REPUBLIKA E SHQIPËRISË
AUTORITETI I KOMUNIKIMEVE ELEKTRONIKE DHE POSTARE

Përfundime të Këshillimit Publik

Në përfundim të procesit të Keshillimit Publik te realizuar për dokumentin **"Rregullore mbi masat teknike dhe organizative për të garantuar sigurinë dhe integritetin e rrjeteve dhe/ose shërbimeve të komunikimeve elektronike"** u administruan dhe shqyrtuan komentet si më poshtë vijon:

- Komente të sipërmarrësit A datë 14.09.2015 me referencë LRD /0132/IK (AKEP shkresë Nr. Prot 992/4, datë 14.09.2015);

- Komente të sipërmarrësit B Nr.prot.4633 datë 11.09.2015 (AKEP shkresë Nr. Prot 992/6, datë 17.9.2015);

- Komente të sipërmarrësit C datë 11.09.2015 nr. 7339 (AKEP shkresë Nr. Prot 992/5, datë 15.9.2015);

- Komente të sipërmarrësit D datë 11.09.2015 nr.prot 1555 (AKEP shkresë Nr. Prot 992/3, datë 14.9.2015).

Neni 1

Nuk ka

Neni 2

Sipërmarrësi A

A sugjeron qe perkufizimet ne kete nen te jene ne perputhje me standardet perkatese nderkombetare dhe manualet guide te Enisa. Ne kete kontekst sugjerojme qe perkufizimi lidhur me "Mohimin e sherbimit - denial of service" te riformulohet duke saktesuar se mohimi i sherbimit quhet i tille atehere kur shkaktohet nga nderhyrje/veprime te jashtme dhe jo te brendshme te operatorit.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e operatorit A ne lidhje me perkufizimin ne nenin 2, pika 3 "Mohimi i Sherbimit".

Lidhur me perkufizimin e "incidentit te sigurise", ne perputhje me Ligjin 9918/2008, neni 122, si dhe Rregulloren per Autorizimin e Pergjithshem dhe detyrimet perkatese qe lindin nga Autorizimet e Pergjitshme te leshuara nga AKEP, masat teknike dhe organizative per te realizuar sigurine e rrjeteve dhe/ose te sherbimeve te ofruara prej tyre lidhen me garantimin e sherbimit qe operatoret e komunikimeve elektronike publike I ofrojne publikut. Ne perputhje me kuadrin ligjor si me lart, A

vlereson se "Incident i sigurise" ne kete Rregullore duhet te quhet shkelja e evidentuar e sigurise ose humbja e integritetit te rrjetit e cila afekton sherbimin e komunikimit elektronik publik (thirrje, SMS. MMS, internet) ndaj paitimtareve fundore dhe te dhenave e tyre personale, qe ka lidhje te drejtperdrejte me ofrimin e rrjeteve dhe sherbimeve nga operatori i komunikimeve elektronike, si dhe persa eshte nen kontrollin normal te operatorit te komunikimeve elektronike ne perputhie me detyrimet ligjore dhe te rregullores per autorizimin e pergjithshem. Ne kete kuptim, "Incidenti i sigurise" per qellimin e kesaj Rregullore nuk duhet te perfshije shkeljet e sigurise dhe humbja e integritetit qe lidhet me sistemet e sherbimet e brendshme te kompanise qe nuk kane lidhje me pajtimtaret fundore, si dhe shkeljet e sigurise qe mund te shkaktohen nga pale te treta te cilat kontaktojne drejtperdrejt perdoruesin e internetit pa nderhyrjen e operatorit te komunikimeve elektronike.

Qëndrimi i AKEP:
AKEP i qendron perkufizimit te gjendur, pasi eshte ne perputhje me percaktimet e ENISA ne "Article 13a Technical Guideline On Security Measures" dhe behet fjale per ato incidente te cilat kane ndikim në funksionimin e rrjeteve dhe sherbimeve të komunikimeve elektronike dhe te dhenat e pajtimtareve.

Sipërmarrësi B

Pika 2.1. Integriteti duhet të specifikohet si term më vete.

Qëndrimi i AKEP: *Komentet e operatorit B jane ne perputhje me percaktimet e rregullores, neni2, pika 1.*

Neni 3

Sipërmarrësi A

Neni 3 "Qellimi": Si edhe me lartpermendur lidhur me perkufizimin e "Incidentit te sigurise", ne perputhje me ligjin 9918/2008, neni 122, si dhe Rregulloren per Autorizimin e pergjithshem, A propozon qe qellimi i kesaj Rregulloreje te saktesohet sa i perket garantimit te sigurise, integritetit dhe funksionimit te rrjeteve sistemeve te komunikimit elektronik qe kane lidhje me ofrimin nga operatoret qe operojne nen regjimin e Autorizimit te Pergjithshem, te sherbimeve te komunikimeve elektronike (voice. SMS, MMS. Internet) per publikun dhe kane te dhena personale, per aq sa eshte nen kontrollin e ligjshem te operatoreve.

Qëndrimi i AKEP:
AKEP i qendron percaktimit te nenit 3 te rregullores pasi nuk shikohet e nevojshme cilesimet ne lidhje me llojet e sherbimeve (voice. SMS, MMS. Internet) dhe ne lidhje me kontrollin e ligjshem te operatoreve. AKEP nuk mund te dale jashte percaktimeve ligjore te detyrueshme per operatoret.

Neni 4

Sipërmarrësi A

Per te njejten arsye si me lart, propozojme qe pika a) e nenit 4 te rregullores te saktesohet duke shtuar pas fjalise se fundit: dhe ofrimit te panderprere te sherbimeve te komunikimeve elektronike (voice, SMS. MMS, intemet) perpublikun nga operatoret qe operojne nen regjimin e Autorizimit te pergjithshem, per aq sa eshte nen kontrollin e ligjshem te operatoreve"

Qendrimi i AKEP:
AKEP vlereson se nuk eshte e nevojshme te cilesohet pasi eshte e qarte dhe nenkuptohet se AKEP nuk mund te kerkoje me teper se sa eshte nen kontrollin e ligjshem te operatoreve.

Sipërmarrësi B

Pika (f), Përcaktimi i sanksioneve, masave administrative në rast se operatorët dështojnë në përmbushjen e detyrimeve të përcaktuara në këtë rregullore.

Komenti i B: Masat ndëshkimore duhet të bazohen në afatet që duhet të kenë Operatorët në implementimin e këtyre kërkesave. Ky dokument duhet të saktesojë qartë afatin kohor që do të kenë Operatorët për të implementuar këto kërkesa mbasi ky dokument të hyjë në fuqi. Nëse Operatori njofton AKEP për vështirësitë teknike që mund të ketë gjatë implementimit të këtyre kërkesave a do të ketë përsëri penalizim.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e ardhur nga B , mbi percaktimin e afatit kohor per permbushjen e detyrimeve qe rrjedhin nga kjo rregullore. Percaktimet mbi keto afate parashikohen ne neni nr.13 "Dispozite Kalimtare"

Neni 5

Nuk ka

Neni 6

Sipërmarrësi A

Ne vijim, ne nenin 6 pika 1, lidhur me detyrimin per njoftimin e AKEP per "Software te demshem" (Spam, virus, spyware..) kur keto dergohen permes internetit nga pale te treat, pa lidhje me operatorin e rrjetit dhe sherbimeve te komunikimeve elektronike; Ne perputhje me 2 nga 6 Ligjin 9918/2008, nenet 121,123, operatoret e komunikimeve elektronike kane detyrim ligjorte respektojne fshehtesine dhe konfidencialitetin e komunikimit elektronik dhe te mos interceptojne permbajtjen e komunikimit te perdoresve te rrjeteve dhe sherbimeve te tyre. Ne kete kuptim, sa i perket mesazheve me permbajtje malware qe mund te shperndahen permes internetit nga pale te treta pa lidhje me operatorin, A vlereson se operatoret e kane te ndaluar ligjerisht qe te identifikojne paraprakisht nje mesazh te tille, e per rrjedhoje te pamundur teknikisht per ta parandaluar dhe per ta raportuar si incident sigurie. Gjithashtu, ne kuptimin e Ligjit 9918/2008, neni 122 dhe Rregullores per Autorizimin e Pergjithshem, dergimi permes internetit nga pale te treta pa lidhje me operatorin e komunikimeve elektronike. i mesazheve SPAM qe mund te permbajne malware. nuk perben shkelje te detyrimeve per ruajtjen dhe garantimin e sigurise se perdoruesve nga ana e operatorit.
Per me teper, sa i perket e njoftimeve per software te demshem qe mund te shperndahen permes internetit (p.sh. pas marrjes dijeni si rezultat i ankesave te perdoruesve), ne kontekstin e qellimit te draft-ligjit "Per administrimin e sigurise kibernetike", monitorimi dhe raportimi i ketyre "software te demshem" vendoset nen kompetencen e ALCIRT, i cili do te jete sipas ketij Ligji organi pergjegjes per menaxhimin e procesit te administrimit te sigurise kibernetike ne bashkepunim me Keshillim e Sigurise Kibernetike dhe operatoret e infrastrukturave kritike te informacionit.
Persa me siper, sugjerojme qe SPAM te hiqet nga kategoria e software te demshem, dhe kategoria software te demshem te specifikohet si vijon:Software te demshem (virus, spyware, etj.) te cilet dergohen e jane nen kontrollin e drejtperdrejte te operatorit te komunikimeve elektronike."

Qëndrimi i AKEP:
AKEP merr ne konsiderate sygjerimi i ardhur, duke hequr SPAM nga kategoria e software te demshem.

Ne nenin 6 pika 5 e tij; mbrojtja e mjedisit te ciles i referohet AKEP gjykojme se eshte e paqarte si perkufizim dhe mbi te gjitha jashte kontekstit te Rregullores dhe objektit te saj. Mbrojtja e mjedisit rregullohet ne menyre te vecante me kuader specifik dhe te profilizuar, ndaj sugjerojme qe reference ne rregullore duhet te hiqet.

Qëndrimi i AKEP:
AKEP merr ne konsiderate propozimin e A dhe pika 5 e nenit 6 hiqet nga rregullorja.

Pika 13 e nenit 6 te Rregullores lidhur me informimin e perdoruesve per nje rrezik te vecante le vend per nje interpretim te gjere nga operatoret. Per kete, propozojme qe kushtet apo karakteristikat qe duhet te kete rreziku ne menyre qe te cmohet per nderhyrjen e operatorit sic percaktohet ne kete pike te Rregullores, te percaktohet qarte ne menyre qe te evitohen keqinterpretimet dhe kjo pike e rregullores te jete e zbatueshme ne menyre efikase.

Qëndrimi i AKEP:
AKEP sqaron se rrezik i vecante eshte cdo rrezik i cili kategorizohet si incident me impakt te larte ose te mesem, i cili afakton nje numer te konsdirueshem pajtimtaresh apo perben potencial per te afektuar.

Lidhur me piken 14 te nenit 6 te Rregullores, duke qene se eshte e ngjashme me percaktimet ne nenin 122 (pika 4) e Ligjit 9918/2008, kerkojme te sqarohet nga AKEP ne kete Rregullore se njoftimi ne AKEP do te kryhet ne rastet kur cenimi i te dhenave personale dhe shkeljeve te te dhenave personale eshte vene re nga vete operatori dhe jo nese operatori ka marre dijeni per shkeljen permes nje ankese te iniciuar nga vete perdoruesi per cenimin apo shkeljen e te dhenave te tij personale. Ne kete te fundit kompetenca me ligj i takon Komisionerit per te Drejten e Informimit dhe Mbrojtjen e te Dhenave Personale" ne perputhje me percaktimet e Ligjit 9887/2008 "Per Mbrojtjen e te dhenave personale".

Qëndrimi i AKEP:
AKEP sqaron se i permbahet perckaktimit te gjendur ne rregullore pasi kjo eshte nje detyrim qe rrjedh nga Ligji 9918, neni 122, pika 4.

Lidhur me piken 19 te nenit 6 te Rregullores, me qellim qartesimin e terminologjise se perdorur, A propozon qe pjesa e fjalise "Operatoret qe kryejne transaksione financiare online te zevendesohet me" Operatoret qe ofrojne vete apo permes te treteve transaksione financiare online".

Qëndrimi i AKEP:

AKEP merr ne konsiderate propozimin e ardhur nga operatori A.

Sipërmarrësi B

Pika (1),Operatorët duhet të informojnë AKEP brenda 3 ditëve, për secilin prej incidenteve të sigurisë. Komenti i B : Per Piken (1), si me siper, eshte i papercaktuar afati qe kane Operatoret per te njoftuar Akep, ky afat do të jetë për 3 ditë kalendarike apo për 3 ditë pune?

Qëndrimi i AKEP:
AKEP sqaron se behet fjale per 3 dite pune.

Pika (2), Operatorët duhet të informojnë AKEP menjëherë rreth incidenteve të zbuluara të sigurisë dhe/ose Cenimit të Integritetit, të cilat kanë pasur, kanë ose mendohet se do të kenë një impakt të rëndësishëm dhe / ose mesatar në ofrimin e rrjeteve të komunikimit publik dhe/ose në shërbimet e komunikimit elektronik publik të përdoruesit.

Komenti i B: Per Piken (2), si me siper,nuk percaktohet afati kohor.

Qëndrimi i AKEP:
Termi "menjehere" i referohet kohes se nevojshme, pa vonesa, qe i duhet operatorit per te pergatitur njoftimin i cili dergohet ne AKEP, por jo vone se 24 ore nga evidentimi i incidentit. Neni 6 pika 2 ndryshon dhe behet si me poshte vijon:

> ***"****Operatoret duhet te informojne AKEP rreth incidenteve te zbuluara te sigurise dhe/ose Cenimit te Integritetit, te cilat kane pasur, kane ose mendohet se do te kene nje impakt te rendesishem dhe / ose mesatar ne ofrimin e rrjeteve te komunikimit publik dhe/ose ne sherbimet e komunikimit elektronik publik te perdoruesit jo me vone se 24 ore nga evidentimi i incidentit.****"***

Pika (3) Operatorët duhet të implementojnë mjetet dhe metodat e duhura teknike dhe organizative për të garantuar sigurinë e rrjeteve të komunikimit publik dhe të shërbimeve të ofruara prej tyre. Këto mjete duhet të sigurojnë nivelin e sigurisë në përputhje me rrezikun e paraqitur dhe të evitojnë incidentet e sigurisë nga ndodhja e tyre ose të reduktojnë impaktin ose pasojat kur këto incidente ndodhin.

Komenti i B : Implementimet dhe rifreskimi i konfigurimeve të këtyre masave kërkon kohë, buxhet dhe burimet të tjera, ky proces është rekursiv dhe mund të ketë dhe probleme teknike gjatë procesit. Në këtë pikë AKEP mund të percaktojë kohën që duhet të kenë Operatorët për të implementuar këto kërkesa.

Qëndrimi i AKEP:
AKEP ben me dije se koha per marrjen e ketyre masave dhe implementimi i mjeteve, eshte percaktuar ne nenin 13 "Dispozita Kalimtare". Afati eshte 12 muaj nga hyrja ne fuqi te kesaj rregullore.

Pika (4) Operatorët duhet te implementojne mjetet e duhura teknike dhe organizative per te garantuar integritetin e rrjeteve te komunikimit publik, duke siguruar në këtë mënyrë ofrimin e pandërprerë të shërbimeve të tyre.

Komenti i B : Implementimet dhe rifreskimi i konfigurimeve të këtyre masave kërkon kohë, buxhet dhe burimet të tjera, ky proces është rekursiv dhe mund të ketë dhe probleme teknike gjatë procesit. Në këtë pikë AKEP mund të percaktojë kohën që duhet të kenë Operatorët për të implementuar këto kërkesa.

Qëndrimi i AKEP:
AKEP ben me dije se koha per marrjen e ketyre masave dhe implementimi i mjeteve, eshte percaktuar ne nenin 13 "Dispozita Kalimtare". Afati maksimal eshte 12 muaj nga hyrja ne fuqi te kesaj rregullore.

Pika (14) Në rast të cenimit të të dhënave personale, sipërmarrësi që ofron shërbime të komunikimeve elektronike të vlefshme për publikun njofton pa vonesë AKEP-in për këtë shkelje.

Komenti i B : Per piken (14), si me siper, nuk percaktohet afati kohor.

Qëndrimi i AKEP:
Termi "pa vonese" i referohet kohes fizike se nevojshme, qe i duhet operatorit per te pergatitur njoftimin i cili dergohet ne AKEP por jo me vone se 24 ore nga evidentimi i incidentit.
Neni perkates ndryshon si me poshte vijon:

> *"Në rast të cenimit të të dhënave personale, sipërmarrësi që ofron shërbime të komunikimeve elektronike të vlefshme për publikun njofton AKEP për këtë shkelje jo me vone se 24 ore nga evidentimi i saj."*

Pika (15) Kur një shkelje e të dhënave personale mund të ndikojë në privatësinë e pajtimtarit ose individit, sipërmarrësi, gjithashtu, njofton pa vonesë pajtimtarin ose individin për shkeljen.

Komenti i B : Per piken (15), si me siper, nuk percaktohet afati kohor.

Qëndrimi i AKEP:
Termi "pa vonese" i referohet kohes fizike se nevojshme, qe i duhet operatorit per te pergatitur njoftimin i cili dergohet pajtimtarit por jo me vone se 24 ore nga evidentimi i incidentit.
Neni perkates ndryshon si me poshte vijon:

> *"Kur një shkelje e të dhënave personale mund të ndikojë në privatësinë e pajtimtarit ose individit, sipërmarrësi, gjithashtu, njofton pajtimtarin ose individin për shkeljen jo me vone se 24 ore nga evidentimi i shkeljes"*

Pika 1 që shpreh detyrimin e referimeve në AKEP duhet t'i referohet edhe pikës dy për të specifikuar nivelin e rëndësisë së incidenteve që raportohen. Brenda tre ditëve, apo menjëherë dhe për cilat incidente? Afati kohor i raportimeve duhet te jetë i qartë në ditë kalendarike/pune.

Qëndrimi i AKEP:
Afati kohor i raportimit eshte 3 (tre) dite pune.

Pika 3 - Kush e bën vlerësimin e rrezikut të paraqitur?

Qëndrimi i AKEP:
Vleresimi i rezikut te paraqitur behet nga sipermarresi sipas rregullave te percaktuara ne legjislacionin ne fuqi.

Pika 7a. Qëllimet e përdorimit janë jo vetëm ligjore por kryesisht biznesi dhe me pas edhe ligjore, në të dyja rastet vetëm bazuar në legjislacionin përkatës.

Qëndrimi i AKEP:
Komenti i operatorit B eshte marre ne konsiderate. Eshte ndryshimi perkates si me poshte vijon:

a) të sigurojnë që të dhënat personale të jenë të aksesueshme vetëm nga personeli i autorizuar bazuar në legjislacionin përkatës

Pika 8. Publikimi i referohet publikimit brenda kompanisë dhe palëve të treta të autorizuara?

Qëndrimi i AKEP:
Publikimi i rregullave per sigurine i referohet publikimit brenda kompanisë dhe palëve të treta të autorizuara.

Pika 11. Termi manual duhet të zëvendësohet me “udhëzime” dhe të specifikohet më qartë termi “ incidente të zakonshme të sigurisë” p.sh., në lidhje me të dhënat personale, në lidhje me viruse, etj.

Qëndrimi i AKEP:
Komenti i operatorit B eshte marre ne konsiderate.Termi “ incidente me të zakonshme të sigurisë” u referohet incidenteve te cilat ndodhin me shpesh dhe ne menyre te perseritur.

Sipërmarrësi B kerkon qe neni 6 te riformulohet si me poshte:
2. Operatoret duhet te informojne AKEP menjehere rreth shkalles incidenteve te zbuluara te sigurise dhe/ose Cenimit te Integritetit, te cilat kane pasur, kane ose mendohet se do te kene nje impakt te rendesishem dhe / ose mesatar ne ofrimin e rrjeteve te komunikimit publik dhe/ose ne sherbimet e komunikimit elektronik publik te perdoruesit.

Qëndrimi i AKEP:
Operatoret duhet te informojme AKEP rreth incidenteve te zbuluara dhe rreth shkalles se kategorizimit te incidentit.

3. Operatoret duhet te implementojne zgjidhje teknike,masat e duhura teknike dhe organizative dhe metodat e kontrolleve të brendshme për të garantuar sigurinë e rrjeteve të komunikimeve publike dhe shërbimeve të ofruara prej tyre.
Keto mjete duhet te sigurojne nivelin e sigurise ne perputhje me rrezikun e paraqitur dhe te evitojne incidentet e sigurise nga ndodhja e tyre ose te reduktojne impaktin ose pasojat kur keto incidente ndodhin.

Qëndrimi i AKEP:
AKEP i qendron percaktimit dhe formulimit te nenit 6 pika 3 te rregullores.

7. Operatoret duhet të sigurojnë një nivel të mbrojtjes dhe sigurisë së përshtatshme ndaj rreziqeve të mundshme, të parashikuara. Masat qe operatoret do te ndermarrin duhet që, të paktën:
a) të sigurojnë që të dhënat personale të jenë të aksesueshme vetëm nga personeli i autorizuar për te suportuar ne sherbimet qe ofrojne ;
b) të mbrojnë të dhënat personale të ruajtura ose të transmetuara nga aksidentet apo nga shkatërrimi i kundërligjshëm, humbja ose ndryshimi aksidental dhe ruajtja, përpunimi, aksesi apo zbulimi i paautorizuar ose i jashtëligjshëm;
c) të sigurojnë implementimin e politikave të sigurisë, lidhur me përpunimin e të dhënave personale.

Qëndrimi i AKEP:
Komenti i operatorit B eshte marre ne konsiderate pjeserisht. Verehet se jane paraqitur komente me qendrime te ndryshme per neni 6, pika 7.

12. Operatoret duhet te informojne perdoruesit e sherbimeve te rrjeteve te komunikimit publik ne lidhje me punet e planifikuara per mirembajtjen ose perditesimet, të paktën 1 dite përpara fillimit të punimeve te cilat mund te kene ndikim të lart dhe kohëzgjatja per mirëmbajtjen tejkalojnë SLA qe kane me palet e tyre te kontraktuara per dhënien e ketyre shërbimeve.

Qëndrimi i AKEP:
Komenti i operatorit B eshte marre ne konsiderate pjeserisht. Pika perkatese ndryshon dhe behet si me poshte:

"Operatoret duhet te informojne perdoruesit e sherbimeve te rrjeteve te komunikimit publik ne lidhje me punet e planifikuara per mirembajtjen ose perditesimet, të paktën 1 dite përpara fillimit të punimeve te cilat mund te cilat mund te kene ndikim të lart dhe te sjellin nderprerje provizore te sherbimeve."

13. Operatoret duhet të informojnë përdoruesit e tyre për një rrezik të veçantë te lartë, mënyrën se si rreziku mund të reduktohet nga përdoruesit, si dhe kostot e mundshme, që duhet të mbulohen nga përdoruesi, nëse rreziku që ndodh është jashtë masave, që mund të marrë sipërmarrësi.

Qëndrimi i AKEP:
Komenti i operatorit B eshte marre ne konsiderate.

Neni 7

Sipërmarrësi A

Ne nenin 7 nevojitet nje rinumertim per shkak te lapsuseve te formatimit ne tekst.

A vlereson se qellimi ne piken 7 te nenit 7 AKEP eshte njoftimi i perdoruesve te rrjeteve dhe sherbimeve te diet jane prekur nga incidenti i sigurise i vleresuar i larte. Me qellim qartesine dhe evitimin e keqinterpretimeve, propozojme qe kjo pike te riformulohet si vijon: "Njofton perdoruesit e rrjeteve dhe/ose sherbimeve te prekur, rreth incidentit te sigurise, ne rast se e konsideron e larte impaktit e incidentit te sigurise."

Qëndrimi i AKEP : *Eshte marre parasysh komenti i A ne lidhje me saktesimin e kesaj pike ne nenin 7. Neni perkates ndryshon si me poshte vijon:*

"Njofton perdoruesit e rrjeteve dhe/ose sherbimeve te prekur, rreth incidentit te sigurise, në rast se e konsideron si te larte impaktin e incidentit te sigurise."

Sipërmarrësi B

Ne Nenin (7), Pika (3) dhe (4) mungojnë.

Pika (7) AKEP Njofton përdoruesit e rrjeteve dhe/ose shërbimeve rreth incidentit të sigurisë, në rast se e konsideron si të lartë impaktin e incidentit të sigurisë.

Komenti i B: Nuk eshte e qarte situata nese operatorët do të njoftohen në këtë rast?
Duke pasur parasysh qe një proces i tillë mund të ketë impakt negativ në biznes për operatorin AKEP duhet te njoftoje edhe operatoret.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e ardhur nga B . Neni perkates ndryshon si me poshte vijon:

"Njofton perdoruesit e rrjeteve dhe/ose sherbimeve te prekur, rreth incidentit te sigurise, në rast se e konsideron si te larte impaktin e incidentit te sigurise duke vene ne dijeni operatorin e rrjetit ose sherbimit perkates."

Pika (8) Kryen kontrolle në mënyrë periodike në bashkëpunim me ALCIRT, për të verifikuar implemetimin e kësaj rregulloreje.

Komenti i B : Eshte e papërcaktuar koha kur Operatorët do të njoftohen për këto audite. Perderisa citohet se do te jene kontrolle periodike duhet te percaktohet peridoiciteti i tyre nese do te jene 6 mujore apo vjetore etj.

Në këto kërkesa duhet të përcaktohen sistemet të cilat do të jenë subjekt i këtij auditi si dhe formati standart i auditimit i cili te jete si aneks i kesaj rregulloreje.

Audituesit duhet të kenë një program të veçantë pune i cili te bazohet ne formatin standart dhe duhet të rishikohet nga Operatori.

Pika 6. Nuk është e qartë mënyra e investigimit të AKEP: në bashkëpunim me operatorët? Në këtë rast këta të fundit duhet të llogarisin edhe pjesën e nevojshme të personelit; nëse është në mënyrë të pavarur, konkluzionet duhet të jenë transparente edhe për operatorët.

Sipërmarrësi B kerkon qe neni 7 te riformulohet si me poshte:
9. Ndermerr masat taknike sipas legjislacionit në fuqi nese operatoret nuk plotesojne kërkesat dhe kushtet e kesaj rregulloreje.

Qëndrimi i AKEP:
AKEP merr ne konsiderate pjeserisht komentin e B duke saktesuar ne rregullore rastet kur mund te behen kontrollet. Neni perkates ndryshon si me poshte vijon:

> *"Kryen kontrolle ne bashkepunim me ALCIRT, per te verifikuar implemetimin e kesaj rregulloreje ne rastet kur shihet e nevojshme."*

Pika (9) Ndërmerr masa sipas legjislacionit në fuqi nëse operatorët nuk plotësojnë kërkesat dhe kushtet e kësaj rregulloreje.

Komenti i B: Formulimi ne piken (9), si me siper, per marrjen e masave sipas legjislacioni ne fuqi nese operatoret nuk plotesojne kerkesat dhe kushtet e kesaj rregullore eshte evaziv dhe le hapesire te gjere per interpretime.

Te percaktohet ne rregullore se cilat jane masat qe ndermerr rregullatori ne raste te tilla. Per me teper duhet percaktuar edhe intervali kohor ku Operatorit i lihet kohë për t'i mbyllur/korrigjuar problematikat e evidentuara nga auditoret.

Qëndrimi i AKEP:
AKEP ne pergjigje te komentit te B ben me dije se masat qe mund te marre AKEP jane te percaktuar ne ligjin nr.9918. Persa i perket intervalit kohor operatoret kane 12 muaj kohe, bazuar ne nenin 13 per te bere auditin e sistemeve te tyre dhe per te korrigjuar problemet nese indentifikohen.

Neni 8

Sipërmarrësi B

Pika 6. Operatorët kanë nevojë që të dhënat t'i aksesojnë edhe **në" kuadër të përmirësimit të shërbimeve"**, jo vetëm për ofrimin.

Sipërmarrësi B kerkon qe neni 8 te riformulohet si me poshte:
4. Operatoret, personat e autorizuar, punonjesit, dhe cdo individ i përfshirë në sistemet e komunikimeve elektronike, pjesë e strukturave të Operatorit jane pergjegjes per ruajtjen e te dhenave dhe mbrojtjen e konfidencialitetit te te dhenave dhe komunikimeve dhe periudhes se ruajtes se te dhena te percaktuar prej rregullatorit.

Qëndrimi i AKEP:
AKEP i qendron percaktimit ne nenin 8 pika 6.

Neni 9

Sipërmarrësi A

Lidhur me vleresimin e impaktit te incidenteve te sigurise, A eshte dakord me ndarjen ne incident te ulet te mesem e te larte. si dhe me rekomandimin per te njoftuar AKEP vetem per incidentet e vleresuara te mesme e te larta.
Sa i perket kritereve te klasifikimit/vleresimit te incidenteve te sigurise, kombinimit te tyre, ne kuptim te objektit dhe qellimit te Rregullores, i cili lidhet ngushte me sherbimet dhe rrjetet te cilat ofrojne sherbime dhe kane te dhena personale te perdoruesve, A vlereson se kriteri primar i cili duhet te klasifikoje nje incident nese eshte I ulet, 1 mesem apo i larte eshte numri i pajtimtareve te prekur, e kombinuar me kohezgjatjen e incidentit dhe vetem ne rastet kur numri i pajtimtareve eshte i panjohur incidenti mund te vleresohet nga shtrirja gjeografike per rastet e mohimit te sherbimit.
Ne kete kontekst, duke marre parasysh standardet nderkombetare, propozojme si vijon:

Pika 3 e Nenit 9 te ndryshohet si vijon:
a. "Incidentet e sigurise konsiderohen si incidente me impakt te larte nese numri i perdoruesve te ndikuar nga incidenti eshte minimalisht sa 5% e numrit total te perdoruesve, por jo me pak se 1000 perdorues."
b. "Incidentet e sigurise konsiderohen si incidente me impakt te ulet nese numri i perdoruesve te ndikuar nga incidenti eshte minimalisht sa 0.2% e numrit total te perdoruesve. por jo me shume se 1000."
Sa me siper e propozojme me qellim vleresimin analog e te drejte te incidentit per cdo operator pavaresisht numrit total te pajtimtareve te tij.

Qëndrimi i AKEP:
AKEP merr ne konsiderate pjeserisht komentit e A,duke reflektuar perkufizimin ne lidhje me incidentin e sigurise me impakt te ulet ne lidhje me numrin e pajtimtareve ne piken 2 te nenit 9.

Pika 4 e Nenit 9 te ndryshohet si vijon: "Ne rast se numri i pajtimtareve eshte i panjohur, incidentet e sigurise do te konsiderohen si incidente me impakt te larte nese zona gjeografike e shtrirjes se tij eshte minimalisht 10 km, per rastet kur incidenti eshte shkaktuar si pasoje e mohimit te sherbimit."

Qëndrimi i AKEP:
AKEP ne rastin e pikes 4 te nenit 9 ben me dije se kriter vleresim eshte shtrirja e incidentit bazuar ne zone gjeografike.

Sipërmarrësi C

Lidhur nenin 9/2, “Incidentet e sigurise qe kane pasur kohezgjatje me pak se 1 ore, ne menyre automatike konsiderohen si te nje impakti te ulet dhe nuk eshte i nevojshem plotesimi i tabeles", C kerkon modifikimin e ketij neni/pike si me poshte;

Neni 9/2
"Incidentet e sigurise qe kane pasur kohezgjatje me pak se 1(nje) ore me pak se 2 (dy) ore, ne menyre automatike konsiderohen si te nje impakti te ulet dhe nuk eshte i nevojshem plotesimi i tabeles"

Qëndrimi i AKEP:
AKEP i qendron percaktimit ne rregullore duke e mbajtur afatin kohor maksimal ne 1 (nje) ore

Persa i perket nenit 9/3, "Incidentet e sigurise konsiderohen si incidente me impakt te larte nese numri i perdoruesve te ndikuar nga incidenti ose perqindja e tyre ndaj perdoruesve total eshte minimalisht 1000 ose 5%. C kerkon qe ky nen/pike te ndryshohet/modifikohet sime poshte;

Neni 9/3;
"Incidentet e sigurise konsiderohen si incidente me impakt te larte nese numri i perdoruesve te ndikuar nga incidenti ose perqindja e tyre (%) ndaj perdoruesve total eshte minimalisht 1000 ose mbi 10% e abonenteve te te gjithe kategorive te sherbimit.

Qëndrimi i AKEP:
AKEP i qendron percaktimit ne rregullore duke e mbajtur limitin e perqindjes te abonenteve ne 5%, pasi vlereson se kjo perqindje eshte nje vlere e konsiderueshme e bazes se pajtimtareve.

Po ashtu, ne nenin 9/4, ku percaktohet se;"Incidentet e sigurise konsiderohen si incidente me impakt te larte nese zona gjeografike e shtritjes se tij eshte minimalisht 10 km, C argumenton qe;
Impakti qe sjell nje incident sigurie i cili ndodh ne nje lokalitet ku gjenden qendrat me te rendesishme te funksionimit te shtetit dhe per me teper me perqendrim te larte abonentesh, nuk eshte i njejte me impaktin qe do te sillte ndodhja e nje incidenti ne zona/rajone apo lokalitete ku keta faktore jane me pak prezent. Per kete arsye C kerkon ndryshimin/modifikimin e ketij neni/pike si me poshte;

Neni 9/4;
'Incidentet e sigurise konsiderohen si incidente me impakt te larte nese zona gjeografike e shtritjes se tij eshte me shume se 10 km per rrjetin fix, 10 km per rrjetin mobile ne qytetin e Tiranes, si dhe 60 km per zona te tjera te Shqiperise".

Qëndrimi i AKEP:
AKEP vlereson komentin e C duke e marre ne konsiderate pjeserisht. Incidentet e sigurise konsiderohen si incidente me impakt te larte nese zona gjeografike e shtritjes se tij eshte minimalisht 20 km^2.

Sipërmarrësi B

Komenti i B: Formula e përllogaritjes së impaktit është jo shumë e qartë dhe në disa raste jo e saktë.

Nëse do të ketë raste të veçanta të Incidenteve të Sigurisë së Informacionit (p.sh., incidentet e Interceptimit) edhe intervale më të shkurtra kohore se 1 orë prej B konsiderohen incidente të një impakti tepër të lartë pasi në këtë rast janë thyer të gjitha mekanizmat e sigurisë së rrjetit të komunikimit.

Ne tabelën e Aneksit 2, limiti i sipërm për ndërprerjet mund të zgjerohet me teper se 4 orë.

Afati kohor prej 15 ditësh nuk është i mjaftueshëm në disa raste për të nxjerrë një vlerë të saktë të impaktit. Nëse konsiderojmë që disa prej sistemeve tona janë të hostuara jashtë Shqipërisë ky proces mund të marrë më shumë se 15 ditë, pasi vlerësimi do të kalojë në disa grupe vlerësimi dhe më pas në B për vlerësimin final.

Qëndrimi i AKEP:

AKEP vlereson komentin e B duke marre ne konsiderate pjeserisht.
Limiti kohor per vleresimin perfundimtar behet 30 dite. Ne lidhje me limitin kohor ne Aneks 2 AKEP vlereson se limit kohor prej dy oresh duhet te qendroj dhe jo te zgjatet ne 4 ore, pasi edhe dy ore eshte nje interval kohor i konsiderueshem.

Pika 2, 3, dhe 4. Klasifikimi i incidenteve të sigurisë duke marrë parasysh vetëm kohëzgjatjen, apo shtrirjen fizike mund të çojë në klasifikim jo të saktë; kohëzgjatja duhet të jetë si referente për impaktin e incidentit kur ky i fundit rezulton në ndërprerje të shërbimeve; vlerësimi i kritikalitetit duhet të jetë një metodologji që kombinon tregues të tipit të të dhënave që impaktohet, nr të klienteve, kohëzgjatjen dhe **kohën e nevojshme për t'u kthyer në gjendjen e mëparshme.**

Qëndrimi i AKEP:
Per te klasifikuar nje incident si incident me impakt te larte mjafton qe njeri nga parametrat e percaktuar (kohezgjatja, numri i pajtimtareve dhe shtrirja gjeografike) te permbushet.

Pika 6. Përcakton vetëm incidentin madhor. Nuk qartësohet kush është një incident mesatar.

Qëndrimi i AKEP:
Incident mesatar klasifikohet cdo incident i cili kalon limitet e percaktuara per nje incident te ulet por gjithashtu parametrat nuk arrijne ne limitet per tu klasifikuar sin je incident me impakt te larte.

Po rasti nëse një parametër është i lartë dhe parametri tjetër është i ulët? Metodologjia e vlerësimit të impaktit duhet të varet nga tipi i incidentit.

P.sh., një interceptim i paautorizuar është më vete një incident serioz pavarësisht nga kohëzgjatja ose nr i personave të ndikuar; gjithashtu vlerësimi i një programi/software të dëmshëm nuk mund vlerësohet në bazë të orëve ose të hapësirës gjeografike.

Në fakt, meqë të gjithë operatorët kanë metoda të bazuara në rregullore/standarte ndërkombëtare për klasifikim dhe reagimin ndaj incidenteve, do ishte mirë që AKEP të merrte parasysh këto metodologji për të standartizuar edhe mënyrën e raportimit. Mungesa e këtij standartizimi do ketë dy efekte:

1. Përpjekje ekstra dhe kosto për operatorët për të mbajtur dy mënyra raportimi dhe reagimi;
2. Gabime në raportim dhe klasifikime të ndryshme nga operatorë të ndryshëm që mund të shkaktojnë kosto ekstra dhe mungesë të saktë informacioni në lidhje me risqet e rëndësishme të tregut.

Qëndrimi i AKEP:
Per te klasifikuar nje incident si incident me impakt te larte mjafton qe njeri nga parametrat e percaktuar (kohezgjatja, numri i pajtimtareve dhe shtrirja gjeografike) te permbushet.

Pika 8. Mund të ndodhë që incidenti i sigurisë të kërkojë më shumë kohë për investigim;

Qëndrimi i AKEP:
Eshte marre ne konsiderate propozimi i operatorit B duke e rritur kohen e nevojshme per investigim nga 15 ne 30 dite.

B Albania kerkon qe neni 9 te riformulohet si me poshte:

1. Operatoret duhet te kryjne vleresimin periodik te impaktit te incidenteve te sigurise sipas tabeles se paraqitur ne Aneksin 2.

Qëndrimi i AKEP:
AKEP cmon se vleresimi i impaktit duhet te jete referuar pas ndodhjes se cdo incidenti dhe jo ne menyre periodike.

2. Incidentet e sigurise qe kane pasur kohezgjatje me pak se 1 ore, ne menyre automatike konsiderohen si te nje impakti te ulet dhe nuk eshte i nevojshem plotesimi i tabeles.

Qëndrimi i AKEP:
Operatori B eshte i te njejtit qendrim me percaktimin ne rregullore te AKEP.

3. Incidentet e sigurise konsiderohen si incidente me impakt te mesatar nese numri i perdoruesve te ndikuar nga incidenti ose perqindja e tyre (%) ndaj perdoruesve total eshte minimalisht 1000 ose 5%.

Qëndrimi i AKEP:
AKEP i qendron percaktimit se incidenti me numer te perdoruesve total minimalisht 1000 ose 5% e totalit klasifikohet si incident me impakt te larte.

4. Incidentet e sigurise konsiderohen si incidente me impakt te larte nese zona gjeografike e shtrirjes se tij eshte minimalisht 10 km² ose perqindja eshte me teper se 5%.

Qëndrimi i AKEP:
Operatori B eshte i te njejtit qendrim me percaktimin ne rregullore te AKEP.

5. Ne cdo rast tjeter, incidentet e sigurise konsiderohen si incidente me impakt mesatar.

Qëndrimi i AKEP:
Operatori B eshte i te njejtit qendrim me percaktimin ne rregullore te AKEP.

Neni 10

Sipërmarrësi A

Ne nenin 10 pika 2 e Rregullore, lidhur me kerkesen per kryerjen e auditit te sigurise nga nje organ I certifikuar dhe i pavarur, ose nga autoriteti kompetent nje here ne 2 vjet per subjektet me te ardhura vjetore te vitit paraardhes mbi vleren 100,000,000 leke, A vlereson se ne kete pike mbetet e paqarte se cili do te jete objekti i auditit te sigurise. i cili do te konsiderohet nga AKEP i vlefshem per qellimet e kesaj Rregulloreje, cilet organe kuailfikohen si organe te certifikuara te pavaruar qe mund te kryejne auditin e sigurise sipas kesaj Rregulloreje, si dhe kush eshte autoriteti kompetent te cilit i ben reference neni perkates, cka kerkojme te sqarohen duke riformuluar nenin perkates.

Konkretisht ne kuader te auditimit te pervitshem financiar nga auditoret tane te jashtem (PWC aktualisht), A auditohet edhe sa i perket masave te sigurise per disa nga sistemet kritike te informacionit A sugjeron qe edhe auditoret financiare te jashtem si PWC te konsiderohen organe te certifikuara e te pavaruara, si dhe auditimi Lidhur me sigurine i kryer prej tyre te konsiderohet auditim i mjaftueshem sigurie nga AKEP per nevojat e kesaj Rregulloreje.

Gjithashtu, duke qene se procesi i auditimit te jashtem nder te tjera eshte i kushtueshem dhe kerkon alokimin e burimeve njerezore dhe financiare te nevojshme, A sugjeron qe auditimi i sigurise te kryhet ne menyre periodike nga vete AKEP, i cili eshte organi mbikqyres pergjegjes per zbatimin e kerkesave te Ligjit 9918/2008, Autorizimit te pergjithshem dhe rregulloreve perkatese lidhur me masat e sigurise se rrjeteve e sherbimeve te ofruara nga operatoret e komunikimeve elektronike.

Qëndrimi i AKEP:

AKEP vlereson komentin e A dhe sqaron se objekti i auditit te sigurise do te jete i njejte me objektin dhe procedurat e percatuara ne Aneks 3, bashkelidhur kesaj rregullore. Ne lidhje me auditin e certifikuar e pavarur AKEP ben me dije se eshte ne vullnetin e kompanise te zgjedhe auditin, i cili te jete i pavarur nga operatori, por duke plotesuar kushtet qe te jete i certifikuar per ISMS (Information Security Managment Systems). Ne lidhje me kryerjen e auditit nga vete AKEP, ju bejme me dije se ne AKEP do te kryehet vetem depozitimi i rezultateve te auditit ne rastin e operatoreve te me te ardhura vjetore mbi 100.000.000 leke.

Sipërmarrësi C

Nderkohe, C vlereson si tejet te rendesishme percaktimet e nenit 10 te draft Rregullores
mbi raportimin e masave te sigurise dhe auditit. Ne kete nen eshte percaktuar nje kategorizim i sipermarresve bazuar ne raportimin vjetor te te ardhurave te ketyre te fundit,sipas te cilit vlera prej 100.000.000 lek sherben si vlera varesisht te ciles sipermarresi eshte subjekt i detyrimit per raportimin ne forme vet-deklarimi mbi masat e sigurise ose te dorezoje prane AKEP raportin me rezultatet e auditit te sigurise.

Formulimi ne teresi i nenit 10, vjen ne kundershtim me percaktimet e nenit 7, pika 3/e) e Ligjit nr. 9918 dt. 19.05.2008, i ndryshuar Komunikimet Elektronike ne Republiken e Shqiperise" sipas te cilit AKEP nxit konkurencen eficente per sigurimin e rrjeteve dhe te sherbimeve te komunikimeve elektronike per te siguruar mosdiskriminimin dhe barazine ne trajtimin e ofruesve te rrjeteve dhe sherbimeve. Keshtu, te gjithe sipermarresit duhet te jene subjekt i detyrimeve me natyre te njejte per sa kohe qe po keta sipermarres pergjigjen po ne menyre te njejte perballe AKEP dhe perballe detyrimeve te percaktuara nga Ligji, kryejne pagesat sipas percaktimeve te Ligjit sipas vlerave te percaktuara ne aktet ligjore njesoj per te gjithe sipermarresit etj. Ndaj, dhe ne kete kuptim, nuk mundet qe nje kategori e caktuar sipermarresish te trajtohet ne menyre diskriminuese favorizuese dhe nje pjese tjeter te rendohet me nje kosto tejet te larte financiare.

Pavaresisht madhesise se rrjetit apo nivelit te te ardhurave, siguria dhe integriteti i rrjeteve eshte po njesoj i rendesishem si per pajtimtarin e nje operatori te vogel ashtu edhe per pajtimtarin e nje operatori te madh. Madje, operatore te medhenj (praktikisht ata qe sipas kesaj draft rregulloreje kane te ardhura vjetore me shume se 100.000.000 leke) kane ne fakt rrjete dhe teknologji me te zhvilluar ku masat e sigurise dhe te integritetit te rrjetit i kane si nje ceshtje te rendesishme per interesin e vet kompanise, investimeve ne rrjet dhe cilesise se sherbimeve te ofruara, pertej cdo detyrimi te vendosur. Nderkohe qe, me se shumti ndeshet pikerisht tek keta sipermarres "te vegjel" mos permbushja e standarteve ne operimin e aktivitetit te ofrimit te rrjeteve dhe sherbimeve dhe mosplotesimi i kushteve dhe rregulloreve te AKEP ne lidhje me ndertimin dhe funksionimin e rrjeteve te komunikimeve elektronike. Ndaj dhe nese do te ishte e nevojshme, certifikimi me audit sigurie do te duhej pikerisht per keta sipermarres dhe jo per operatoret qe kane rrjete me shtrirje te gjere dhe teknologji te zhvilluar te cilet, ashtu sic referuam me lart, interesin per mbrojtjen e rrjeteve dhe sherbimeve e kane edhe kryesisht pavaresisht detyrimeve rregullatore .

Per me teper, neni 122, pika 10 e Ligjit i cili percakton mundesine per vendosjen e detyrimeve per vete-deklarimin mbi masat e sigurise apo paraqitjen e auditit te sigurise nuk parashikon mundesine per trajtimin e diferencuar te sipermarresve varesisht ndonje kriteri dhe akoma me shume, ky nen nuk percakton asnje kriter fmanciar te lidhur me te ardhurat e sipermarresit per kategorizimin e ketyre te fundit me qellim vendosjen e detyrimeve. Keshtu, ne percakimin e detyrimeve ndaj operatoreve dhe per me teper kur keto detyrime jane me kosto te larte financiare per sipermarresit, do duhej qe ne cdo

rast ky kriter te ishte i parashikuar qartesisht nga Ligji. Po ashtu, edhe percaktimi i vleres prej 100.000.000 lek krijon diskutime te shumta pasi ne kete rast brenda te njejtes kategori, sic mund te jete rasti i sipermarresve me te ardhura mbi 100.000.000 leke, ka sipermarres qe nga keto te ardhura kane fitime te konsiderueshme po ashtu ka sipermarres qe jo vetem nuk kane fitim por kane rezulutar me humbje duke bere teresisht te ndryshme pozicionin financiar te sipermarresve brenda se njejtes kategori. AKEP i disponon te gjitha te dhenat financiare te operatoreve ndaj dhe AKEP duhej te kishte konsideruar edhe kete fakt ne vendosjen e ketij kriteri ne draft rregullore.
Per sa parashtruam me lart, C kerkon qe neni 10 te rifromulohet ne teresi si me poshte;

Neni 10
Te gjithe sipermarresit e sherbimeve te komunikimeve elektronike duhet te raportojne ne AKEP ne formen e nje vetdeklarimi masat e marra te sigurise periodikisht nje here ne vit brenda muajit Janar per vitin paraardhes sipas Aneksit 3.

Ose ne meyre alternative;

Neni 10
Te gjithe sipermarresit e sherbimeve te komunikimeve elektronike duhet qe te dorezojne prane AKEP raportin me rezultatet e auditit te sigurise, te kryer nga nje organ i certifikuar dhe i pavarur ose nga autoriteti kompetent.
Raporti duhet te dorezohet periodikisht per nje periudhe jo me shume se dy vjecare. Kostoja e auditit do te paguhet nga sipermarresi.

Qëndrimi i AKEP:
AKEP bazuar ne madhesine e operatoreve dhe ne gamen e gjere te sistemeve dhe sherbimeve qe disponojne operatoret e grupuar ne piken 2 te nenit 10 vlereson se pervec vetedeklarimit, eshte i nevojshem dhe kryerja e auditit nga nje organ i specializuar.
Ne lidhje me operatoret te clet do te depozitojne vetem vetedeklarim sipas Aneks 3, AKEP ben me dije se gjate inspektimeve qe do te kryehen do te behet dhe verifikimi i raportimeve, ku do te vleresohet perputhshmeria ne lidhje me cfare eshte deklaruar dhe cfare eshte zbatohet konkretisht nga sipermarresi.

Persa i perket percaktimit ne nenin 10/7 te projekt-rregullores ku percaktohet se ;
"AKEP mund te kerkoje te dhena te tjera shtese, pervec atyre ne formularin perfundimtar, ne lidhje me incidentin e sigurise. Per kete arsye, operatoret jane te detyruar te ruajne te gjithe te dhenat ne lidhje me incidentet esigurise se raportuar per nje periudhe kohore prej 18 muaj qe nga koha e dorezimit te njoftimitperfundimtar rreth incidentit te sigurise.
C kerkon qe;
Afati kohor i ruajtjes se te dhenave duhet te jete me i shkurter se 18 muaj pasi akualisht C apo cdo operator tjeter, si pasoje e detyrimeve ligjore per qellime specifike detyrohet te ruaje te dhena per afate edhe me te gjata. Nje detyrim i ri sipas kesaj projekt-rregulloreje per te ruajtur edhe keto te dhena dhe me afate te tilla te gjata do te rendonte mbi proceset operative te kompanise si dhe ne kostot financiare per grumbullimin, ruajtjen/manaxhimin e ketyre te dhenave. Per kete arsye C kerkon qe ky nen/pike te ndryshohet/modifikohet si me poshte;

Neni 10/7;

AKEP mund te kerkoje te dhena te tjera shtese, pervec atyre ne formularin perfundimtar, ne lidhje me incidentin e sigurise. Per kete arsye, operatoret jane te detyruar te ruajne te gjithe te dhenat ne lidhje me incidentet e sigurise se raportuar per nje periudhe kohore prej 6 muajsh nga koha e dorezimit te njoftimit perfundimtar rreth incidentit te sigurise.

Qëndrimi i AKEP : *AKEP merr ne konsiderate komentin e C dhe jane pasqyruar ndryshimet perkatese ne nenin 10, pika 7 ku periudha kohore eshte bere 6 muaj.*

Sipërmarrësi B

Pika (2), Sipërmarrësit e komunikimeve elektronike që rezultojnë sipas raportimeve të kryera në AKEP me të ardhura vjetore te vitit paraardhës nga komunikimet elektronike mbi vlerën 100,000,000 lekë, duhet që të dorezojnë pranë AKEP raportin me rezultatet e auditit të sigurisë, të kryer nga një organ i çertifikuar dhe i pavarur ose nga autoriteti kompetent.

Raporti duhet të dorëzohet periodikisht për një periudhë jo më shumë se dy vjecare. Kostoja e auditit do të paguhet nga sipërmarrësi.

Komenti i B : Këto Audite kanë një kosto të lartë pasi bazohen në numrin e sistemeve, aplikimeve dhe pajisjeve që do të jenë në proces. Në disa raste mund të krijojnë dhe probleme me shërbimet e biznesit. AKEP mund të marrë në konsideratë që kjo periudhë kohe të jetë më e madhe.

Qëndrimi i AKEP:
AKEP vlereson se periudha 2 vjecare eshte kohe e mjaftueshme per te kryer nje audit sigurie.

Pika 2. Duhet përcaktuar qartë kush është organi i çertifikuar, ose autoriteti kompetent. Zakonisht këto audite bëhen nga trupa çertifikuese të cilat gjithashtu kërkojnë një audit të brendshëm paraprak. Për plotësimin e kësaj pike, duhet që operatorëve t'i lihet një kohë më e gjatë në dispozicion në mënyrë që të implementojnë kërkesat.

Qëndrimi i AKEP:
AKEP ben me dije se eshte ne vullnetin e kompanise te zgjedhe auditin e certifikuar i cili te jete i pavarur nga operatori, por duke plotesuar kushtet qe te jete i certifikuar edhe per ISMS (Information Security Managment Systems).

Neni 11

Sipërmarrësi A

Ne nenin 11 pika 1. A sugjeron qe ne fund te fjalise te shtohet pjesa, "....me kerkesen e AKEP', ne menyre qe sipermarresit te ofrojne informacion lidhur me politikat e dokumentuar ate sigurise me kerkesen e AKEP.

Qëndrimi i AKEP:
AKEP vlereson se komenti i A eshte i perfshire me kete pike te nenit.

Sa i perket nenit 11 pika 3. A vlereson se informacioni i shkembyer me AKEP lidhur me incidentet perben informacion konfidencial te operatorit e duhet trajtuar si i tille nga AKEP ne baze te Ligjit 9918/2008, neni 8 pika nje, neni 16 pika 5, e nuk duhet te publikohet pa pelqimin paraprak te sipermarresit. Per me teper, publikimi i informacionit lidhur me incidentet e sigurise vleresojme se eshte ne objektin e veprimtarise ligjore te ALCIRT, i cili eshte autoriteti pergjegjes qe ne bashkepunim me sipermarresit dhe ne baze te ligjit (ende draft) "Per administrimin e sigurise kibernetike", do te duhet te percaktoje kriteret dhe kushtet e qarta e transparente, qe duhet te permbushen ne menyre qe nje incident sigurie te behet publik. Bazuar ne sa me siper, per nevojat e kesaj Rregulloreje propozojme qe ne fund te paragrafit 3 te nenit 11 te shtohet:

" per sa kohe qe nuk cenon integritetin e rrjeteve te operatorit dhe nuk shperndan informacion konfidencial ose sekret biznesi"

Qëndrimi i AKEP:
AKEP duke respektuar parimet e konfidencialitetit i qendron pikes 3 te nenit 12 pasi eshte e bazuar ne ligjin nr.9918 datë 19.5.2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë", i ndryshuar, neni 122, pika 12:

> *"AKEP-i mund të informojë vetë publikun ose të kërkojë nga sipërmarrësi që ta njoftojë atë, nëse vlerëson që bërja publike e kësaj shkeljeje është në interes të publikut."*

Sipërmarrësi C

Se fundmi, persa i perket nenit 11, paragraf 3, ne te cilin prashikohet qe AKEP per arsye sigurie mund te njoftoje publikun rreth incidenteve te sigurise qe kane ndodhur ose qe mund te ndodhin, edhe pa marre pelqimin paraprak te operatorit;
C kerkon qe ne kete nen, ose te hiqet pjesa " edhe pa marre pelqimin paraprak te operatorit" dhe te behet "me pelqimin paraprak e operatorit" ose te garantohet kujdesi nga AKEP per mos cenimin e imazhit te operatorit nga publikime te tilla apo menyra e publikimit.

Qëndrimi i AKEP:

AKEP duke respektuar parimet e konfidencialitetit i qendron pikes 3 te nenit 12 pasi eshte e bazuar ne ligjin nr.9918 datë 19.5.2008 "Për Komunikimet Elektronike në Republikën e Shqipërisë", i ndryshuar, neni 122, pika 12:

> *"AKEP-i mund të informojë vetë publikun ose të kërkojë nga sipërmarrësi që ta njoftojë atë, nëse vlerëson që bërja publike e kësaj shkeljeje është në interes të publikut."*

Sipërmarrësi B

Per arsye sigurie, AKEP duke patur Raportin e Vleresimit te Impaktit mund te njoftoje publikun rreth incidenteve te sigurise, qe kane ndodhur ose qe mund te ndodhin ne te ardhmen ne komunikimet elektronike publike edhe pa marre pelqimin paraprak te operatorit.
Komenti i B : AKEP mund të publikojë këtë raport mbasi të ketë marrë prej Operatorit Raportin e Vlerësimit së Impaktit.

#SO 11: Kontrolli i aksesit në rrjetin dhe sistemet e informacionit.

Komenti i B: Regjistrimet e hyrjeve/Logs që do të jenë qëllimi i proceseve duhet të jenë te lidhura vetëm me regjistrimet e të dhënave kritike.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e B. Pika 3 e nenit 12 behet si me poshte:
"Per arsye sigurie, AKEP mund te njoftoje publikun rreth incidenteve te sigurise, qe kane ndodhur pasi ka marre vleresimin e impaktit te incidentit te sigurise ose qe mund te ndodhin ne te ardhmen ne komunikimet elektronike publike edhe pa marre pelqimin paraprak te operatorit".

Sipërmarrësi B kerkon qe neni 11 te riformulohet si me poshte:

Investigimi i Incidenteve te Sigurise dhe Cenimit te Integritetit

Duke vleresuar nivelin e riskut te incidentit te sigurise dhe/ ose cenimit te integritetit te raportuar sipas Formularit ne aneksin 1, AKEP mund te ndermarre veprimet e nevojshme per investigimin e ketij incidenti te sigurise dhe po ashtu per sqarimin e te gjitha rrethanave percaktuar nga njoftimi i operatorit.

Qendrimi i AKEP:
Komenti i sipercituar eshte i njejte dhe ne perputhje me percaktimin e kesaj pike ne rregullore.

Nese eshte e nevojshme, ne kuader te investigimit, AKEP do te informoj Agjensine Kombetare te Sigurise Kompjuterike (ALCIRT) dhe organet e tjera konpetente ne perputhje me legjislacionin për transmetimin e te dhenave nderkombetare.

Qendrimi i AKEP:
Komenti i sipercituar eshte i njejte dhe ne perputhje me percaktimin e kesaj pike ne rregullore.

Per arsye sigurie, AKEP duke patur Raportin e Vleresimit te Impaktit mund te njoftoje publikun rreth incidenteve te sigurise, qe kane ndodhur ose qe mund te ndodhin ne te ardhmen ne komunikimet elektronike publike edhe pa marre pelqimin paraprak te operatorit.

Qendrimi i AKEP:
AKEP merr ne konsiderate komentin e ardhur nga operatori B, i cili eshte reflektuar ne piken 3 te nenit 11.

Neni 12

Sipërmarrësi A

Ne nenin 12 pika 1, referenca e nenit ne piken e pare nuk kane permbushur nje ose disa nga detyrime te nenit 5 duhet te jete neni 6.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e A.

Ne nenin 12 pika 3, sugjerojme qe te ndryshoje si vijon: "Kane bere qellimisht vleresim jo te vertete te impaktit te incidentit te sigurise duke menjanuar ne kete menyre detyrimin e raportimit sipas standardeve te sigurise ISO.

Qëndrimi i AKEP:
AKEP i qendron perckatimit te kesaj pike.

Neni 13

Nuk ka

Neni 14

Nuk ka

Aneksi 1

Sipërmarrësi A

Ne Aneksin 1 - seksioni Pershkrimi i incidentit te sigurise dhe/ose cenimit te integritetit tek pika "Zona gjeografike e prekur nga Incidenti i sigurise dhe/ose cenimi i integritetit" sugjerojme qe te percaktohet njesia e raportimit (p.sh. km^2).
Me tej lidhur me plotesimin e pikave "Burimet e prekura" dhe "Pasojat" kerkojme sqarim per menyren e plotesimit.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e A duke shtuar njesine km^2 ne piken perkatese. Ne lidhje me kerkesen per sqarim ben me dije se me "Burimet e Prekura" i referohet sistemeve dhe sherbimeve te operatorit te cilat jane prekur nga incidenti. Me "Pasojat" i referohet efekteve dhe demeve te cilat ka sjelle incidenti.

Sa i perket menyres se plotesimit te fushes "Numri i perdoruesve", ne Aneksin 1, propozojme ne qe vleresimi i numrit total te persoruesve te prekur te behet duke marre parasysh numrin e perdoruesve te cileve nje stacion i sherben ne 24 ore/ si mesatare e nje muaji.

Qëndrimi i AKEP:
AKEP merr ne konsiderate komentin e A dhe se eshte ne gjykimin dhe vleresimin e operatorit qe te jap nje numer te perafert te perdoruesve ne rastet kur nuk eshte e mundur vleresimi i sakte i numrit te pajtimtareve te prekur.

Sipërmarrësi B

Tek pjesa" Fushat e Formularit të raportimit të incidenteve" termi autoritetet rregullatore duket sikur është përdorur gabim në vend të termit "operator"

Qëndrimi i AKEP:
AKEP ben me dije se termi "autoritetet rregullatore" eshte perdorur ne menyre te sakte.

Aneksi 2

Sipërmarrësi A

Ne Aneksin 2 "Tabela per vleresimin e impaktit te incidentit te sigurise", ne seksionin e pare "kohezgjatja e incidentit te sigurise", propozojme qe "vjedhja" te hiqet pasi kohezgjatja e saj nuk mund te matet.
Gjithashtu, ne perputhje mesa kemi komentuar ne piken 10 me siper te komenteve tona, propozojme qe impakti lidhur me numrin e perdoruesve te ndahet ne mesatar dhe te larte si me siper.

Qëndrimi i AKEP:
AKEP merr ne konsiderate propozimin e A duke e hequr termin "vjedhja" nga seksioni i pare ne Aneks 2 dhe duke bere ndryshimet perkatese ne rregullore.

Sipërmarrësi B kerkon qe aneks2 te riformulohet si me poshte:

TABELA PER VLERESIMIN E IMPAKTIT TE INCIDENTIT TE SIGURISE		
Kohezgjatja e incidentit te sigurise(nderprerjes se sherbimit, interceptimit te komunikimeve, softëare te demshem, vjedhja, modifikimi i te dhenave)	Me teper se 1 ore, por me pak se 2 ore	Me teper se 4 ore
Numri i perdoruesve te prekur nga incidenti ose % e tyre ndaj numrit total te perdoruesve te ofruesit		
>1000 ose <5%	I Ulet	Mesatar
Ne rast te nje numri te panjohur te perdoruesve te prekur nga incidenti i sigurise, zona gjeografike e shtrirjes se incidentit te sigurise		
>10 km²	Mesatar	I Larte
Vleresimi Perfundimtar i Impaktit:	Mesatar	I Larte

Qëndrimi i AKEP:
AKEP i qendron percaktimeve dhe parametrave sipas ANEKS 2 "TABELA PER VLERESIMIN E IMPAKTIT TE INCIDENTIT TE SIGURISE"

Aneksi 3

Sipërmarrësi B Albania

Pika SO1- . masat e sigurisë pika 2.e dhe SO 4 – pika 2 D. Rishikimi i politikës së sigurisë pas çdo incidenti nuk mund të jetë mandator dhe shpesh është i panevojshëm. Detyrimi për të riparë politikën apo çdo dokument tjetër pas çdo incidenti, duhet të jetë vetëm nëse investigimi ka nxjerrë si konkluzion nevojën për përditësim.

Qendrimi i AKEP:
AKEP merr ne konsiderate komentin e operatorit B, pika 2 e), SO1 ndryshon dhe behet si me poshte vijon:
"Rishiko politikën e sigurisë pas incidenteve nese konsiderohet e nevojshme."

AKEP merr ne konsiderate komentin e operatorit B, pika 2 d), SO4 ndryshon dhe behet si me poshte vijon:
"Rishiko politikën e sigurisë për palët e treta, pas incidenteve ose ndryshimeve nese konsiderohet e nevojshme"

Sipërmarrësi B kerkon qe aneks 3 te riformulohet si me poshte:

D5: Menaxhimi I Incidenteve
SO 17: Procesi i Zbulimit të Incidenteve

Qendrimi i AKEP :
AKEP merr ne konsiderate propozimin e operatorit B duke bere ndryshimet perkatese.

D6: Menaxhimi I Vazhdimit të Biznesit

SO 19: Strategjia e Vazhdimit të Shërbimit dhe Disaster Recovery

Qendrimi i AKEP :
AKEP i qendron percaktimit te pikes SO19 ne Aneks 3.

SO 20: Aftësia e Rregullimit të Pasojave

Qendrimi i AKEP :
AKEP i qendron percaktimit te pikes SO20 ne Aneks 3.

SO 21: Planet e Emergjencës

Qendrimi i AKEP :
AKEP i qendron percaktimit te pikes SO21 ne Aneks 3.

SO 22: Qeverisja dhe Menaxhimi i Riskut

Qendrimi i AKEP :
AKEP merr ne konsiderate propozimin e operatorit B duke bere ndryshimet perkatese.

	standartet e industrisë. d) Siguro që personeli kryesor përdor metodologjinë dhe mjetet e menaxhimit të riskut e) Rishiko vlerësimet e riskut pas ndryshimeve ose incidenteve. f) Siguro që risqet e mbetura pranohen nga menaxhimi.	*• Udhëzimi për personelin në vlerësimin e risqeve. • Listë e risqeve dhe evidencë e rishikimeve/përditësimeve. • Rishiko komentet ose ndryshimet në vlerësimet e risqeve. • Miratimi dhe aprovimi i menaxhimit për risqet e mbetura.*

Qendrimi i AKEP :
AKEP merr ne konsiderate propozimin e operatorit B duke bere ndryshimet perkatese.

SO 11: Kontrolli i Aksesit në rrjet dhe sistemet e informacionit

	Masat e Sigurisë	*Evidenca*
1	*a) Përdoruesit dhe sistemet kanë identifikim unik dhe autentikohen dhe autorizohen kur aksesojnë shërbimet ose sistemet.* *b) Implemento mekanizmin e duhur të kontrollit logjik për rrjetin dhe sistemet e informacionit për të lejuar*	• *Loget e aksesit tregojnë identifikues unik për përdoruesit dhe sistemet kur lejojnë ose mohojnë aksesin.* • *Përmbledhje e autentikimit dhe metodave të kontrollit të aksesit për sistemet dhe përdoruesit.*

Qendrimi i AKEP :
Komenti i sipercituar eshte i njejte dhe ne perputhje me percaktimin e kesaj pike ne rregullore.

SO 16: Incident Management Procedures

	Masat e Sigurise	Evidencat
3	d)Investigimi i incidenteve kryesore dhe raportimi i tyre final, duke perfshire veprime lehtesuese te ndermarra dhe rekomandime per te zvogeluar incidente te ngjashme e)Vleresimi i politikave te menaxhimit te incidenteve / procedurave bazuar ne incidente te shkuara.	•Raporte individuale i perballimit te shumices se incidenteve Perditesimi i politikave te menaxhimit / procedurave , rishikim komentesh dhe/ ose ndryshim i logs.

Qendrimi i AKEP :
AKEP merr ne konsiderate propozimin e operatorit B duke bere ndryshimin perkates.

SO 17 : Aftesia e zbulimit te incidenteve

	Masat e Sigurise	Evidenca
2	b) Implementimi ne sisteme konfigurimet standarde të industrisë dhe procedurat për zbulimin e incidentit. c) Implementimi i sistemeve dhe procedurave për regjistrimin dhe përcjellja incidente ne kohë te njerëzit e duhur.	Sistemet dhe procedurat e zbulimit te incidentit, të tilla si incidentet e Sigurise dhe për Menaxhimin e Ngjarjeve (SIEM) mjete, Helpdesk siguri për personelin, raportet dhe advisories nga kompjuteri Ekipet emergjente Përgjigje (certs), mjetet për vend anomali, e të tjera.

Qendrimi i AKEP :

AKEP merr ne konsiderate propozimin e operatorit B duke bere ndryshimin perkates.

SO:21 Politikat e Logimit dhe Monitorimit

	Masat e Sigurise	Evidenca
1	a)Imlementimin e monitorimit dhe loggin e te dhenave kritike	•Logot dhe raportet e monitorimit të rrjetit kritik dhe të sistemeve te informacionit.
2	b) Implementon politikën e ngjarjeve dhe monitorimin e sistemeve kritike. c) Vendos mjete për monitorimin e sistemeve kritike d) Vendos mjetet për të mbledhur dhe ruajtur shkrimet e te dhenave kritike.	•Politika te dokumentuara për monitorimin dhe ngjarjet, duke përfshirë kerkesat minimale per monitorimin dhe ngjarjet, periudhën e mbajtjes, dhe objektivat e përgjithshme të ruajtjes monitoringdata dhe shkrimet. • Mjetet për sistemet e monitorimit dhe mbledhjen e logeve

Qendrimi i AKEP :
AKEP i qendron percaktimit te pikes SO21 ne Aneks 3.

Sipërmarrësi D

AKEP ne VKD nr. 2592 shprehet se eshte bazuar per nxjerrjen e kesaj rregulloreje ne nenin 122 te Ligjit nr.9918 date 19.05.2008 "Per komunikimet elektronike dhe postare ne Republiken e Shqiperise", i ndryshuar, i cili trajton masat mbrojtese qe duhet te merren nga sipermarresit ne kuader te mbrojtjes se te dhenave dhe te privatesise.
Por, me tej sqaron se kjo rregullore, perafron Nenin 13 s) Kapitulli III s) te Direktives Kuader 2002/21/EC e amenduar i cili trajton sigurine dhe integritetin e rrjeteve dhe sherbimeve me Nenin 4 te Direktives e-Privacy ne te cilin percaktohet detyrimi per sigurine e rrjetit ne kuader te mbrojtjes se te dhenave personale, duke percaktuar ne objektin e rregullores dhe ne nenet e saj njekohesisht detyrime per sipermarresit si per garantimin e funksionalitetit te rrjetit/sherbimeve ashtu edhe per konfidencialitetin e ofrimit te sherbimeve.
D, gjykon qe keto detyrime duhet te percaktohen ne rregullore te veganta duke specifikuar perkatesisht procedurat respektive. Konkretisht, detyrimi per te marre masa per te garantuar sigurine, integritetin dhe mirembajtjen e funksioneve te rrjeteve te komunikimit elektronik eshte parashikuar ne Nenin 7 pika 3 d) te Ligjit nr.9918, piken 9.1 a) te Aneksit C te Rregullores Nr. 24 date 02.02.2012 "Per Autorizimin e Pergjithshem" si dhe Rregullores nr.31, date 26.12.2013 "Per termat e pergjithshme te kontrates se pajtimit per lidhjen dhe aksesin rrjetin publik te komunikimeve elektronike". Megjithate transpozimi i plote i Nenit 13 s) Kapitulli III s) te Direktives Kuader 2002/21/EC e amenduar, ne lidhje me marrjen e masave per integritetin e rrjeteve dhe vazhdueshmerine e ofrimit te sherbimeve ne keto rrjete, mund te kryhet ne nje rregullore te vecante, pra duke e trajtuar ne menyre te pavarur nga mbrojtja e te dhenave dhe e privatesise.
Ne lidhje me detyrimet mbi masat mbrojtese per te realizuar sigurine dhe integritetin e rrjeteve ne kuader te mbrojtjes se te dhenave dhe privatesise te percaktuara ne Nenin 122 te ligjit nr.9918, piken 9.3 te Aneksit C te Rregullores Nr. 24 si dhe ne Termat e Pergjithshme te Pajtimit, D thekson se i ploteson te gjitha keto detyrime dhe se ka derguar dokumentacionin e plote per zbatimin e tyre prane AKEP me shkresen nr. 51 date 26.01.2015.

Per sa i perket marrjes se masave per sigurine dhe integritetin e rrjetit per vazhdueshmerine e ofrimit te sherbimeve per pajtimtarin, D ka qendrimin e tij dhe komentet perkatese, per i kerkon AKEP se pari parashikimin dhe detajimin e tyre ne nje rregullore te vecante.
Sa me lart, D sugjeron organizimin e nje takimi sqarues nga AKEP me palet e interesuara per trajtimin e problematikave te mesiperme, te cilat i shohim se duhen trajtuar ne menyre te vecante nga njera tjetra, perpara dergimit te komenteve perfundimtare nga palet.

Qëndrimi i AKEP:
AKEP vlereson komentet e derguara nga D por gjykon se keto komente nuk kane te bejne me objektin e ketij konsultimi publik.