombëtare ndëruniversitare, për të krijuar dhe ngritur kapacitetet e burimeve njerëzore në fushën e sigurisë kibernetike, sugjerojmë riformulimin e kësaj shkronje në përputhje me parashikimet e ligjit nr. 80/2015 “Për arsimin e lartë dhe kërkimin shkencor në institucionet e arsimit të lartë në Republikën e Shqipërisë”. | MB | Pranuar pjesërisht | Është riformuluar, por jo në referencë e bërë: ndërvepron me qendrën ndëruniversitare të sigurisë kibernetike, për të krijuar dhe ngritur kapacitetet e burimeve njerëzore në fushën e sigurisë kibernetike; |
| Neni 8, pika 1, shkronja “f” Me synim shmangien e ndonjë impakti të padëshiruar në sistemet dhe shërbimet e operatorëve, propozojmë që pika e mësipërme të riformulohet si vijon:  *f) vlerëson dhe analizon nivelin e sigurisë së sistemeve për infrastrukturat kritike dhe të rëndësishme të informacionit, nëpërmjet kontrolleve dhe testimeve simuluese* ***në dakordësim paraprak me operatoret e infrastrukturave kritike dhe të rëndësishme”*** | AAB | Refuzuar | Është riformuluar si pikë në përputhje me kompetencat e Autoriteti. Refrenca ne proejtkligj ka ndryshuar ( neni 9 pika ë) |
| **XI. Mbi përmbajtjen e nenit 9** | Në nenin 9, pika 1.1. shkronja “f”, të përcaktohen shprehimisht se cilat janë institucionet e tjera përgjegjëse për ruajtjen dhe përpunimin e të dhënave qeveritare. Gjithashtu, në pikën 1.2, shkronja “f” të jepen sqarime se cilat janë subjektet që ofrojnë shërbime në sektorin akademik. | MD | Refuzuar | Referenca neni 11, i referohet sektorit arsimor. |
| Në nenin 9, “Subjektet përgjegjëse për Sigurinë Kibernetike”, konstatojmë se janë lënë jashtë përfshirjes sektori i komunikimeve elektronike/telekomunikacionit, ministria përgjegjëse si dhe Autoriteti i Komunikimeve Elektronike dhe Postare, të cilët aktualisht kanë detyra të caktuara me ligjin nr. 9918/2008 për mbikëqyrjen e veprimtarisë së operatorëve të komunikimeve elektronike për çështjet e sigurisë dhe integritetit të rrjetit të komunikimeve elektronike. Si e tillë, sugjerojmë të përfshihen në këtë nen. | MIE | Pranuar |  |
| Në nenin 9 të projektligjit konstatojmë se parashikohen fillimisht në pikën 1 të tij një numër institucionesh të cilët cilësohen si subjekte përgjegjëse të sigurisë dhe mbrojtjes kibernetike, ndërkohë në pikën 2 të po këtij neni është bërë një kategorizim i subjekteve përgjegjëse sektoriale të sigurisë së rrjeteve dhe sistemeve të informacionit.  Neni 7 është i paqartë nëse ka patur për qellim që në pikën 1 të tij të përcaktojë institucionet përgjegjëse për sektorët e referuar në pikën 2. | BSH | Pranuar | Është marrë në konsideratë dhe është riformuluar neni 11 lidhur me subjektet përgjegjëse për sigurinë kibernetike. |
| Gjithashtu, referuar pikës 1.2 shkronja “c” ku parashikohet “Sektori i ekonomisë, financës, sektorin e infrastrukturës së tregut financiar, sektorin bankar fintek, shoqëritë e sigurimeve si dhe sistemet mikrofinanciare” nuk është e qartë nëse CSIRT sektoriale të përmendura në këtë dispozitë do të jenë pjesë e një CSIRT sektorial, apo secili sektor i përmendur do të jetë pjesë e një CSIRT të veçantë sektorial. Sektori i Ekonomisë dhe Financës nuk mund të ndahet lehtësisht. Përgjegjësitë sektoriale i atribuohen institucioneve ekzekutive (qeverise) dhe jo institucioneve te pavarura. Sqarojmë se, konkretisht nga këndvështrimi i Bankës së Shqipërisë krijimi i strukturave te posaçme apo dhe investimi ne burime njerëzore/procese apo dhe teknologji është diçka qe shkon përtej kompetencave dhe hapësirave te Ligjit për Bankën se Shqipërisë, persa i përket objektivit kryesor dhe objektivave të tjerë të institucionit. | BSH | Pranuar pjesërisht | Mënyra e ngritjes, organizimi dhe funksionimi i CSIRT-eve sektoriale përcaktohet me Vendim të Këshillit të Ministrave |
| Më tej, duke ju referuar sërish nenit 9, pika 1.2 shkronja “c”, mendojmë se duhet të përkufizohet termi sektori “bankar fintek” për të qartësuar se cilat subjekteve i referoheni. Në të kundërt duhet rishikuar terminologjia duke qenë se në legjislacionin bankar nuk ekziston një term i tillë, pra nuk ndahen subjektet bankare në subjekte fintek dhe jo fintek. | BSH | Pranuar | Është hequr termi fintek. |
| Të hiqet gërma “ë’’, pika 1.2 ku citohet se:  “Subjektet përgjegjëse për ofrimin e shërbimeve të sektorëve sa më poshtë vijon:  ë) Subjektet që ofrojnë shërbime në sektorët për përpunimin dhe transmetimin e informacionit të klasifikuar që lidhen me sigurinë publike”;  pasi krijon konfuzion në të kuptuarit se cilët janë sektorët që meren me përpunimin dhe transmetimin e informacionit të klasifikuar që lidhen me sigurinë publike.  Sektorët që meren me transmetimin dhe përpunimin e informacionit të klasifikuar janë objekt i ligjit nr. 10/2023 “Për informacionin e klasifikuar” dhe konkretisht në pikën 1, gërma a neni 49 përcaktohet se:  1.Autoriteti Kombëtar i Sigurisë së Informacionit të Klasifikuar, i cili funksionon edhe si:  a) Autoritet Kombëtar i Akreditimit të Sigurisë (AKAS), përgjegjës për akreditimin e sigurisë SKI-së, të cilat nuk janë pjesë e infrastrukturave kritike dhe të rëndësishme të informacionit, si dhe sistemeve të NATO-s, BE-së dhe shteteve/organizatave të huaja që operojnë në institucionet e administratës publike. (ASIK) | AKSIK | Pranuar | Reflektuar |
| Neni 13 i projektligjit Detyrat e CSIRT sektorial në paragrafin e parë përcakton “Subjektet përgjegjëse për ofrimin e shërbimeve sipas përcaktimeve të bëra në nenin 9 të këtij ligji, duhet të kenë në strukturën e vet CSIRT-in sektorial, përgjegjës për incidentet e sigurisë kibernetike sipas fushës së përgjegjësisë së tyre, i cili”. Në lidhje me subjektet përgjegjëse ri sjellim në vëmendje që neni 9 është i paqartë mbi subjektet përgjegjëse dhe fushat që do të mbulojnë si subjekte të tilla. | BSH | Pranuar | Reference neni 11, është riformuluar |
| **XII. Mbi përmbajtjen e nenit 10** | Lidhur me pikën 3 të nenit 10, sugjerojmë të mbahet në konsideratë neni 122 i ligjit nr. 9918 datë 19.5.2008 “Për komunikimet elektronike në RSH” të ndryshuar, i cili parashikon: “...*13. AKEP-i mund të shkëmbejë informacion për shkeljet e sigurisë me Komisionin Evropian dhe Agjencinë Evropianë për Sigurinë e Rrjeteve dhe të Informacionit (ENISA), si dhe me autoritetet kompetente në vendet e tjera, në përputhje me kërkesat e ligjit për mbrojtjen e të dhënave për transferimin ndërkombëtar.”* | MIE | Pranuar | Referenca ne projektligj neni 23, pika 7.  Marre ne konsiderate. Reference : legjislacionin në fuqi për marrëveshjet ndërkombëtare dhe për mbrojtjen e të dhënave personale. |
| **XII. Mbi përmbajtjen e nenit 11** | Në nenin 11, të Kreut II, të projektligjit, sugjerojmë që:  shkronja “c” të riformulohet sipas përmbajtjes: “*c) Monitoron, analizon dhe menaxhon kërcënimet kibernetike, vulnerabilitetet dhe incidentet në nivel kombëtar dhe ofron asistencë teknike për infrastrukturat kritike dhe të rëndësishme të informacionit sipas kërkesave nga operatorët e infrastrukturave kritike;”* | AKSHI | Pranuar | Referenca ne projektin aktual neni 13, pika c |
| Neni 11, shkronja “ç” të riformulohet sipas përmbajtjes: *“ç) Monitoron në bashkëpunim me operatorët e infrastrukturave, rrjetet dhe sistemet në infrastrukturat e tyre, kritike dhe të rëndësishme të informacionit mbi incidente të sigurisë kibernetike apo sulme të mundshme kibernetike;”* | AKSHI | Pranuar | Referenca ne projektin aktual : Neni 13 pika d.  Riformuluar : “monitoron në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, rrjetet dhe sistemet në infrastrukturat e tyre mbi incidente të sigurisë kibernetike apo sulme kibernetike; |
| Neni 11, shkronja “d”, të riformulohet sipas përmbajtjes: *“d) Trajton incidentet kibernetike të raportuara nga operatorët e infrastrukturave dhe jep zgjidhje konkrete duke u bazuar në politikat dhe masat e përcaktuara në këtë ligj, si dhe bashkëpunon me institucionet përkatëse ligjzbatuese në rast se konstaton ekzistencën e një krimi kibernetikë;”* | AKSHI | Pranuar pjesërisht | Reference ne projektin aktual neni 13  Riformulimi: “dh) trajton incidentet kibernetike në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit dhe jep zgjidhje konkrete duke u bazuar në politikat dhe masat e përcaktuara në këtë ligj, si dhe bashkëpunon me institucionet përkatëse ligjzbatuese kur dyshon për elementë të krimit kibernetikë; |
| Neni 11 shkronja *ë): “Siguron ruajtjen e logeve për një periudhë të përcakuar sipas procedurës së caktuar në rregulloren e miratuar nga Drejtori i Pergjithshëm”.* Është e paqartë se për cilat loge bëhet fjalë. | BSH | Pranuar | Është riformuluar : “Siguron ruajtjen e logeve të incidenteve të evidentuara ose të raportuara për një periudhë të përcakuar në rregulloren e miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit.” |
| Neni 11 shkronja *g): “Vlerëson kur infrastruktura është në një situatë me risk të lartë dhe kryen veprime reaktive, pas ndodhjes së incidentit kur shërbimi i ofruar nga infrastruktura ka ndaluar së funksionuari për më shumë se 4 orë-*është e paqartë se për cilën Infrastrukturë bëhet fjalë, të cilit subjekt. Gjithashtu mendojmë se “Veprimet reaktime” se pari kryhen nga vete subjekti.  Ndoshta duhet te jete me e qarte tipi i veprimeve reaktive qe ndermerr CSIRT Kombetar. | BSH | Refuzuar | Ligji jep parashikime të përgjithshme. Nuk bëhet fjalë për një subjekt specifik por i drejtohet të gjitha infrastrukturave të informacionit. |
| Neni 11 shkronja *h): “Ndërhyn pranë çdo infrastrukture për të mbështetur në mënyrë aktive zgjidhjen e incidenteve” -* Ndërhyrja çfarë nënkupton kjo dispozitë, sugjerojmë një riformulim “*Mbështet subjektet e infrastrukturave kritike për zgjidhjen e incidenteve” mund te ishte shprehja e përshtatshme*. | BSH | Refuzuar | Është riformuluar: “I përgjigjet çdo infrastrukture, në zbatim të procedurave të sigurisë , për të mbështetur në mënyrë aktive zgjidhjen e incidenteve.” |
| Neni 11 pika h: Ky parashikim nuk është pjese e Direktivës. Ndërhyrja bëhet vetëm me dakordësi të OIKR në përputhje me rregulloret dhe ligjet e tjera në fuqi pa cenuar mbarëvajtjen funksionale të OIKR.  Me synim shmangien e ndonjë impakti të padëshiruar në sistemet dhe shërbimet e operatorëve, si dhe duke konsideruar se operatorët kanë përgjegjësinë, proceset dhe “knowhow” të specializuar për sistemet e tyre, Autoriteti duhet të ofrojë shërbime plotësuese përforcuese, propozojmë që pika e mësipërme të riformulohet si vijon:  h) “Në dakordësim paraprak me operatoret e infrastrukturave kritike dhe të rëndësishme, ofron sipas kërkesës së operatoreve mbështetje aktive për zgjidhjen e incidenteve” | Shoqata Shqiptare e Bankave | Refuzuar | Kjo pike është riformuluar: h) i përgjigjet çdo infrastrukture, në zbatim të procedurave të sigurisë , për të mbështetur në mënyrë aktive zgjidhjen e incidenteve. |
| l) Simulon rrjetet dhe sistemet e operatorëve për të gjetur pikat e dobëta të infrastrukturës dhe shërbimeve të tyre.  *Koment AAB* – dhe në pikën e msipërme propozojmë qe të shtohet/parashikohet që ky “Simulim”, bëhet më kërkesë të operatorit ose me dakordësimin e tij. | Shoqata Shqiptare e Bankave | Pranuar | Riformuluar:  l) Simulon rrjetet dhe sistemet për të gjetur pikat e dobëta të infrastrukturës duke njoftuar paraprakisht operatorët. |
| Neni 11 shkronja *ll) “Analizon incidentin për të gjetur shkakun e tij si edhe koordinon aktivitetin me operatorët, CSIRT-et sektoriale, institucionet ndërkombëtare dhe qeveritare kur e shikon të arsyeshme”.* Duket se kjo dispozitë është përsëritje e parashikimit nëpiken (i) të po këtij neni. | BSH | Refuzuar | Janë 2 parashikime të ndryshme. |
| Dispozitat mbi Detyrat dhe Përgjegjësitë (neni 11) mund të forcohen duke shtuar detyrën/përgjegjësinë e mëposhtme në listë:  "Koordinon me Policinë e Shtetit Shqiptar dhe çdo zyrë të prokurorisë përkatëse për të ruajtur dhe mundësuar mbledhjen e provave të krimeve të dyshuara kibernetike apo terrorizmit që përfshijnë një infrastrukturë kritike informacioni ose infrastrukturë të rëndësishme informacioni." | Ambasada  Amerikane | Pranuar pjeserisht | Riformuluar. Neni 13, “o” : “koordinon me Policinë e Shtetit dhe çdo institucion përkatës për të ruajtur dhe mundësuar mbledhjen e provave kur dyshon për elementë të krimit kibernetik apo veprave të tjera penale të lidhura me to në infrastrukturat e informacionit.” |
| Në nenin 11, pika 1, shkronja “h”, ku përcaktohet se Autoriteti vepron në cilësinë e CSIRT-it Kombëtar dhe ndërhyn pranë çdo infrastrukture për të mbështetur në mënyrë aktive zgjidhjen e incidenteve, sugjerojmë të konkretizohet forma e ndërhyrjes, duke mbajtur në konsideratë që kjo ndërhyrje të mos cenojë veprime të tjera ligjore që vijnë pas konstatimit të incidentit. | MB | Pranuar | Është bërë riformulim : “I përgjigjet çdo infrastrukture, në zbatim të procedurave të sigurisë , për të mbështetur në mënyrë aktive zgjidhjen e incidenteve” |
| g) Vlerëson kur infrastruktura është në një situatë me risk të lartë dhe kryen veprime reaktive, pas ndodhjes së incidentit kur shërbimi i ofruar nga infrastruktura ka ndaluar së funksionuari për më shumë se 4 orë.  Në pikën e mësipërme duhet shtuar: Në koordinim me Infrastrukturen kritike. | Shoqata Shqiptare e Bankave | Pranuar pjesërisht | Riformuluar: gj) vlerëson kur infrastruktura është në një situatë me risk të lartë dhe kryen veprime reaktive, në bashkëpunim me infrastrukturën pas vënies ne dijeni të ndodhjes së incidentit kur shërbimi i ofruar nga infrastruktura ka ndaluar së funksionuari për më shumë se 4 orë. Metodologjia për vlerësimin e riskut të infrastrukturës përcaktohet me udhëzim të Drejtorit të Përgjithshëm të Autoritetit pas konsultimit me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit; |
| **XIV. Mbi përmbajtjen e nenit 12** | Neni 12 i projektligjit parashikon se “Organizimi dhe funksionimi i CSIRT-eve sektoriale, dhe CSIRT-eve pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit përcaktohet me Vendim të Këshillit të Ministrave”. Vlerësojmë se CSIRT sektoriale nuk mund të krijohen me akt nënligjor. Është e rëndësishme që ligji të jetë i qartë se cilët do të jenë CSIRT sektoriale që do të krijohen dhe institucionet përgjegjëse, kjo veçanërisht nëse do të lindi nevoja për të investuar në kapacitete të reja njerëzore dhe mjete pune të cilat do të kenë efekte financiare për institucionet që do ti implementojnë këto detyrime. Detajet e mënyrës së funksionimit të tyre vlerësojmë se mund të përcaktohen me VKM. | BSH | Refuzohet | Ligji jep parashikime të përgjithshme prandaj është përcaktuar që mënyra e ngritjes, organizimit dhe funksionimit do të përcaktohet me VKM. |
| Neni 12: Ky nen parashikohon nxjerren e aktit nënligjor brenda 6 muaj nga miratimi. Të parashikohet ngarkesa, kostoja dhe nevoja për ndryshim gjatë vendosjes se këtij organizimi. | Shoqata Shqiptare e Bankave | Refuzuar | Nuk mund të përcaktohet në ligj. Vlerësimi eshte bere tek Raporti i vlerësimit te ndikimit (RIA) . |
| **XV. Mbi përmbajtjen e nenit 13** | Referuar parashikimit në pikën ç të Nenit 13 dhe pikës 1 shkronja dh) të nenit 14, theksojmë se, në pikën 1 të nenit 101 të ligjit nr. 9918 date 19.5.2008 “Për komunikimet elektronike në RSH” të ndryshuar, është e përcaktuar ruajtja dhe administrimi i të dhënave për qëllime të ndjekjes penale... “*1. Pavarësisht përcaktimeve të tjera në këtë ligj, sipërmarrësit e rrjeteve dhe të shërbimeve të komunikimeve elektronike publike detyrohen të ruajnë dhe të administrojnë, për një afat 2-vjeçar, skedarët e të dhënave për pajtimtarët e tyre. Në rastin e komunikimeve në internet të dhënat përfshijnë dhe loget e komunikimit”.* | MIE | Pranuar | Është bërë riformulimi i kësaj pike : “*ruan loge të incidenteve të evidentuara ose të raportuara për një periudhë të përcaktuar në rregulloren e miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit”* |
| Në nenin 13, shkronja “ë”, të riformulohet parashikimi përkatës pasi është i paqartë dhe joshterues. | MD | Refuzuar | Eshtë i qartë si parashikim. Rëndësia e trajnimeve dhe certifikimeve periodike pasi vetë fusha është e tillë dhe kërkon staf të specializuar. |
| Neni 13 detyrat e CSIRT sektorial parashikon në shkronjën c): “mban përgjegjësi për raportimin e incidenteve kibernetike të ndodhura në infrastrukturat kritike dhe të rëndësishme të informacionit që ata dhe operatorët administrojnë sipas fushës së veprimtarisë së tyre”. Sjellim në vëmendje se raportimi i incidentit fillon nga operatori i infrastrukturës kritike, dhe si fillim është përgjegjësi e operatorit për ta raportuar. | BSH | Refuzuar | Parashikimi ka të bëjë me koordinimin dhe bashkëpunimin ndërmjet operatorëve dhe CSIRT-eve me qëlllim trajtimin në kohë të incidentit. |
| ç) ruan loge për një periudhë të përcaktuar sipas procedurës së caktuar me rregulloren e miratuar nga Drejtori i Përgjithshëm.  Koment AAB – Nevojite të mbahet në konsideratë që Periudha duhet të ndjekë praktikat më të mira. Afati përtej një mesatareje 3-6 muaj do krijonte shumë vështirësi. E konsiderojmë mjaft të rëndësishme përfshirjen në procesin e konsultimit të rregullores. | Shoqata Shqiptare e Bankave | Pranuar pjesërisht | Kjo pike është riformuluar. Marrja në konsideratë për përfshirjen në procesin e konsultimit të rregullores. |
| Neni 13 shkronja dh): “njofton CSIRT-in kombëtar menjëherë pasi identifikon incidentin, si dhe e njofton këtë të fundit në rast të zgjidhjes së shpejtë të incidentit të ndodhur në infrastrukturat që administrojnë” - CSIRT sektorial është menduar të jetë hallke ndërmjetëse midis CSIRT Kombëtar dhe operatorit? Na rezulton se raportimi kryhet nga CSIRT i operatorit (neni 14). Nëse do të duhet edhe ky subjekt te raportoje për incidentet e operatoreve këtu thjesht do kishim një dublim te raportimeve. Mbase duhet te jene me te qarta detyrat ne tërësi për CSIRT sektorial. Incidentin e identifikon CIRT-i pranë operatorit (neni 14). | BSH | Refuzuar | Nuk ka dublim të raportimeve. Vetëm koordinim dhe bashkëpunim |
| **XVI. Mbi përmbajtjen e nenit 14** | Neni 14, paragrafi 1, c)- shtoni gjuhën e theksuar:  Trajton incidentin dhe ofron zgjidhje konkrete bazuar në politikat dhe masat e përcaktuara në këtë ligj, si dhe bashkëpunon me institucionet përkatëse të zbatimit të ligjit në rast se gjen mundësinë e ekzistencës së një krimi kibernetik ose terrorizmi. | Ambasada  Amerikane | Pranuar pjesërisht. | Referenca neni 13 pika dh)trajton incidentet kibernetike në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit dhe jep zgjidhje konkrete duke u bazuar në politikat dhe masat e përcaktuara në këtë ligj, si dhe bashkëpunon me institucionet përkatëse ligjzbatuese kur dyshon për elementë të krimit kibernetikë; |
| Neni 14: Në shkronjën “d” të përcaktohet akti përmes së cilit do të miratohen formati i raporteve të incidenteve dhe afatet përkatëse. | MD | Pranuar | Reflektuar |
| Neni 14, shkronja “dh” pikes1:  Theksojmë se Rregullorja ne fuqi e miratuar dhe e ndryshuar në vitin 2022 nuk e ka të mirë përcaktuar këtë procedurë, mendojmë që duhet të bëhet një referencë me e saktë përkundrejt rregullores. | Shoqata Shqiptare e Bankave | Pranuar | Është riformuluar duke : Ruan loge për një periudhë të përcakuar në rregulloren e miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit. |
| Në shkronjën “ë” është i paqartë koncepti i sigurimit të stafit të mjaftueshëm dhe të kualifikuar nga ana e CSIRT pranë operatorëve, në kushtet kur referuar përkufizimit të dhënë, këto të fundit në thelb janë vetë ekipi i vendosur pranë operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit. | MD | Pranuar | Është hequr. |
| Neni 14 pika 1 shkronja f): *“Raporton pranë CSIRT–it kombëtar dhe CSIRT-it sektorial çdo incident të sigurisë kibernetike të ndodhur në infrastrukturat e tyre, i cili përcakton impaktin e incidentit të sigurisë kibernetike”.* Ky parashikimduket përsëritje e pikës (d) të këtij neni. Raportimi mendojmë se mund të bëhet edhe vetëm tek njeri prej tyre duke qenë se kanë detyrimin e komunikimit mes tyre. Në lidhje me impaktin e incidentit kuptojmë se këtë e përcakton CSIRT i operatorit (neni14, pika 1.b). | BSH | Refuzuar | Eshte per efekt bashkëpunimi koordinimi. Nuk ka përsëritje. |
| Nnei 14 pika f) Raporton pranë CSIRT–it kombëtar dhe CSIRT-it sektorial çdo incident të sigurisë kibernetike të ndodhur në infrastrukturat e tyre, i cili përcakton impaktin e incidentit të sigurisë kibernetike.  **Koment AAB –** Mendojmë se duhet të kemi një raportim të vetëm. Tek CSIRT sektorial, kur ky ekziston, dhe më tej ky e përcjell të CSIRT kombëtar, ose direkt të CSIRT kombëtar. Raportimet e shumta për të njëjtin incident ngarkojnë dhe marrim kohë të vyer. | Shoqata Shqiptare e Bankave | Refuzuar | Eshte per efekt bashkëpunimi koordinimi. Nuk ka përsëritje |
| Neni 14: Parashikimi i pikës 2 është tërësisht i paqartë dhe nuk kuptohet arsyeja e sanksionimit të këtij detyrimi, për sa kohë projektligji ka parashikuar ngritjen e CSIRT pranë operatorëve sipas përcaktimeve të vetë këtij ligji. | MD | Refuzuar | Është i nevojshëm si parashikim, pasi secili ka detyrat e përcaktuara si dhe eshte e rëndësishme forcimi i bashkëpunimit dhe koordinimit midis tyre. |
| Neni 14 pika 2: *“Operatori i infrastrukturës kritike të informacionit ngre në strukturën e vet CSIRT-in, ekipin përgjegjës për incidentet e sigurisë kibernetike....”*. Kjo pikë vlen vetëm për operatorët e infrastrukturës kritike të informacionit, apo edhe për operatorët e infrastrukturës së rëndësishme të informacionit, nëse po do të duhet të dali qartë. | BSH | Pranuar | Eshte bere riformulimi dhe përcaktimet përkatëse lidhur CSIRT-et (neni 15 i projektligjit : **.** Subjektet përgjegjëse për ofrimin e shërbimeve sipas përcaktimeve të bëra në nenin 11 të këtij ligji, ngrenë në strukturën e vet CSIRT-in sektorial, përgjegjës për incidentet e sigurisë kibernetike.  2. Operatori i infrastrukturës kritike dhe operatori i infrastrukturës së rëndësishme të informacionit ngre në strukturën e vet ekipin e përgjigjes ndaj incidenteve të sigurisë kibernetike, CSIRT-in....) |
| Neni 14 pika 2: Operatori i infrastrukturës kritike të informacionit ngre në strukturën e vet CSIRT-in, ekipin përgjegjës për incidentet e sigurisë kibernetike, që për shkak të rëndësisë të ketë një ekip me të paktën 3 (tre) persona, ku njëri prej tyre të jetë i trajnuar për qeverisje të sigurisë kibernetike.  **Koment AAB –** Të qartësohet nëse kjo strukturë duhet të jetë e dedikuar për trajtimin e incidenteve të sigurisë kibernetike, si dhe të qartësohen aftësitë dhe shkollimi i nevojshëm për të 3 pjesëtarët e detyrueshëm. | Shoqata Shqiptare e Bankave | Refuzuar | Ky përcaktim eshte hequr. |
| **XVII. Mbi përmbajtjen e nenit 15** | Neni 15 pika 3: Çdo ndryshim në të dhënat e pikave të kontaktit i komunikohen zyrtarisht CSIRT-it kombëtar dhe CSIRT-it sektorial, nga operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit brenda 7 ditëve kalendarike.  **Koment AAB** – Ky afat duket i shkurtër, konsideruar që për mosrespektimin e tij, gjoba varion nga 200.000 në 400.000 lekë. | Shoqata Shqiptare e Bankave | Refuzuar | Afati është vendosur në përputhje me rëndësinë që ky përcaktim paraqet. |
| **XVIII. Mbi përmbajtjen e nenit 16** | Neni 16 pika 2: Operatorët e infrastrukturës kritike dhe të rëndësishme të informacionit përdorin produkte të certifikuara gjatë ngritjes së infrastrukturave të tyre të informacionit.  **Koment AAB** – Duhet të përcaktohet së çfarë kuptohet me “produkte të certifikuara” në kuptimin e kësaj pike, si dhe është e paqartë se nga cili autoritet duhet të jenë të certifikuara këto produkte. Si edhe të parashikohet çfarë duhet bërë me infrastrukturat e ngritura para këtij ligji. | Shoqata Shqiptare e Bankave | Refuzuar | Eshte hequr si përcaktim. Lidhet me skemën e certifikimit te sigurisë kibernetike. |
| Neni 16 pika 5, të riformulohet me përmbajtje si vijon: “Masat e sigurisë kibernetike kanë për qëllim evidentimin, zbulimin parandalimin dhe minimizimin e efektit të incidentit në sigurinë e rrjeteve dhe sistemeve të informacionit”. | MB | Refuzuar | Formulimi është i qartë duke iu përgjigjur funksionit të masave të sigurisë: “Masat e sigurisë kibernetike kanë për qëllim parandalimin dhe minimizimin e efektit të incidentit në sigurinë e rrjeteve dhe sistemeve të informacionit.” |
| **XIX. Mbi përmbajtjen e nenit 17** | Në nenin 17, pika 2, ku përcaktohet se gjatë implementimit të masave organizative dhe teknike për menaxhimin e riskut operatorët marrin në konsideratë disa elementë, sugjerojmë shtimin e shkronjës “dh” me përmbajtje “Raportimin në kohë reale”. | MB | Refuzuar | Nuk përfshihet si element përbërës sugjerimi i dhënë. |
| Neni 17 pika 1 shkronja a): “Përcaktimin e riskut të incidentit” – fjala përcaktim sugjerojmë të bëhet vlerësim. Neni 17 pika 2 shkronja a) Sigurinë e sistemeve dhe shërbimeve; - sugjerojmë te shtohet shprehja “dhe te dhënave”. | BSH | Refuzuar | Dispozita ështe e qartë. Pika 2 është riformuluar. |
| **XX.Mbi përmbajtjen e nenit 18** | Neni 18 pika 1: “*Në rast të një incidenti kibernetik apo kërcënimi të mundshëm, aplikohen masat e sigurisë kibernetike të kategorizuara si më poshtë....*” – Mendojmë që kjo dispozitë të shprehet me qarte pasi duket kufizuese, ne fakt masat e listuara janë edhe parandaluese edhe reaguese dhe aplikohen jo ne rast te incidentit por përpara ndodhjes se tyre. | BSH | Refuzuar | Ligji jep parashikime të përgjithshme. Jepen tre kategoritë e këtyre masave a)Masa paralajmëruese;  b)Kundërmasat;  c)Masa mbrojtëse të natyrës së përgjithshme |
| **XXI. Mbi përmbajtjen e nenit 19** | Neni 19 pika 1, të riformulohet si vijon: “Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, marrin masa për të evidentuar, zbuluar, parandaluar dhe minimizuar ndikimin e rreziqeve dhe incidenteve të sigurisë kibernetike në infrastrukturat e tyre të informacionit” | MB | Refuzuar | Dispozita e përcakton qartë funksionin: parandalim+ minimizim  “Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, marrin masa për të parandaluar dhe minimizuar ndikimin e rreziqeve dhe incidenteve të sigurisë kibernetike në infrastrukturat e tyre të informacioni.” |
| **Neni 19, pika 3:** Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, raportojnë të gjitha llojet e incidenteve të sigurisë kibernetike pranë CSIRT-it kombëtar dhe CSIRT-it sektorial, brenda 4 orëve, nga koha e ndodhjes së incidentit.  **Koment AAB** – Së pari propozojmë që shprehja e mësipërme “koha e ndodhjes së incidentit” të ndryshohet në “koha e identifikimit të incidentit” - kjo pasi nga fillimi i incidentit deri në detektim koha mesatare është përafërsisht 210 ditë’.  Propozojmë që në fund të fjalizë të shtohet: “.... e ndodhjes se incidentit kibernetik kritik.”  Duhet të dakordësohet /përcaktohet saktësisht çfarë konsiderohet një incident për t’u raportuar. Sipas përshkrimit të termave incident konsiderohej “cenimi i sigurisë së shërbimeve / infrastrukturës duke sjell efekt negativ”.  Koha e raportimit 4 orë mund të jetë vetëm për incidentet kritike, ky parashikim duhet të përputhet me kohët e reagimit edhe nga ekipet përgjegjës ndaj incidenteve pranë operatoreve apo pranë CIRT sektorial. Gjithashtu duhet të parashikohen fillimisht forma të shkurtuara raportimi kur koha është aq e shkurtër (4 orë), ky afat mund të rishikohet me qëllim zgjatjen e tij. Mendojmë se parashikimi i afateve duhet të rregullohet në aktet nënligjore. | Shoqata Shqiptare e Bankave | Pranuar pjesërisht | Pika është riformuluar duke vendosur: nga momenti i identifikimit të incidentit.  Referuar pjesës së përcaktimit të incidentit kritik është refuzuar, afati i përgjithshëm 4 orë është vendosur në përputhje me rregulloren e përshakallëzimit të incidenteve. Lidhur me parashikimin e afateve me akte nënligjore pika 8 e këtij neni përcakton:  8. Llojet dhe kategoritë e incidenteve të sigurisë kibernetike, të cilat prekin sistemet dhe rrjetet e informacionit, formatin, elementët e raportimit, afatet e raportimit dhe mënyrën e dokumentimit të incidenteve kibernetike, përcaktohen me rregullore të miratuar me urdhër të Drejtorit të Përgjithshëm të Autoriteti |
| Pika 4: Përveç listimit të parametrave duhet të përcaktohet dhe matrica e ndërlidhjes së tyre dhe se si përcaktohet saktësisht rëndësia duke nisur prej tyre. Nevojitet të përcaktohet me akte nënligjore. Propozojmë që të shtohet/referohet ne nenin 37 “Aktet nenligjore” | Shoqata Shqiptare e Bankave | Refuzuar | Nuk shihet e nevojshme përcaktimi i matrices së ndërlidhes së tyre. Për më tepër që përcaktimet e nevojshme do të jepen në rregulloren për incidentet ( reference pika 8 e po këtij neni) |
| Lidhur me nenin 19, pika 5 të projektligjit, të jepen sqarime mbi natyrën e marrëveshjeve që synohen të lidhen, duke mbajtur në konsideratë që të dhënat personale gëzojnë mbrojtje kushtetuese dhe si të tilla, në rast shkëmbimi të këtyre të dhënave, këto marrëveshje duhet t’i nënshtrohen procedurës së ratifikimit sipas ligjit nr. 43/2016, “Për marrëveshjet ndërkombëtare në Republikën e Shqipërisë”. Ky koment të mbahet në konsideratë edhe për nenin 28, pika 1, duke konkretizuar referimin e kryer “*në përputhje me legjislacionin në fuqi*”. | MD | Pranuar pjesërisht | Është bërë riformulimi duke bërë referencë në legjislacionin në fuqi për marrëveshjet ndërkombëtare. Gjithashtu janë shtuar elmement ne përputhje me NIS 2 Direktiven, referuar shkëmbimit te te dhënave. |
| Në nenin 19, pika 5, ku përcaktohet se “Autoriteti vendos në dispozicion të organizmave ndërkombëtare në fushën e sigurisë kibernetike, të dhënat e administruara në lidhje me incidentet e sigurisë kibernetike, me qëllim trajtimin dhe zgjidhjen e tyre”, sugjerojmë përfshirjen e parashikimeve për vënien në dispozicion të të dhënave, edhe institucioneve ligjzbatuese kombëtare. | MB | Refuzuar | Ligji jep parashikime të përgjithshme. Në çdo rast garantohet bashkëpunim, konfidencialiteti, mbrojtja e të dhënave personale. Jane bere parashikime referuar edhe bashkepunimit me institucionet ligjzbatuese kombetare. |
| **XXII. Mbi përmbajtjen e nenit 21** | Nnei 21 pika 1: CSIRT-i kombëtar informon publikun me transparencë për incidentet e ndodhura në infrastrukturat kritike dhe të rëndësishme të informacionit, kur ky informim është i nevojshëm, duke ruajtur konfidencialitetin e të dhënave të incidentit.  Koment AAB – Sipas kësaj pike duket se CSIRT mund të informojë publikun për incidentet e ndodhura në infrastrukturën e bankës por ky komunikim duhet të jetë jashtë ndikimit të bankës. Edhe pse aty thuhet duke ruajtur konfidencialitetin e të dhënave, mendojmë se duhet përcaktuar më qartë se çfarë duhet dhe mundet CSIRT të komunikoje pa cënuar bankën. Nevojitet të qartësohet se si do të përcaktohet nevoja për informim? A përfshihet në të dhënat konfidenciale të incidentit, emri apo të dhënat identifikuese të operatorit të infrastrukturës. | Shoqata Shqiptare e Bankave | Refuzuar | Ky përcaktim nuk mund të jepet në ligj. Përcaktimet e bëra janë çdo herë në respektim të parimit të mbrojtjes së të dhënave personale si dhe konfidencialitetit. |
| Neni 21 pika 2: Informimi i publikut mbështetet në një procedurë komunikimi të miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit.  **Koment AAB** –Kjo procedure duhet të dakorësohet dhe nga Operatorët, veçanërisht bankat pasi për shkak të ndjeshmërisë impakti mund të jetë i paparashikueshëm.  Theksojmë se në të dyja parashikimet e pikës 1 dhe 2 më lart informimi i publikut për incidente që lidhen me një operator specifik privat duhet të menaxhohet nga vetë operatoret nëpërmjet departamenteve të specializuara për shkak të impaktit mbi operatorin si edhe në përputhje me detyrimet ligjore për informimin e klientëve të tyre dhe publikut. | Shoqata Shqiptare e Bankave | Refuzuar | I referohemi atyre situatave kur informimi i publikut shihet i nevojshëm. Procedura e komunikimit do të përcaktohet me urdher te Drejtorit te Përgjithshëm të Autoriteti, duke përcaktuar edhe elementët që do të përmbajë. |
| **XXIII. Mbi përmbajtjen e nenit 22** | Neni 21 pika 1: Nëpunësit e Autoritetit që marrin pjesë në zgjidhjen e incidentit kibernetik, janë të detyruar të ruajnë konfidencialitetin e plotë, për të gjitha të dhënat e përpunuara gjatë procedurës së zgjidhjes së tij.  **Koment AAB** – Ky detyrim duhet te vleje për te gjithë institucionin, jo vetëm për disa punonjës të tij. | Shoqata Shqiptare e Bankave | Refuzuar | Përcaktimi është i qartë. Të gjithë ata që kanë marrë pjesë në zgjidhjen e incidentit kibernetik, janë të detyruar të ruajnë konfidencialitetin e plotë…. |
| Në nenin 22, pika 2, të përcaktohen se cilat janë rastet e përjashtimit nga detyrimi i konfidencialitetit pas ndërprerjes së marrëdhënies së punës. | MD | Refuzuar | Ligji bën parashikime të përgjithshme. Përjashtimet i referohen parashikimeve ligjore në fuqi. |
| Neni 22 pika 3: Konfidencialiteti i të dhënave të incidentit kibernetik trajtohet sipas legjislacionit në fuqi për mbrojtjen e të dhënave personale.  **Koment AAB** – Nëse një incident kibernetik ndodh pranë një institucioni bankar, ligji për mbrojtjen e të dhënave personale mbron individin por jo personin juridik. Si do mbrohet institucioni?  Sugjerojmë që përpara miratimit të këtij projektligji të merret dhe opinioni i Komisionerit për Mbrojtjen e të Dhënave Personale. Ky opinion tu bëhet i ditur dhe vetë subjekteve te interesuara, në rastin tonë bankave.  Bazuar në ligjin “Për mbrojtjen e te dhënave personale”, Autoriteti duhet të ketë marrëveshje me OIKR për përpunimin e tyre. | Shoqata Shqiptare e Bankave | Refuzuar | Komisioneri ne përgjigjen e dërguar lidhur me projektligjin në fjalë ku janë shprehur se projektlgji në tërësi implementon rregullat dhe parimet e ligjit nr.9887 datë 10.03.2008 “Për mbrojtjen e të dhënave personale”, i ndryshuar. Gjithashtu një nga parimet bazë të projektligjit është ai I mbrojtjes së të dhënave personale. |
| **XXIV. Mbi përmbajtjen e nenit 23**  **Kriza Kibernetike** | Neni 23 pika 1: “*Gjendja e krizës kibernetike shpallet me vendim të Këshillit të Ministrave, me propozimin e Kryeministrit. Vendimi për shpalljen e gjendjes së krizës kibernetike njoftohet në media” –* Vlerësojmë se kjo pikë duhet te përmbajë disa ketë kritere/kushte të përcaktuara në ligj. | BSH | Pranuar | Neni pë krizën kibernetike ( referenca neni 28) është riformuluar |
| **XXV. Mbi përmbajtjen e nenit 24** | Të rishikohet në tërësi neni 24, me qëllim përkufizimin e saktë të CERT-it, duke iu referuar edhe përkufizimit të dhënë në nenin 4 të këtij projektligji, si dhe komentit tonë të dhënë më sipër lidhur me atashimin e këtij Ekipi, duke shmangur fjalët të cilat në thelb nuk vendosin rregulla materiale ligjore. Nga ana tjetër, përbërja e këtij Ekipi është e paqartë pasi nuk kuptohet mënyra e përzgjedhjes dhe emërimit të tyre. | MD | Pranuar pjesërisht | Riformuluar |
| Në nenin 24, pika 2, ku përcaktohet se “me qëllim trajtimin në kohë dhe me efiçencë të incidenteve dhe kërcënimeve gjatë krizës kibernetike përfshihen ekspertët më të mirë të fushës”, në drejtim të qartësisë së normës, sugjerojmë të rishikohet togfjalëshi “më të mirë”. | MB | Pranuar | Është marrë në konsideratë |
| **Koment AAB –** Sugjerojmë që në hartimin e planit të masave te mbahet parasysh konfidencialiteti i të dhënave duke qenë se në CERT marrin pjesë persona nga sektorë të ndryshëm. Gjithashtu propozojmë që Struktura duhet të ketë një bërthamë të përcaktuar të mos i lihet tërësisht mënyrës ad-hoc, kjo për tu marrë në konsideratë në vendimin e Këshillit të Ministrave | Shoqata Shqiptare e Bankave | Pranuar pjesërisht | Është shtuar konfidencialiteti. Lidhur me faktin që struktura mos të jetë ad hoc, është përcaktuar si e tillë pasi do të jetë vetëm në raste krize dhe emergjencë kiberntike. |
| **XXVI. Mbi përmbajtjen e nenit 25** | Neni 25 pika c): zhvillon skanime të rrjeteve dhe sistemeve të operatoreve, për efekt të kontrollit të masave të sigurisë në lidhje me vulnerabilitete të mundshme, duke siguruar transparencë të procesit dhe garantuar konfidencialitetin e | Shoqata Shqiptare e Bankave | Refuzuar | Ligji jep parashikime të përgjithshme. Nuk mund te bëhet specifikisht për një sektor apo për disa. |
| informacionit. Parashikimi i më sipërm është shumë i përgjithshëm. Sugjerojmë që të qartësohet çfarë skanimesh kryhen, metodologjia, etj.  Me qëllim reduktimin e riskut kibernetik dhe vijueshmërinë e biznesit në sektorin bankar, në parashikimin e më sipërm duhet të shtohet një paragraf i cili të saktësojë/specifikojë që vetëm për operatorët bankar qëllimi i skanimeve të limitohet në infrastrukturën e jashtme dhe që këta operatorë duhet të njoftohen paraprakisht si dhe të garantohet që nuk do të ketë impakt në sistemet e shërbimit të operatorit.  Janë përcaktime te përgjithshme. Sugjerojmë që të qartësohet çfarë skanimesh kryhen, metodologjia, etj |
| Neni 25, pika 2, shkronja ç:  Të shtohet : *në përputhje me ligjin dhe aktet nënligjore.* | Shoqata Shqiptare e Bankave. | Refuzuar | Përcaktimi është i qartë. |
| Neni 25, pika 2, shkronja d:  Duhet përcaktuar /**parashikuar** që këto informacione dhe të dhëna merren nga subjektet, pas një kërkese të argumentuar me shkrim. | Shoqata Shqiptare e Bankave | Refuzuar | Nuk shihet e nevojshme marrja e konfirmimit me shkrim për ushtrimin e funksioneve përkatëse mbikëqyrëse. |
| **XXVII. Mbi përmbajtjen e nenit 26** | Në nenin 26, sugjerojmë që:  pika 1 të riformulohet sipas përmbajtjes: “*1. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të raportojnë të gjitha infrastrukturat e tyre kritike dhe të rëndësishme të informacionit pranë Autoritetit*.” | AKSHI | Pranuar pjeserisht | *Eshte riformuluar*  *“Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit kanë detyrimin të raportojnë të gjitha infrastrukturat e tyre kritike, te rëndësishme, si dhe të gjithë infrastrukturat e tjera që ndërveprojnë me to pranë Autoritetit.* |
| **Neni 26 pika 1**: Duhet të saktësohet çfarë kuptohet me “infrastrukturë infromacioni” dhe pasi të kryhet kjo duhet dhe të parashikohen mënyra e ruajtjes së këtij informacioni tej mase sensitiv, veçanërisht për bankën. Propozojmë që parashikimi duhet të limitohet vetëm me ndarjen e informacionit vetëm te infrastruktura që i klasifikon këtë operatore si infrastrukture kritike, e konsiderojmë të nevojshëm me qëllim reduktimin e riskut kibernetik dhe vijueshmërinë e biznesit. Sugjerimi është të ketë raportim pa brand pasi cënimi i këtij informacioni ekspozon bankën në mënyrë të lartë. | Shoqata Shqiptare e Bankave | Refuzuar | Përcaktimi është bërë në nenin 5, pika 13 dhe 14. Lidhur me mënyrën e ruajtjes së këtij informacioni nuk mund të jepet në ligj. Gjithsesi projektligji zbaton parimin e mbrojtes së të dhënave personale si dhe parimin e konfidencialitetit. |
| Pika 2, e nenit 26, të riformulohet sipas përmbajtjes: *“2. Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, në kuadër të aktivitetit mbikqyrës, i ofrojnë CSIRT-it kombëtar akses të drejtpërdrejtë në ambientet e infrastrukturave dhe sistemet e tyre të informacionit, në zbatim të procedurave të sigurisë te çdo operatori të këtyre infrastrukturave, të cilat janë të lidhura me shërbimet e ofruara prej tyre.”* | AKSHI | Pranuar | Reflektuar |
| Neni 26, pika 2:  Në këtë pikë duhet të shtohet ***“vetëm akseset  e nevojshme për të ushtruar detyrat e mbikëqyrjes dhe sipas aplikueshmerisë”,*** pra nevojite që parashikimet të limitohen vetëm me ndarjen e informacionit të nevojshëm për të reduktuar riskun kibernetik dhe vijueshmërinë e biznesit.  Parashikimi nuk është në linje me Direktivën 2016/1148. | Shoqata Shqiptare e Bankave | Refuzuar | Reference neni 31: Kjo pike është riformuluar: “5.Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, në kuadër të aktivitetit mbikqyrës, i ofrojnë CSIRT-it kombëtar akses të drejtpërdrejtë në ambientet dhe sistemet e tyre të informacionit, në zbatim të procedurave të sigurisë të çdo operatori të këtyre infrastrukturave, të cilat janë të lidhura me shërbimet e ofruara prej tyre.” |
| Neni 26, pika 4:  të riformulohet në tërësi, pasi nuk kuptohet nëse kemi të bëjmë me një raport të vetëm apo me tri raporte të ndryshme, si dhe të jepet një përkufizim për Organizmin e Vlerësimit të Konformitetit. | MD | Pranuar | Riformuluar  Raport i vlerësimit të konformitetit.( raport lidhur me implementimi e masave te sigurisë kibernetike)  Neni 5 pika 23 Organ i vlerësimit te konformitetit per sigurinë kibernetike -perkufizimi |
| Neni 26, pika 4:  Duhet të shpjegohet pak me gjerë/të saktësohet për çfarë testimi, vlerësimi dhe konformiteti bëhet fjalë dhe cilat janë Organizmat e Testimit dhe Konfirmimit? | Shoqata Shqiptare e Bankave | Refuzuar | Është bërë unifikim terminologjie “organ i vlerësimit të konformitetit per sigurinë kibernetike”  si dhe gjithashtu shpjegimi është bërë tek përkufizimet. Duke qenë se janë në kuadër të skemës së certifikimit të sigurisë kibernetike është përcaktuar me akt nënligjor tarifa dhe procedura e regjistrimit te këtyre organeve. |
| **XXVIII. Mbi përmbajtjen e nenit 27** | Për bashkëpunimin në nivel kombëtar parashikuar në nenin 27, vlerësojmë se duhet të ketë një pikë të veçantë për bashkëpunimin me AKEP që mbulon një spektër të gjerë të rregullimit në TIK/komunikimet elektronike përfshirë rrjetet e komunikimeve fikse, të lëvizshme, satelitore etj. | MIE | Pranuar | Reflektuar |
| Në pikën 3, të nenit 27 të projektligjit, sugjerojmë të shtohet gërma “c”, me përmbajtje:  *“Autoriteti bashkëpunon me autoritetin kombëtar përgjegjës për mbrojtjen e të dhënave personale, në rastet kur trajtohen incidente të cilat rezultojnë në përhapje të paligjshme të të dhënave personale”.*  Sugjerimi bazohet gjithashtu edhe në referencë të parashikimit të pikës 4, të nenit 16 të Direktivës (BE) 2016/1148 të Parlamentit Evropian dhe Këshillit. | KDIMDHP | Pranuar | Reflektuar |
| Neni 27, paragrafi 3, a)- shton gjuhën e theksuar:  "Bashkëpunon ngushtë me Policinë e Shtetit dhe çdo prokurori përkatëse në rastet kur, nga informacionet e siguruara për efekt të këtij ligji, dyshon në elementë të krimit kibernetik ose terrorizmit." | Ambasada Amerikane | Pranuar | Rifromuluar dhe pasqyruar |
| Në nenin 27, pika 3, shkronja “a”, ku përcaktohet se : “Autoriteti bashkëpunon ngushtë me Policinë e Shtetit në rastet kur nga informacioni i siguruar për efekt të këtij ligji, dyshon për elementë të krimit kibernetik”, sugjerojmë riformulimin e kësaj pike mbi bazën e kategorizimit të incidenteve. | MB | Pranuar pjeserisht | Riformuluar  Neni 31, pika 3 shkronja a) bashkëpunon me Policinë e Shtetit dhe institucionet përkatëse në rastet kur nga informacioni i siguruar për efekt të këtij ligji, dyshon për elementë të krimit kibernetikë ose veprave të tjera penale të lidhura me to; |
| **XXIX. Mbi skemën e certifikimit të sigurisë kibernetike.** | Në nenin 27, pika 7, është i paqartë momenti i hyrjes në fuqi të skemës së certifikimit të sigurisë kibernetike. | MD | Pranuar | Skema e certifikimit të sigurisë kibernetike do të jetë në përputhje me skemat e BE –së. Kjo skemë do të hyjë në fuqi kur të miratohe ë BE, duke qenë se aktualisht nuk ka një të tillë.Rregullimi ne përcaktimin e akteve nenligjore. |
| Nnei 29 pika 5: Në këtë skemë duhet të përfshihen vetëm sistemet kritike dhe të rëndësishme. Është e pamundur që të certifikohet çdo shërbim dhe çdo proces, konsideruar këtu praktikat ndërkombëtare. | Shoqata Shqiptare e Bankave | Refuzuar | Skema e certifikimit të sigurisë kibernetike është tërësia e rregullave, kërkesave teknike, standardeve dhe procedurave që zbatohen për certifikimin ose vlerësimin e konformitetit të produkteve, shërbimeve dhe proceseve që lidhen me sigurinë kibernetike në TIK. |
| Në pikën 1 të nenit 29, sugjerojmë të duhet shtohet miratimi me vendim të Këshillit të Ministrave, sikurse parashikohet në nenin 30. | MIE | Refuzuar | Është bërë përcaktimi në nenin 30: “miratimi me vendim të Këshillit të Ministrave”. ( referenca ne projektin aktual 41) |
| Referuar nenit 30 në raport me nenin 4, pika 32 të këtij projektligji, të jepen sqarime nëse skema e certifikimit të sigurisë kibernetike është e njëjtë me skemën kombëtare të certifikimit të sigurisë kibernetike, dhe nëse po, të shmangen kontradiktat pasi nga njëra anë, parashikohet miratimi i skemës nga Autoriteti dhe nga ana tjetër, miratimi i tyre nga Këshilli i Ministrave | MD | Refuzuar | Është e njëjta. Përkufizimi sqaron skemën e certifikimit të sigurisë kibernetike, ndërsa neni 30 ( 41 projekti aktual) përcaktimi me akt nënligjor duke qenë se kjo skemë nuk është miratuar ende në BE. |
| **XXX. Mbi përmbajtjen e nenit 31: Masat Korrigjuese** | Neni 31, pika 1:  Propozojmë që në fund të fjalisë të shtohet: *“...përkatëse* ***sipas aplikueshmërisë****.”*  . | Shoqata Shqiptare e Bankave | Refuzuar | Koncepti është që si infrastrukturë ke detyrime. Konstatimet qe do te bëhen janë ato qe ti ke detyrime ti përmbushësh sipas parashikimeve të bëra në ligj Pjesa e aplikueshmërisë është gjë tjetër. |
| **XXXI. Mbi përmbajtjen e nenit 32 Kundërvajtjet administrative** | Pika d) Gjithashtu dhe sa i përket nenit te referuar në këtë pikë, parashikimi i nenit 31, pika 3, nuk nxjerr qarte nëse operatoret duhet të njoftojnë autoritetin sa herë që marrin masa korrigjuese? Apo Autoriteti do auditojë periodikisht masat korrigjuese? | Shoqata Shqiptare e Bankave | Refuzuar | **42 pika**  përcakton se Operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, janë të detyruar të zbatojnë masat korrigjuese të lëna nga Autoriteti, si dhe të raportojnë mbi implementimin e tyre. |
| **XXXII. Mbi përmbajtjen e nenit 33** | Nneri 33: Rritja e gjobës është eksponenciale me 12 herë më shumë. Mendojmë se duhet të ulet ky penalitet. | Shoqata Shqiptare e Bankave | Refuzuar | Janë vendosur në kuadër të forcimit të zbatimit të dispozitave. Siguria kibernetike paraqet një rëndësi të veçantë dhe është e nevojshme zbatimi me përpikmëri i kuadrit ligjor me qëllim forcimin e kësaj të fundit. |
| **XXXIII. Pezullimi i ushtrimit të aktivitetit** | Shprehemi kundra këtij parshikimi.  Duhet të konsiderohet dhe parametri kohë në këtë përcaktim. Pra 3 masa brenda një viti mund të përbejnë premisat për diçka të tillë.  Gjithashtu ne ligj duhet të parashikohet/përcaktohet afati për pezullimin e aktivitetit (nuk mund të jetë pa afat). Nje kompetence e tille e autoritetit ka nevoje per me shume parashkime ligjore. | Shoqata Shqiptare e Bankave | Pranuar pjeserisht | Është riformuluar duke dhene me shume përcaktime. Lidhur me masat janë vendosur 2 te tilla. |
| Pezullimi i ushtrimit të aktivitetit, sikurse është parashikuar në nenin 34 është i paqartë sesi do të zbatohet, pasi për rrjete të ndryshme, licensimi/mbikqyrja e veprimtarisë/masat shtrënguese bëhen nga autoritete të ndryshme: rrjetet e komunikimeve elektronike - AKEP, rrjetet e energjisë - ERE, sistemi i financave/bankave - BSH. Në këto kushte, vlerësojmë se është e domosdoshme të ketë një parashikim për koordinim midis instiutioneve dhe procedurat që duhen ndjekur nga autoriteti si dhe të përcaktohet nëse pezullimi do të bëhet për çdo shkelje apo vetëm për shkelje serioze | MIE | Pranuar | Është riformuluar. |
| Në lidhje me parashikimin e nenit 34 të projektligjit, sugjerohet që të vendoset një afat për pezullimin e ushtrimit të aktivitetit, në përputhje me natyrën e kësaj mase, e cila nuk mund të jetë e pakufizuar në kohë, me qëllim shmangien e abuzimeve të mundshme gjatë zbatimit të kësaj dispozite në të ardhmen. | MD | Pranuar | Riformuluar |
| Neni 34 i projektligjit parashikon “Pezullimi i ushtrimit të aktivitetit”.  Pezullimi i ushtrimit të aktivitetit mendojmë që bëhet nga autoriteti i cili i ka dhënë licencën për ushtrimin e aktivitetit subjektit përkatës, në rastet kur kjo është e aplikueshme Në këtë rast, mund të parashikohet bashkëpunimi i CSIRT kombëtar me autoritetet mbikëqyrëse të fushave të caktuara si dhe me CSIRT sektorial për marrjen e masës së pezullimit të aktivitetit të subjektit.  Për shembull nëse do të marrim një tjetër ligj për referencë, ne nenin 26 të Ligji nr. 9917, datë 19.05.2008 “Për Parandalimin e Pastrimit të Parave dhe Financimin e Terrorizmit”, i ndryshuar, Autoriteti i propozon subjekteve mbikëqyrëse përkatëse (Banka e Shqipërisë në rastin tonë) kufizimin, pezullim apo revokimin e licencës.  Gjithashtu, nuk është e qartë nëse shprehja “...ndaj të cilit janë marrë më shumë se 3 (tre) masa administrative të një pas njëshme” nënkuptohet që Autoriteti mund të ketë marrë më parë masa korrigjuese ( neni 28) dhe/ose sanksione administrative (neni 30). Sugjerojmë të dali qartë në ligj përshkallëzimi i masave deri në propozimin për pezullimin e aktivitetit. | BSH | Pranuar | Riformuluar |
| **XXXIV. Mbi përmbajten e nenit 35** | Në nenin 35, duhet saktësuar dhe plotësuar se ndaj ndaj kujt bëhet ankim administrativ: vendimit të AKCESK, urdhrit të Drejtorit të AKCESK, të inspektorëve, ankim për gjobën, ankim për pezullim aktiviteti etj | MIE | Refuzuar | Referenca eshte bere ne ligjin per kundravajtjet administrative. |
| Neni 35 i projektligjit parashikon “Ankimin administrativ”. Sugjerojmë zgjerimin e kësaj dispozite duke vendosur disa rregullave bazë në lidhje me ankimin administrativ në ligj. Për shembull, kur lind e drejta për personat, afatin kohor, ku drejtohet subjekti etj. | BSH | Refuzuar | Referencë: Ligji për kundravajtjet administrative. |
| **XXXV. Dispozitat kalimtare** | Në nenin 10, sugjerohet që pika 3 e tij të vendoset në kreun VIII, në dispozitat e fundit të këtij projektligji pasi përmban detyrime që kushtëzohen nga hyrja në fuqi e këtij projektligji e në vijim. | MD | Pranuar | Reflektuar |
| Pika 2, e nenit 39, të riformulohet si vijon:  “2. Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike vazhdon të ushtrojë veprimtarinë e tij si institucioni përgjegjës në fushën e sigurisë kibernetike, deri në riorganizimin e tij në përputhje me dispozitat e këtij ligji.” | DAP | Pranuar | Reflektuar |
| Neni 39 pika 2 i projektligjit përcakton se “Autoriteti Kombëtar për Certifikimin Elektronik dhe Sigurinë Kibernetike vazhdon të ushtrojë veprimtarinë e tij, pa ndërprerje, si institucioni përgjegjës në fushën e sigurisë kibernetike në përputhje me dispozitat e këtij ligji”.  Nëpërmjet kësaj dispozite kuptojmë se AKCESK do të jetë Autoriteti përgjegjës për Sigurinë Kibernetike në kuptim të këtij ligji. | BSH | Pranuar | Reflektuar |
| Ndërkohë, për të mos pasur problematika në lidhje me shtesën që aktualisht përfitojnë nëpunësit e AKCESK (në masën deri në 800.000 lekë) deri në miratimin e projektligjit të sipërcituar, e më pas të vendimit përkatës të Këshillit të Ministrave për këtë qëllim, sugjerojmë që në nenin 39, të projektligjit “Për sigurinë kibernetike” të shtohet pika 3, me përmbajtjen si vijon:  “3. Deri në miratimin e ligjit të posaçëm që përcakton kompetencat e caktimit të pagave, të trajtimeve të tjera financiare dhe të përfitimeve për të punësuarit në institucionet e administratës publike, Drejtori i Përgjithshëm dhe nëpunësit e njësive teknike të përmbajtjes së AKCESK-ut, do të vijojnë të përfitojnë shtesën aktuale për natyrë të veçantë pune.”. | DAP | Refuzuar | Lidhur me shtesën per natyre te vecante pune eshte bere ne neni 7 pika 5. |
| Neni 39 pika 1 i projektligjit përcakton se “subjektet përgjegjës në fushën e sigurisë kibernetike janë të detyruar të harmonizojnë veprimtarinë e tyre me dispozitat e këtij ligji brenda 24 muajve nga data e hyrjes në fuqi të këtij ligji”. Mbështetur dhe në komentet tona të mësipërme mbetet e pa qartë se cilat janë subjektet përkatëse për të cilat lind ky detyrim. | Banka e Shipërisë | Pranuar | Riformuluar neni 9( ne projektin aktual neni 11)  Sipas përcaktimeve të bëra në këtë projektligj me subjekte përgjegjëse në fushën e sigurisë kibernetike i referohemi operatorëve të infrastrukturave kritike dhe të rëndësishme të informacionit, subjektet e tjera përgjegjëse sipas përcaktim eve të nenit 9. |
| Lidhur me nenin 39 paragrafi 1. Subjektet përgjegjëse në fushën e sigurisë kibernetike janë të detyruar të harmonizojnë veprimtarinë e tyre me parashikimet e këtij ligji brenda 24 muajve nga data e hyrjes në fuqi e këtij ligji.  - Afati duket i vogël/i shkurtër, duke marrë parasysh që në shumë pika aktet nënligjore do të përcaktoheshin 6 muaj pas daljes së ligjit apo deri në një vit, rrjedhimisht afati efektiv do jetë 1 vit, çka është kohë e pamjaftueshme. | Shoqata Shqiptare e Bankave | Pranuar pjeserisht | Konsiderohet e mjaftueshme për harmonizimin e veprimtarisë.  Gjithashtu lidhur me nxjerrjen e akteve nenligjore dispozita eshte riformuluar. |
| **XXXVI. Sqarime** | Gjithashtu, sugjerohet të përcaktohen se cilat janë të dhënat që përmban regjistri elektronik i incidenteve, sikurse parashikohet në nenin 12, pika 1 të ligjit në fuqi. | MD | Refuzuar | Përcaktimi me akt nënligjor. Llojet dhe kategoritë e incidenteve të sigurisë kibernetike, të cilat prekin sistemet dhe rrjetet e informacionit, formatin, elementët e raportimit, afatet e raportimit,mënyrën e dokumentimit dhe regjistrimit të incidenteve kibernetike, përcaktohen me rregullore të miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit. ( referenca ne projektin aktual pika 8 e nenit 23) |
| Pika 7 e nenit 1 të Direktivës parashikon se çdo akt sektorial (lex specialis) që rregullon sigurinë kibernetike në një sektor të veçantë, do të zbatohet vetëm nëse respekton të paktën kërkesa ekuivalente me Direktivën (lex generalis). Projektligji shqiptar nuk e ka bërë një parashikim të tillë | Ministri i Shtetit dhe Kryenegociatori | Pranuar pjeserisht | Marre ne konsiderate. Pasqyruar ne projektligj ne nenin 24 ( sipas përcaktimeve ne nenin 4 te Direktives NIS2 ) |
| Në muajin Mars 2023, Departamenti i Administratës Publike ka dhënë mendim në lidhje me projektligjin “Për identifikimin elektronik dhe shërbimet e besuara”, ku përfshiheshin dispozita në lidhje me organizimin dhe funksionimin e Autoritetit të Sigurisë Kibernetike, projektligj që nga ana tjetër shfuqizon ligjin nr. 9880, datë 25/02/2008, “Për nënshkrimin elektronik”, të ndryshuar (ku aktualisht rregullohet krijimi i AKCESK-ut).  Për sa më sipër, sugjerojmë që të përfshihen në relacionin e projektligjit “Për sigurinë kibernetike”, sqarimet e nevojshme në lidhje me organizimin dhe funksionimin e autoritetit në projektligjin “Për identifikimin elektronik dhe shërbimet e besuara”. | DAP | Pranuar | Reflektuar. Përcaktuar në këtë ligj organizimi dhe funksionimi i Autoritetit Kombëtar për Sigurinë Kibernetike. |
| Gjithashtu, sqarojmë se me direktivën NIS2 kemi prekje të direktivës për komunikimet elektronike 2018/1972/EU pasi shfuqizohen nenet 40 dhe 41 të saj që praktikisht janë të përfshira në projektligjin “Për komunikimet elektronike”, në nenet 49-51. Ndërkohë që direktiva NIS2 nuk prek/cënon zbatimin e direktivës 2002/58/EC për privatësinë në komunikimet elektronike që aktualisht e kemi në ligjin nr. 9918/2008. Si rrjedhojë, projektligji për sigurinë kibernetike duhet të bëjë një harmonizim të mirë me ligjin për komunikimet elektronike dhe të qartësojë bashkëpunimin me AKEP dhe Ministrinë përgjegjëse për telekomunikacionet. | MIE | Pranuar | Është marrë në konsideratë. Gjithashtu Referuar shfuqizimit të Direktivës NIS1 sqarojmë se efektet e shfuqizimit të NIS 1 fillojnë nga 18 tetori 2024. Gjithsesi Autoriteti marrë në konsideratë rekomandimin e dhënë nga Komisioni Evropian ka punuar me Direktivën NIS 2. |
| Ldhur me parashikimin në nenin 11, shkronja “g”, në funksion të qartësisë vlerësojmë se, duhet të jepen shpjegimet përkatëse në relacionin shoqërues, se cilat do të konsiderohen si situata me risk të lartë dhe për cilat incidente kemi të bëjmë. | AKSHI | Refuzuar | Përcaktimi i bere eshte i qarte ndërsa referuar situata me risk te larte ato variojne rast pas rasti ne përputhje me vlerësimet e bëra.( reference ne projektin aktual neni 13 pika gj) |
| Në shkronjën “ç”, të nenit 13, të Kreut II, të projektaktit të propozuar parashikohet se: “Subjektet përgjegjëse për ofrimin e shërbimeve sipas përcaktimeve të bëra në nenin 9 të këtij ligji, duhet të kenë në strukturën e vet CSIRT-in sektorial, përgjegjës për incidentet e sigurisë kibernetike sipas fushës së përgjegjësis së tyre, i cili: ç ) ruan loge për një periudhë të përcaktuar sipas procedurës së caktuar me rregulloren e miratuar nga Drejtori i Përgjithshëm.”  Ndërkohë në pikën 15, të nenit 4, parshikohet se termi “Loge” ka kuptimin mesazh apo e dhënë mbi ngjarje lidhur me sigurinë kibernetike.  Lidhur me këto parashikime, vlerësojmë se duhet të qartësohet se kujt institucioni dhe cilit titullar institucioni i referoheni me Drejtor të Përgjithshëm. | AKSHI | Pranuar | Është bërë riformulimi i kësaj pike : “ruan loge të incidenteve të evidentuara ose të raportuara për një periudhë të përcaktuar në rregulloren e miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit’ |
| Neni 13 i projektit parashikon detyrat e CSIRT-ve sektoriale, dhe në shkronjën “ç” parashikohet: cit “*ruan loge për një periudhë të përcaktuar sipas procedurës së caktuar me rregulloren e miratuar nga CSIRT Kombëtar*”. Ruajtja e logeve çfarë nënkupton në këtë rast? Vlerësojmë se ashtë një proces qe kërkon investime dhe do te duhet te garantoje privatësi.  Në lidhje me këtë parashikim, nëse konsultojmë Direktivën e (BE) 2016/1148 “*Në lidhje me masat për një nivel të lartë të përbashkët të sigurisë së rrjeteve dhe sistemeve të informacionit në të gjithë bashkimin evropian*”, ku keni mbështetur dhe projektin nuk gjejmë kompetenca të tilla për autoritetet kombëtare apo CSIRT-et, pavarësisht organizimit që do të ketë shteti përkatës në lidhje me këto autoritete. Edhe Aneksi I i Direktivës (**Kërkesat dhe detyrat e CSIRT-ve**) nuk përmban asnjë reference ndaj kompetencave të mundshme që lidhen me ruajtje logesh.  Për sa më lart, jemi të mendimit se detyra e përcaktuar në shkronjën “ç” të nenit 13 nuk është në përputhje me Direktivën e BE-së. | BSH | Refuzuar | Projektligji bën parashikimin: “ruan loge të incidenteve të evidentuara ose të raportuara për një periudhë të përcaktuar në rregulloren e miratuar me urdhër të Drejtorit të Përgjithshëm të Autoritetit”  Gjithashtu projektligji përcakton qartë ruajtjen e të dhënave personale, konfidencialitetin si dhe parimin e neutralitetit te teknologjisë. |
| Neni 4 pika 4 i projektligjit “CSIRT Sektorial” - Si do jete skema e nënndarjeve te CSIRT, pasi CSIRT Qeveritar i bie te ketë prerje me te gjithë CSIRT sektoriale. Cili eshte roli dhe pergjegjesite e CSIRT Qeveritar, pasi nuk duken te jene trajtuar fare ne nenet e ketij akti. | BSH | Refuzuar | Ligji jep parashikme të përgjithshme. Nuk mund të përcaktohet këtu.Menyra e ngritjes, organizimit dhe funksionimit te tyre do te beheht me VKM ( reference ne projektin aktual neni 15 pika 5) |
| Neni 8 përcakton kompetencat e Autoritetit Kombëtar Për Sigurinë Kibernetike në lidhje me shkronjën a): “identifikon dhe klasifikon infrastrukturat kritike dhe të rëndësishme të informacionit” jemi të paqartë se nga cili institucion e bën identifikimin vetë autoriteti kombëtar siç parashikohet në këtë pikë apo vetë subjektet. | BSH | Refuzuar | Procesi I identifikimit është një process I cili bëhet nga Autoriteti në bashkëpunim me subjektet përgjegjëse për sigurinë kibernetike. Neni 10 i projektligjit pika 1 “Autoriteti, bashkërendon në vazhdimësi punën me subjektet e tjera përgjegjëse për sigurinë kibernetike, për identifikimin e infrastrukturave kritike dhe të rëndësishme të informacionit.” ( reference ne projektin aktual neni 12). Gjithashtu detajimi do beheht me akt nënligjor, metodologjia per iderntifikimin dhe klasifikimin e këtyre infrastrrukturave. |
| Neni 8 shkronja f): “... testimeve simuluese” - Çfarë nënkuptohet me testime simuluese. Nëse i referoheni Table top exercise nuk kemi kundërshtim, por ndërhyrje mbi sistemet do ishte e papranueshme. | BSH | Refuzuar | I referohemi black box penetration testing. Nderhyrja do behet per te zbuluar dobesite si dhe do te njoftohet infrastruktura per keto testime. |
| **Neni 8 pika ë:** Nevojitet të përcaktohet qartë, se çfarë lloj informacioni do monitorohet nëpërmjet “agjenteve”. Agjentët nuk duket të monitorojnë të dhëna personale, të dhëna klientësh, apo të dhëna konfidenciale, të cilat përbejnë sekret bankar. Ky monitorim duhet të kryhet vetëm nëse dakordësohet procesi mes operatoreve dhe Autoritetit. Në çdo rast kjo duhet të arrihet pasi SOC kombëtar të arrijë pjekurinë e duhur dhe të ketë demonstruar masa të larta sigurie.  - Nevojitet të përcaktohet me definicion se çfarë kuptohet me” agjent”. Instalimi i agjenteve rrit riskun kibernetik kundrejt sistemeve të infrastrukturave kritike dhe rrit riskun operacional (konflikt mes teknologjive të ndryshme, mirëmbajtje, suport); bie ndesh me parimin e sigurisë së informacionit mbi ndarjen e minimumit të nevojshëm të informacionit dhe rrit në mënyrë të panevojshme volumin e të dhënave pa u shoqëruar me kontekst.  - Mendojmë se mbledhja e informacionit në një pikë të vetme ka rrezikshmëri, pasi mund të funksionojë si “single point of failure”. Në rast kompromentimi të SOC sektorial, rrezikon i gjithë sektori financiar. Për këtë arsye është e rëndësishme që legjislacioni të parashikoje dhe masa të larta sigurie të cilat zhvillohen dhe përditësohen në përputhje me “best practices” ndërkombëtar. Gjithashtu informacioni që autoriteti përpunon dhe ruan, nuk duhet të ketë të dhëna konfidenciale mbi infrastrukturat kritike si p.sh teknologjitë e përdorura. Në rast nevoje specifike për të pasur këtë informacion, informacioni duhet të fshihet menjëherë pas përfundimit të procesit.  - Zgjidhja teknike sugjerohet të mos jetë pjesë e ligjit pasi është subjekt e ndryshimeve të shpeshta që ndodhin të teknologji si edhe ligji duhet të jetë me gjithë përfshirës dhe të akomodojë si i sektorin publik edhe atë privat, ambiente të ndryshme dhe teknologji të ndryshme si edhe nivele të ndryshme maturiteti që kanë operatorët e infrastrukturave kritike dhe të rëndësishme në shërbimet e sigurisë kibernetike.  - Kjo pikë nuk është pjesë e Direktivës (BE) 2016/1148 dhe nuk gjendet në asnjë rregullore/ligj të BE ose US si praktikë ose si kompetencë e organeve shtetërore ndaj infrastrukturave financiare. Gjithashtu bie ndesh me kompetencat e OIKR për te garantuar monitorimin dhe implementimin e masave sipas objektit te këtij ligji duke krijuar konflikt kompetencash midis funksioneve te sigurisë se OIKR dhe funksioneve/nën funksioneve monitoruese të Autoritetit. Duhet theksuar që asetet informatike janë ne pronësi të OIKR, të dhënat që ruhen/përpunohen në to i janë dhënë me konsent OIKR nga pronarët e këtyre të dhënave. Në bazë të këtyre argumentimeve aksesi direkt për të monitoruar këto asete mundet ti jepet palëve të treta (në këtë rast AKCESK) vetëm me dakordësi paraprake me OIKR, autorizim nga bordet drejtuese dhe njoftim paraprak tek Komisioneri për Mbrojtjen e të Dhënave Personale. | Shoqata Shqiptare e Bankave | Refuzuar | Agjentët është hequr si koncept. Kjo pike është riformuluar.  Lidhur me pikën e masave më të larta të sigurisë projektligji I garanton këto të fundit në tërësinë e tij. Gjithashtu përcaktohet qartë: parimi i mbrojtjes së të dhënave personale, parimi i  neutralitetit teknologjisë. |
| **Neni 9 pika c**: Nevojitet të qartësohet çfarë të drejtash dhe detyrimesh apo ndërlidhje krijohen mes sektoreve të listuar në të njëjtën gërmë. | Shoqata Shqiptare e Bankave | Refuzuar | Ky nen bën vetëm përcaktimin e subjekteve të tjera përgjegjëse për sigurinë e rrjeteve dhe sistemeve të informacionit (pika e pare) si dhe subjektet përgjegjëse për ofrimin e shërbimeve të sektorëve përkatës (pika e dytë). Ligji jep parashikime të përgjithshme ( referenca ne projektin aktual neni 11) . |
| **Neni 11 pika c:** Për sa parashikohet në këtë pikë, ri sjellim në vëmendje shqetësimet e ngritura në nenin 8, pika ë. Duhet te ketë një marrëveshje dypalëshe për atë çfarë mundet dhe çfarë do të duhet të monitorohet. Duhen specifikime në termat si edhe kushtet mbi ruajtjen dhe përpunimin e informacionit të dhëne (nëse do ketë). | Shoqata Shqiptare e Bankave | Refuzuar | Kjo pikë është riformuluar: c) monitoron, analizon dhe menaxhon kërcënimet kibernetike, vulnerabilitetet dhe incidentet në nivel kombëtar dhe ofron asistencë teknike për infrastrukturat kritike dhe të rëndësishme të informacionit sipas kërkesës nga operatorët e infrastrukturave të informacionit;  Percaktimi eshte i qarte ( referenca ne projektin aktual neni 13 pika c) |
| Neni 11 shkronjaç):parashikon*: “Monitoron rrjetet dhe sistemet e informacionit*...” i projektligjit - Si është menduar të bëhet ky monitorim ndërkohë që monitorimin e rrjetave dhe infrastrukturave e ka detyre çdo subjekt. | BSH | Pranuar | Riformuluar: d) monitoron në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, rrjetet dhe sistemet në infrastrukturat e tyre mbi incidente të sigurisë kibernetike apo sulme kibernetike;  ( referenca aktuale nndei 13 pika d) |
| Neni 11 pika ç: Për sa parashikohet në këtë pikë, ri sjellim në vëmendje shqetësimet e ngritura në nenin 8, pika ë. | Shoqata Shqiptare e Bankave | Refuzuar | Kjo pike është riformuluar dhe është e qartë: d) monitoron në bashkëpunim me operatorët e infrastrukturave kritike dhe të rëndësishme të informacionit, rrjetet dhe sistemet në infrastrukturat e tyre mbi incidente të sigurisë kibernetike apo sulme kibernetike; |
| **Neni 11 pika f:** Metoda e skanimeve duhet të jetë e dakordësuar dhe e njoftuar. Gjithashtu kjo metodë duhet të jetë e rregulluar me akt nënligjor, te konsultuar me bankat. | Shoqata Shqiptare e Bankave | Refuzuar | Përcaktimi i bërë i referohet sipas kërkesës së operatorëve. |
| ll) Analizon incidentin për të gjetur shkakun e tij si edhe koordinon aktivitetin me operatorët, CSIRT-et sektoriale, institucionet ndrkombëtare dhe qeveritare kur e shikon të arsyeshme;  Koment AAB – Nevojitet të qartësohet çfarë nënkuptohet me “simulim” në këtë rast. A do të ketë njoftim paraprak për “simulimin, mendojmë se duhet. | Shoqata Shqiptare e Bankave | Rerfuzuar | Nuk është nevojshme përcaktimi në ligj. Është pjesë e procesit të punës. Referuar vetë konceptit të “simulimit” nuk bëhet njoftim paraprak. |
| Neni 11 shkronja l): “Simulon rrjetet dhe sistemet e operatorëve për të gjetur pikat e dobëta të infrastrukturës dhe shërbimeve të tyre” – Jemi të paqartë se cfarë nënkupton kjo dispozitë do te behën pentest kurdo qe e çmon te përshtatshme. Skemat e rrjetit nuk mund te jepen nga subjektet, gjithashtu marrja ne dijeni e tyre do te duhet e garantohet dhe nga pala marrese. | BSH | Pranuar | Penteste- jo direkt në sistem por në platforma që simulojnë sistemin. |
| Neni 13 shkronja ë): Siguron rritje të kapaciteteve të stafit nëpërmjet trajnimeve dhe certifikimeve periodike sipas sektorëve që mbulojnë - Duke qenë se është e paqartë se si do jene te organizuar CSIRT-et sektoriale, është e paqarte edhe se si menaxhohen kapacitetet njerëzore dhe financiare nga subjekti respektiv. | BSH | Refuzuar | Këto element nuk mund të jepen në ligj . Gjithashtu lidhur me mënyrën e ngritjes , organizimin dhe funksionimin e CSIRT sektoriale përcaktohet se do të bëhet me VKM. |