EESTI
INFOTEHNOLOOGIA JA
TELEKOMMUNIKATSIOONI
LIIT

Pr Liisa-Ly Pakosta
Justiits- ja digiminister
Justiits- ja Digiministeerium
Suur-Ameerika 1
10122 TALLINN

Teie 09.12.2024 nr 2-2/3131-1

Meie 3101.2025 nr 6.1-2/13

Arvamuse esitamine küberturvalisuse seaduse ja teiste seaduste muutmise seaduse (küberturvalisuse 2. direktiivi ülevõtmine) eelnõu kohta

Täname Teid Eesti Infotehnoloogia ja Telekommunikatsiooni Liidu (ITL) kaasamise eest küberturvalisuse seaduse (edaspidi: KüTS) ja teiste seaduste muutmise seaduse eelnõu (edaspidi: eelnõu) menetlusse, millega võtate üle Euroopa Parlamendi ja nõukogu 14. detsembri 2022. a direktiivi (EL) 2022/2555, mis käsitleb meetmeid, millega tagada küberturvalisuse ühtlaselt kõrge tase kogu liidus (edaspidi: NIS2 direktiiv). Oleme ITL-is eelnõud analüüsinud ning käesolevaga esitame selle kohta oma kommentaarid, küsimused ja ettepanekud.

I Peamised murekohad ja ettepanekud

Küberturvalisuse nõuete järgimine parandab ettevõtete ja asutuste toimepidevust ning konkurentsivõimet nii Eestis kui ka rahvusvaheliselt. Oleme üldiselt nõus, et eelnõuga laieneb kehtiva KüTS-i mõjuala kuid kohaldamisala laiendamine peab olema põhjendatud ja läbi mõeldud. ITL toetab NIS2 direktiivi eesmärke, eriti nõuete ja protseduuride ühtlustamist üle Euroopa Liidu. Leiame, et regulatsiooni eesmärk peab olema ka selle subjektidele väärtust luua, sealhulgas läbi selguse ja reaalselt parema küberturvalisuse. **Kahjuks on eelnõus väga mitmeid probleeme, millest peamised on kokkuvõtlikult järgmised:**

1) **Ülevõtmise eelnõuga NIS2 direktiivi kohaldamisala põhjendamatu laiendamine** Eestis, seda nii subjektide nimekirja pikendamise kui ka kohaldamisalas olevate teenusete keskselt lähenemiselt kogu ettevõtte tegevuse hõlmamisele üleminekuga;
2) **Eelnõu jõustamisega kiirustamine ettevõtetele mõistlikku rakendusaega jätmata** – üleminekuaega vajavad kõik subjektid (nii eelnõuga lisanduvad kui ka kehtiva KüTS-i subjektid selleks, et tagada võrdne kohtlemine);
3) **Eelnõu madal normitehniline kvaliteet ja vastuolu hea õigusloome tavaga**, mille tagajärjeks on regulatsiooni ebaselgus. Segane sõnastus nii olulises valdkonnas viib kaugemale õigusselgusest ning vähendab seega küberturvalisust.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Järgnevalt põhjendame oma seisukohti lähemalt ning esitame ka oma ettepanekud välja toodud murekohtade lahendamiseks:

1. Eelnõu eesmärk, kohaldamisala ja kohustuste laiendamine

1.1. Eelnõu materjalidega tutvuma asudes jääb esimesena silma, et puudu on eelnõu vastuvõtmise fookus ja eesmärk, mida Eestis saavutada tahetakse. Millist probleemi selle eelnõuga lahendatakse? Seda pole välja toodud. Mõistame, et tegemist on EL-i direktiivi ülevõtmise eelnõuga ja NIS2 direktiivi eesmärke me toetame. Siiski on tegemist eelnõuga, mis sätestab mitmeid uusi kohustusi väga suurele hulgale ettevõtetele ja asutustele. Seetõttu on vajalik ka selgesõnaliselt põhjendada, miks Eestis seadus sellisel kujul kavatsetakse vastu võtta. Ühe selge eesmärgi sõnastamine aitaks kindlasti kaasa kohustatud isikute suunas vajalikule selgitustööle. See aitaks põhjendada miks selliseid kohustusi kehtestada on vaja ja mis kasu nendest kohustatud isikutele endale sünnib.
ITL-i ettepanek: sõnastada selgelt, mis on eelnõu eesmärk ehk mille vastu need meetmeid kasutusele võetakse. Näiteks, et eelnõu eesmärk on kaitsta kriitiliste teenuste osutamist Eestis või et proportsionaalsed nõuded on vajalikud selleks, et ennetada teatud tagajärgi. Soovitame siduda eelnõu eesmärgi ka Eesti ettevõtete ja majanduse konkurentsivõime paranemisega.

1.2. Eelnõuga laiendatakse kehtiva KüTS-i kohaldamisala väga oluliselt ja rohkem kui NIS2 direktiiv seda ette näeb. See on risti vastupidine tegevus Vabariigi Valitsuse prioriteetsele eesmärgile, mille kohaselt tuleb ettevõtete halduskoormust ja dubleerivaid tegevusi vähendada. Eelnõu jõustumine toob kaasa äärmiselt suure halduskoormuse kasvu väga suurele hulgale ettevõtetele, sealjuures võrgu - ja infosüsteemide osas ilmselt kattuvalt (üht ja sama võrku või infosüsteemi hakatakse kontrollima teenuse kasutaja ja teenuse osutaja ning vahendaja poolt). Samuti lisandub suur täiendav koormus ka erinevatele riigiasutustele, kes peaks praegu hoopis kokkuhoiu kohti leidma. Eesti õigusega NIS2 direktiivi laiendamine ei ole kooskõlas ka NIS2 eesmärgiga ühtlustada küberturvalisuse nõudeid üle kõigi EL-i riikide, sest teiste riikidega võrreldes on Eestis juba tänase KüTS regulatsiooniga saavutatud märkimisväärselt kõrge turvalisuse tase.
NIS2 direktiivi KÜTS-i ülevõtmine laiendavalt on kavandatud näiteks järgmisega:

- ettevõtted, kelle üks teenus kuulub NIS2 direktiivi lisades 1 ja 2 nimetatud sektoritesse, peavad eelnõus sätestatud meetmed kohaldama kogu oma tegevusele, mitte üksnes NIS2 direktiivis nimetatud teenuste osutamisele. KüTS-i kohaldamisalasse kuuluv teenus võib olla ettevõtte enda vaates kõrvaltegevus või ebaproportsionaalselt väikese mahuga võrreldes KüTS-i kohaldamisega kaasnevate kohustustega. Sellisel viisil terve ettevõtte üle kontrolli teostamine ja ülemäärane reguleerimine ei ole põhjendatud;
- turvanõuete koosseisu ja kohustuste vähesel määral täiendamine. Samas seda tehakse nii, et need subjektid, kes peavad oma vastavust rahvusvaheliselt tõendama, peavad eelnõu vastuvõtmisel hakkama selle protsessi käigus selgitusi jagama, millised nõuded on Eestis siseriiklikult juurde lisatud. See suurendab taaskord halduskoormust.

Kehtiva KüTS-i laiendamise näite leiame eelnõu § 1 punktiga 27 **KüTS-i lisatavast § 7 lõige 2[1]. See tekitab segadust, kuna sätestab E-ITS-iga samad reeglid ja ka eelnõu seletuskirjas viidatakse otseselt E-ITS-ile. Kuivõrd KüTS § 7 lg 5 jääb samale kujule (ei plaanita eelnõuga muuta), siis tekib olukord, kus ettevõtted ja nende teenuse osutajad, kes vastavad ISO 27001**

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

standardile, peaksid justkui hakkama rakendama lisaks ka E-ITS-i. Kuigi E-ITS koostamisel on kinnitatud, et on järgitud ISO 27001 reegleid, siis tegelikkuses ei ole seda täiesti üksühele tehtud. Näiteks standardist ISO 27001 ei tule välja samas sõnastuses mõisted ega ole reguleeritud eraldi kaitsetarbe määramise osa. Eelnõu seletuskirjas ei ole hetkel selgitatud, kuidas ISO 27001 rakendajad seda nõuet peaks täitma. Sellise tõlgenduse kohaselt tõuseksid täiendavate auditeerimise kohustustega ka ettevõtetele kulud, mida hetkel ei ole arvestatud. Seletuskirjas ei ole täpsustatud ka ISO standardiga seotud osa, nt kuidas ISO 27001 rakendajad peavad vastama E-ITS või nüüd tulevikus KüTS § 7 lg 1^2 kaitsetarbe nõudele, mis on standardist õigusakti tasemele toodud. Seletuskirjas ei ole ka selgitust sellisel kujul standardi nõuete seadusesse kirjutamise kohta.

ITL-i ettepanek: mitte laiendada direktiivi kohaldamisala ja selles sisalduvaid kohustusi. Ettevõtete halduskoormus ja vastavuskulud on niigi suured. Seetõttu palume:

- tagada eelnõus mõistlik subjektide ring;
- muuta eelnõud nii, et ettevõtted on KÜTS-i kohaldamisalas ainult oma NIS2 kohaldamisalasse jääva tegevusega;
- kõrvaldada eelnõust ebaselgus seoses E-ITS standardi nõuetega ISO 27001 rakendajatele, kuna määruse „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ § 3 lg 2 kohaselt loetakse ISO 27001 standardile vastavus võrdseks E-ITS-ile vastavusega.

Põhjendame oma ettepanekuid järgmiselt:

- Eesti on väike riik, me peame mõtlema, millised on reaalsed ohud ja millised on reaalsed riskid ning kõrvutama seda sellega, mis läheb selle haldus maksma. Meie üleskutse on läbi mõelda, kuidas teha neid asju mõistlikumalt, läbimõeldumalt ning proportsionaalsetena.
- Subjektide nimekirja üle vaatamine ja sisulise kohaldamisala kitsendamine ning dubleerivate elementide eemaldamine vabastab ka asutuste ressurssi. Sellisel juhul ei pea nii suure hulga asutuste ja ettevõtete üle järelevalvet teostama, neid nõustama ja juhendama olukorras, kus tegelik mõjuulatus on väike või olematu. Selle asemel saab keskenduda olulise mõjuga teenuste turvalisuse tagamisele ja tõstmisele.
- NIS2 direktiivi ülevõtmisega ei tohi kaasneda näiteks turvanõuete või ainult Eestis kohaldatavate kohustuste lisamist, et mitte tekitada liiga palju riiklikke eripärasid, mis muudavad keerukamaks ja kallimaks Eesti teenused ja tooted ning annavad teistele konkurentsieelise. Kui teenuseosutajat hakatakse sertifitseerima näiteks EL-i küberturvalisuse sertifitseerimisskeemi alusel, siis KüTS-i eripärad tekitavad keerukust ja bürokraatiat, samuti ebavõrdsust erinevate riikide järelevalve alla kuuluvate teenusosutajate vahel.
- Senise teenusepõhise lähenemise juurde jäämist toetab ka see, et nii või teisiti peavad seonduvad süsteemid ja tegevused, sh partneritega seonduv olema riskihinnangus kajastatud, hinnatud ja turvalisus tagatud. Ettevõte tervikuna ei peaks siiski olema Riigi Infosüsteemi Ameti (RIA) poolt kontrollitav. RIA kontroll võib olla ebaproportsionaalne ja ülemäärane ettevõtte üle tervikuna, kui KüTS kohaldamisala alla jääv teenus ei ole ettevõtte põhitegevus.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

1.3. Eelnõu jätab KüTS kohuslaste nimekirja lahtiseks, kuna kehtestab Vabariigi Valitsuse jaoks volitusnormi (eelnõu § 1 p 1 - KüTS § 1 lg 1^6) uute kohuslaste lisamiseks määrusega. Näeme seoses sellega mitmeid olulisi probleeme:

1.3.1. Kavandatav volitusnorm on liiga lai. See on seotud eelnõu § 1 punktiga 1 KüTS § 1 lisatavas lg 1^4 toodud kriteeriumitega, kuid siiski jääb ebaselgeks, millistel alustel uusi subjekte lisama hakatakse ning kas seejuures saab olema tagatud võrdne kohtlemine.

1.3.2. Volitusnormi lisamise põhjus on arusaamatu. Miks see on lisatud ja mis mõju sellest oodatakse? Eelnõu seletuskirja lugedes jääb mulje nagu oleks see säte lisatud igaks juhuks, kui keegi eelnõust kogemata välja on jäänud. Samal ajal on subjektide ring juba eelnõus toodud loetelu kohaselt väga laiaulatuslik ja ebamäärane (ei saa aru, kellele see kohaldub).

1.3.3. Volitusnormi lisamise põhjendus jääb arusaamatuks ka seetõttu, et eelnõu seletuskirjas (lk 53-54) juba kirjeldatakse võimalikke uusi sektoreid kes võiksid saada KÜTS-i kohuslasteks, kuid hiljem (lk 129) öeldakse, et volitusnormi ei plaanita siiski kohe kasutada ehk tegu on tuleviku jaoks mõeldud paindlikkust lisava võimalusega.

1.3.4. Volitusnormi lisamine läheb vastuollu seaduse mõttega. Osa subjekte määratakse kohe seadusega ja teised hiljem rakendusaktiga. Leiame, et subjektide lisamine peab toimuma kõigi jaoks sama õigusakti (ehk siis seaduse) tasemel.

ITL-i ettepanek: jätta eelnõu § 1 punktiga 1 KüTS §-i 1 lisatav lõige 1^6, millega antakse Vabariigi Valitsusele õigus määrata määrusega valdkonna või sektori, milles oleva isiku suhtes kohaldatakse teenuse osutaja kohta sätestatut olenemata tema suurusest, eelnõust välja. Samuti jätta eelnõust välja seotud säte KüTS § 3 lg 1^4.

1.4. Eelnõust jääb ebaselgeks, kuidas kohuslaseks olevad isikud teada saavad, et nad eelnõus sisalduvaid kohustusi täitma peavad. Eelnõu § 1 punktiga 18 muudetav KüTS § 3 lg 3 sätestab, et RIA tuvastab iga kahe aasta tagant KüTS-i kohaldamisalas olevad teenuse osutajad. Selleks peavad teenuse osutajad hakkama ise RIA-le infot edastama ja RIA omakorda teavitab Eesti teenuse osutajatest Euroopa Komisjoni. Sellest protsessist on puudu osa, kuidas teenuse osutajad ise saavad teada, et neile võib kohalduda või RIA neile kinnitab, et nad on tõepoolest KüTS-i kohaldamisalas.

ITL-i ettepanekud:

- Lisada eelnõusse järgmine protsess:
  - RIA kohustus teavitada võimalikuks subjektiks saamisest isikuid eelotsusena;
  - siis antakse ettevõttele või asutusele võimalus ise hinnata ennast (enda tegevust) vastavalt KüTS-is toodud kriteeriumitele;
  - seejärel väljastab RIA haldusakti, misjärel algab kaheaastane aeg ehk selliselt saaks ka kohuslaseks määramise algusaeg korrektselt fikseeritud.
- Lisada eelnõusse RIA kohustus avalikustada KüTS-i subjektide nimekiri koos põhjendusega, miks seal nimekirjas ollakse (s.t viide asjakohasele KüTS-i sättele). Juhul, kui see on vajalik, siis võib anda RIA-le õiguse otsustada mitte kõiki subjekte avalikustada, kuid sellised erandid peavad olema põhjendatud. Samas on oluline, et mitte avalikustatud subjekti lepingupartnerid teaksid tema subjekti staatusest.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Põhjendame oma käesolevas punktis tehtud ettepanekuid järgmiselt:

- Subjektide nimekirja avalikustamine aitab kaasa avalikule diskussioonile teemal, kellele on mõistlik neid kohustusi kehtestada ja kellele mitte.
- Subjektide nimekirja avalikustamine aitab tagada õigusselguse. Ühiskonnale peab olema mõistetav, kes ja miks subjektina KüTS-i kohaldamisalasse hõlmatud on.
- Eelnõu konkreetne kohaldamisala ja subjektide avalik nimekiri tõstab riigi turvalisust, kuna võimaldab ettevõtetel ja asutustel koostöös paremini valmistuda võimalikeks kriisiolukordadeks. Näiteks nõutakse eelnõu § 1 punktiga 26 KüTS § 7 lg 2 punktis 6, et teenuse osutaja tagaks süsteemi tarneahela turvalisuse, sh teenuse osutaja ja tema koostööpartnerite vaheliste lepetes turvameetmetega seotud aspektide regulaarse ülevaatuse ning ajakohastamise. Selle kohustuse täitmiseks on abiks, kui teenuse osutaja teab, kes ta partneritest või klientidest ka KüTS-i kohuslased on.

1.5. Eelnõust jääb ebaselgeks, kuidas hakkab toimuma subjektide lisamine nimekirja ning nende liikumine kahe nimekirja (elutähtsad ja olulised üksused) vahel. Kuna vahe tegemine on seotud ettevõtte suurusega, nt käibe ja töötajate arvuga, siis saab see olema dünaamiline.

ITL-i ettepanek: välja mõelda ja lisada eelnõusse protsess ja mehhanismid olukordadeks, kui ettevõtte suurus muutub kahe aastase perioodi keskel. Kui otsus on, et kaheks aastaks nimekirjad külmutatakse ja liikumist ei toimu, siis selgitada seda vastava sätte juures eelnõu tekstis.

2. Jõustumisaeg

2.1. Eelnõu jõustumisega seonduv on ebaselge. Eelnõu tutvustamisel on Justiits- ja Digiministeeriumi poolt välja öeldud, et uued subjektid saavad ülemineku aja kolm aastat. Eelnõu materjalidega tutvudes sellist sätet ei leia. Eelnõu rakendusakti kavandist (määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded“ muutmine) leiab üleminekuaja uutele elutähtsa teenuse osutajatele (neil on aega KüTS-i rakendamiseks tähtajani, mis määratakse nende elutähtsa teenuse osutajaks määramise haldusaktis). Lisaks on üleminekuaeg 3 aastat ette nähtud kõigile uutele KüTS-i subjektide standardi (E-ITS või ISO/IEC 27001) rakendamise kohustuse osas, kuid mitte muude kohustuste osas. Eelnõus endas rakendusaega (rakendussätteid selle kohta) ei ole. See ei ole loogiline, et eelnõu osade sätete jõustumine pannakse paika Valitsuse määrusega. Eelnõu § 11 kohaselt jõustub kogu eelnõu 1. juulil 2025. aastal ehk kohe pärast vastu võtmist.

2.2. Ilmselgelt vajavad uued subjektid ülemineku aega ka muude kohustuste osas. Samuti vajavad seda olemasolevad subjektid, sest täiendavaid kohustusi ja uusi nõudeid lisandub ka neile. Näiteks tuleb mitmetel teenuse osutajatel hakata täitma mahukat Euroopa Komisjoni otsekohalduvat rakendusmäärust nr 2024/2690 täpsustatud turvanõuetega, mis suurendab halduskoormust ja tekitab nõuete rakendamisel erisusi. Laieneb kohaldamisalas olevate teenuste ulatus, näiteks usaldusteenuste ja sideteenuste osas. Vähem oluline pole, et muutub ka nõuete kohaldamisala ulatus. Kehtiva KüTS-i kohaselt on teenuse osutajatel kohustused konkreetse teenuse osutamisel süsteemi kasutamisel, eelnõuga planeeritakse kehtestada kohustused kogu ettevõtte tegevusele. Näiteks tuleb täiendada olulisel määral riskianalüüsi,

sisseostu protsessi ja lepinguid, koolituspõhimõtteid, auditeerimist ja tagada, et küberturvalisuse meetmed on täidetud kogu ettevõtte puhul.

ITL-i ettepanek: lisada eelnõusse rakendussäte, mille kohaselt on kõigil kohustatud subjektidel aega eelnõus sisalduvate kohustuste rakendamiseks 3 aastat alates seaduse avaldamisest Riigi Teatajas. Põhjusel, et KüTS eelnõuga kaasneb täiendavaid kohustusi, siis tuleb üleminekuaeg nende kohustuste osas anda kõigile kohustatud subjektidele, mitte üksnes uutele subjektidele. Selline lahendus tagab ka subjektide võrdse kohtlemise.

2.3. Eelnõu jõustumisega seonduvalt vajab selgitamist ka küsimus, millal muutuvad Eestis kohustuslikult täidetavaks Euroopa Komisjoni poolt kehtestatud NIS2 direktiivi otsekohalduvad rakendusaktid. Selles küsimuses esineb erinevaid tõlgendusi (s.h Euroopa Komisjoni ametnike poolt) alates sellest, et otsekohalduvaid rakendusakte peab täitma kohe, kuigi NIS2 pole veel Eesti õigusesse üle võetud kuni selleni, et rakendusaktid ei saa olla kohaldatavad kuni pole siseriiklikus õiguses alusnormi ehk rakendusakti aluseks olev NIS2 pole Eesti õigusesse üle võetud.

3. Eelnõu normitehnilisest kvaliteedist tulenev ebaselgus

3.1. Eelnõu on vastuolus hea õigusloome tavaga:

3.1.1. Normitehniliselt on eelnõu väga raskesti loetav:

3.1.1.1. Eelnõu esimesed paragrahvid on väga pikad ja pool NIS2 direktiivist on võetud üle KüTS-i esimesse paari sättesse. Ka muudatuste kogumaht on suurem kui KüTS-i kehtival tekstil. Mitmete pikkade ülamärkega sätete lisamine teeb seaduse lugemise ja sätete seoste jälgimise väga keeruliseks.

3.1.1.2. Eelnõu sisaldab väga palju viiteid teistele (Euroopa Liidu) õigusaktidele, kusjuures ka küsimustes, mille puhul õigusselgus on äärmiselt oluline, näiteks kohaldamisala.

3.1.2. Eelnõu seletuskiri on väga ebaühtlase kvaliteediga. See on väga mahukas, kuid väga paljude sätete selgituseks öeldakse, milline NIS2 artikkel (või põhjenduspunkti tõlgendus, mis tegelikult ei ole õigusnorm) üle võetakse ja seejuures sätte sisu ei selgitata üldse (näiteks eelnõu § 1 punkt 56 - KüTS § 17^4 lõiked 4-6 seletuskirja lk 103). On pikki paragrahve, mille puhul on valitud selgitada ainult ühte alapunkti (näiteks seletuskirja lk 77 selgitatakse eelnõu § 1 p 22 - KüTS § 5 lg 5 ainult punkti 10).

3.1.3. Eelnõu mõjuhinnang on puudulik ehk sisuliselt tegemata. Eelnõu seletuskirjas tunnistatakse otse, et majanduslik mõju subjektidele on erinev ja seda ei ole võimalik hinnata (lk 3). Eelnõu tegelik mõju on suur, kuna kohustatud isikute ring on väga suur ja kehtestavate kohustuste ulatus samuti. Samas on eelnõu seletuskirjas välja toodud ainult positiivsed mõjud. Negatiivseid mõjusid ei ole tuvastatud, kuid kas see tähendab, et neid tõesti pole? Näiteks ei ole analüüsitud mõjusid tänaste teenuste osutamisele – kindlasti kaasnevad kulud nõuete rakendamisega ja auditeerimisega, mis teeb teenused kallimaks, või et kas eelnõus sisalduvate küberturvalisuse nõuete täitmine toob kaasa ka selle, et mõni teenus läheb keerukamaks ja seega ka lõppkasutaja jaoks aeglasemaks või muutub tehnoloogilisse lahendusse lisanduva turvakomponendi tõttu mittekasutatavaks?

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

ITL-i ettepanekud:

- Palume vaadata eelnõu tekst üle ning järgida seejuures normitehnika eeskirja ja hea õigusloome tava reegleid eesmärgiga tagada eelnõu selgus ja arusaadavus ning sätete omavaheliste seoste jälgitavus.
- Palume kaaluda asendusseaduse ehk uue KüTS tervikteksti tegemist, sest muudatuste maht on võrreldes kehtiva seadusega väga suur.[1] See idee on väärt kaalumist ka seetõttu, et paralleelselt on Justiits- ja Digiministeeriumis ettevalmistamisel kehtiva KüTS-i revisjon (eelnõu seletuskiri lk 11-12) ehk sama seadust ootavad lähiajal ees järgmised (ulatuslikud?) muudatused.
- Viia läbi korrektne ja põhjalik mõjuanalüüs. ITL on valmis kaasa mõtlema, kuidas mõjuanalüüsi kõige paremini teha, et arvestatud saaksid kõik olulised mõjud.

Eelnõu kvaliteedi teemat kokku võttes tõdeme, et eelnõu on ilmselgelt ebaküps ning vajab põhjalikke muudatusi. Õigusakt peab olema selge ja kohustatud isikutele arusaadav, kuid praegusel kujul ei täida eelnõu seda nõuet. Seda näitab ka see, et eelnõu koostajad küsivad seletuskirjas mitmetes küsimustes huvigruppide arvamust, mis oleks pidanud olema tehtud enne eelnõu ametlikku kooskõlastust. Seletuskirja lisatud hinnangud kohaldamisalas olevate üksuste arvude kohta on väga umbkaudsed. Võib arvata, et ka valdkondlikud erialaliidud ei oska skoopi kuuluvate ettevõtete hulka hinnata, sest kohaldamisala on ebaselge. Seega eelnõust ei ole hetkel üheselt arusaadav, mis muret sellega lahendatakse, kellele see kohaldub ja mis mõjud sel on.

II Ettepanekud konkreetsete sätete muutmiseks

1. Kohaldamisala

Kohaldamisala laiendamise küsimust adresseerisime oma kirja I osa punktis 2, kuid kohaldamisala on segane ka sätete ülesehituse ja kasutatava terminoloogia tõttu. Kõigepealt sätestatakse, et eelnõu subjektid on üksused, siis loetletakse üles, milliste tunnustega üksused (lisandub suuruse aspekt) need on. Samas kohustused kehtivad teenuse osutajatele, kes on elutähtsad ja olulised üksused, kes on omakorda eraldi üles loetletud. Tekib küsimus, kas teenuse osutaja võrdub üksus. Üksuse mõiste on Eesti senist õigusruumi ja mõisteid arvestades ebaselge termin. Eelnõu lugeja peab kõvasti pingutama, et aru saada tervikpildist (kes mida tegema peab, kellele kohaldub).

ITL-i ettepanek: vaadata üle kohaldamisala sätted ja tagada arusaadavus. Lisada seletuskirja jooniste kujul ülevaade, kes on subjektid ja millised kohustused neile rakenduvad. ITL-i konkreetsemad ettepanekud on leitavad käesoleva kirja lisast.

2. Mõisted

Eelnõu § 1 punktidega 7-14 lisatakse KüTS-i §-i 2 hulgaliselt uusi mõisteid. Mitmed neist mõistetest viitavad EL-i õigusaktidele ja on seetõttu keerulised lugeda ning aru saada, eriti just KüTS-i uute subjektide poolt. Osadest mõistetest ei saa aru ka eelnõu seletuskirja kõrvale lugedes. Näiteks hallatud teenuse osutaja ja hallatud turbeteenuse osutaja. Nende puhul on kindlasti vajalik leida

[1] Normitehnika eeskirja 13 sätestab järgmist: *Kui muutmisülesanne seisneb valdkonna ulatuslikus ümberkujundamises, siis on seaduse muutmise variant selleks ebasobiv, kuna tulemus ei ole ülevaatlik ega tõsta esile muudatuse õiguspoliitilist olemust ja tähendust*.

arusaadavamad ehk sisu rohkem avavad mõisted eelnõusse või kasutada Eesti õigusruumis juba kasutusel olevaid mõisteid.

ITL-i ettepanek: kirjutada võimalikult palju mõisteid eelnõu tekstis lahti (mitte kasutada viiteid) ja vaadata üle ka seletuskirjas olevad sõnastused. See tagab eelnõu loetavuse ilma vajaduseta termineid muudest õigusaktidest otsida. Mõistete sätet on vaja kirjutada põhjalikumaks ja lisada sinna ka seletamata mõisteid, nt küberturvalisuse alane tegevus. ITL-i konkreetsed ettepanekud mõistete osas leiate käesoleva kirja lisast.
Erandina leiame, et usaldusteenuste ja kvalifitseeritud usaldusteenuste terminit ei ole vajadus eelnõus lahti kirjutada, kuna "kvalifitseeritud usaldusteenus" on niikuinii määratletud kui konkreetsele EU määrusele (nn eIDAS määrusele) vastav usaldusteenus.
Kuigi eelnõu § 1 punktidega 7-14 muudetava KüTS §-is 2 on juba kirjas, et "käesolevas seaduses kasutatakse termineid järgnevas tähenduses", siis teeme ettepaneku ükshaaval üle vaadata kas sama terminit kasutatakse mõnes teises õigusaktis samas kontekstis erinevalt. KüTS on nii paljude valdkondadega seotud, mistõttu tuleb tagada, et ei tekiks paralleeltermineid (eelnõus siiski on palju mõisteid erineva tähendusega kui mujal – kõige lihtsam näide on üldiselt kasutatava mõiste „risk" sisustamine küberturvalisuse kontekstis). Osa termineid on ka praegu sätestatud valdkondliku õigusaktiga ja on sama tähendusega, aga siiski tuleks tagada võimalikult hea ühtlustamine. Kui termin erineb muus õigusaktis olevast siis selguse mõttes on otstarbekas konkreetse termini juurde lisada „käesoleva seaduse tähenduses".

3. Pädevad asutused ja ülesanded

Eelnõu § 1 punktiga 22 muudetakse KüTS §-i 5 ja kirjutatakse põhjalikult lahti RIA pädevused ja ülesanded. Seda sätet lugedes tekib küsimus, kas see kõik peab ikka olema KüTS-is. Näiteks ei ole tavapärane kirjutada valdkonda reguleerivasse seadusesse, et asutusel peavad olema vahendid oma tegevuseks. See on nõue EL-i poolt liikmesriigile, mida liikmesriik peab täitma. KüTS-is on asjakohane reguleerida RIA õigusi sekkumiste teostamisteks teenuste osutajate üle ja ka RIA peamisi kohustusi.

Teise murekohana tekitab segadust see, et RIA kohustused ettevõtetele ja asutustele abi osutamiseks ei ole üheselt selgelt kirjas. Need on eelnõus küll nn põhimääruse osas (KüTS § 5 lg 5 p 9; § 5 lg 8 p 3) kirjas, aga see pole piisav. Lisaks on ka küberturbe intsidentide lahendamise üksusel (CSIRT) paar ettevõtete ja asutuste abistamise punkti (KüTS § 5 lg 5 punktid 4, 7, 8 ja 9). Samas on ka nendes kasutatud sõnu *vajadusel*, *taotluse korral* ning *asjakohasel juhul.* Eelnõu § 1 punktiga 56 eelnõusse lisatavas KüTS §-is 17[4] on koostöö ette nähtud ainult ETO-de ning elutähtsate üksustega. KÜTS-is on vastastikune abi pigem asutuste vahel (Eestis ja EL-is) järelevalve teostamisel. Meie hinnangul on KÜTS-is paigast ära proportsioon ettevõtetele/asutustele abi andmise osas (mis peaks olema väga oluline ning rõhutatud) ja järelevalve osas (järelevalve kasuks). Koostöö tegemist ning näiteks vabatahtlikku teavitamist ei peaks reguleerima õigusakti tasemel.

ITL-i ettepanekud:

- Jätta kas kõik või osa RIA-t puudutav (KüTS § 5 lg 4 – 8) eelnõust välja ning lisada need punktid RIA põhimäärusesse;
- kirjutada eelnõusse selgelt ühte sättesse RIA ülesanded ja kohustused ettevõtetele ja asutustele abi osutamiseks.

Seejuures tuleb arvestada, et RIA põhifunktsioon olla abistaja tähendab olla peamiselt eri osapoolte info koondaja intsidentide puhul. See ei tohi kindlasti tähendada erasektori poolt pakutavate teenustega konkureerimist (näiteks riiklik SOC ja riiklik PEN-test). Riik peab valima, kus ta teenuse osutajana sekkub. Sektor kindlasti ei oota seda, et RIA pakuks kõigile tuge ja kaitset ning asutuse töötajate arv pidevalt kasvaks. RIA ülesanne on olla ühtne kontaktpunkt.

4. Teenuse osutaja juhtorgani kohustused ja vastutus

Eelnõu § 1 punktiga 24 lisatakse KüTS-i uus säte § 6^1, mis kehtestab ettevõtte juhtorganile ja selle liikmetele kohustused kiita heaks turvameetmed, läbida erikoolitusi ja tagada töötajate koolitamine. Eelnõu § 1 punktiga 58 lisatakse ka karistus võimaliku rikkumise eest (KüTS § 18^4). Lisaks saab RIA õiguse nõuda ettekirjutusega elutähtsa üksuse nõukogult või osanikelt juhatuse liikme(te) volituste ajutist peatamist (eelnõu § 1 punktiga 58 lisatav KüTS § 14 lg 13 p 2). Täpsustatud ei ole, kas mõeldakse juhatuse esimeest või kõiki juhatuse liikmeid.

Tegemist on ühe probleemseima sättega eelnõus, mis tekitab küsimuse, kas keegi on mõelnud ka tagajärgedele, mis saab raskustes olevast ettevõttest, kelle juht ametist tagandatakse. Mõistame, et tegemist on NIS2 direktiivist tuleneva sättega, kuid sellist erasektori juhtimisse sekkumist Eesti õigusruum ei toeta. Juhtkonna liikme(te) kõrvaldamine ei aita kaasa rikkumise kõrvaldamisse ega kiiremasse tegutsemisse. Pigem motiveerib trahv asjad korras hoidma ning sunniraha rakendamise võimalus võiks olla Eesti õigusruumi sobiv meede. Samas tähendaks see ka järelevalveasutuse poolt vastavale menetlusvormile ettenähtud protseduuriliste normide järgimist.

Juhime ka tähelepanu, et säte on üle võetud erinevalt NIS2 direktiivist. NIS2 direktiivi artikkel 35 lõige 5 näeb ette, et pädevatel asutustel on õigus üksnes taotleda (mitte nõuda), et asjaomased organid või kohtud keelaksid kooskõlas liikmesriigi õigusega füüsilisel isikul, kes täidab selles elutähtsas üksuses tegevjuhina või seadusliku esindajana juhtimisülesandeid, selles üksuses ajutiselt juhtimisülesannete täitmise.

ITL-i ettepanekud:

- muuta KüTS § 14 lg 13 p 2 sõnastust selliselt, et RIA-l on õigus taotleda, mitte nõuda;
- muuta KüTS § 14 lg 13 p 2 sõnastust selliselt, et taotlus tuleb esitada kohtule, mitte elutähtsa üksuse nõukogule või osanikele;
- lisada eelnõu seletuskirja analüüs, kuidas hakkab selle sätte rakendamine praktikas toimuma, näitena kasutada börsiettevõtteid;
- lisada eelnõu seletuskirja ka analüüs, mis mõju on KüTS § 14 lg 1 p 1 ehk elutähtsa teenuse osutamise lõpetamisel ning hinnata üle, kes saab olema õigustatud sellist meedet kasutama (sellist otsust tegema).

5. Teenuse osutaja süsteemi turvameetmed

Eelnõu § 1 punktidega 25-28 muudetakse KüTS §-i 7. Antud muudatusega laiendatakse subjektide kohustusi. Üldise loogika järgi peavad olema turvameetmed kaetud, kui standard on rakendatud. Eelnõud lugedes aga selgub, et peab järgima lisaks standardile ka eelnõus toodud meetmeid. Kusjuures need meetmed on põhjalikult avatud eelnõu seletuskirjas.

Oluline probleem on see, et selle sätte lõikega 2 laiendatakse NIS2 direktiivi sõnastust. Käände muutmisega KÜTS-is on muudetud NIS2 direktiivi artikkel 21 lõike 2 punktide a)-j) sisu.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Jääb ebaselgeks, kas see on tahtlik või mitte. Oleme seisukohal, et kui NIS2 direktiiv jätab võimaluse subjektil midagi teha, siis ei tohi seda Eesti õiguses kohustuseks muuta.
Seetõttu tekib olukord, kus NIS2 direktiivi artikkel 21 lõike 2 punkt e) sätestab muuhulgas: "*meetmed hõlmavad sh. nõrkuste käsitlemist ja avalikustamist*". KüTS § 7 lg 1 punktis 7 näiteks on aga kohustuseks "*tagama sh. nõrkuste käsitlemise ja avalikustamise*". Kui NIS2 direktiiv ütleb, et avalikustamise protseduur/ulatus peab meetmetes kirjas olema, siis eelnõus on sellest saanud kohustus avalikustada.

ITL-i ettepanekud:

- **vaadata KüTS § 7 sõnastused üle eesmärgiga tagada arusaadavus ja kohustuste ühekordne rakendamine. Vt ka ITL-i konkreetseid märkusi ja ettepanekuid käesoleva kirja lisast;**
- **meetmete kirjeldus kehtestada eraldi rakendusaktina, mis võiks olla juhise kujul ehk elav dokument. Seaduse seletuskiri ei ole õige koht, kuna antud juhul ei ole tegemist kohustuste selgitamise, vaid sisustamisega.**

Eraldi rõhutame vajadust määrusega sisustada kohustusliku koolituse skoop ja nõuded koolituse läbimist tõendavale hindamisele. Kuna tegemist on sanktsioneeritava kohustusega, siis peab olema subjektidele selge, mida neilt nõutakse.

6. Eelnõu alusel vastuvõetava määrusega vastuolus oleva rakendusakti kohaldamine

Eelnõu § 1 punktiga 28 lisatakse KüTS § 7 lõige 6, mis räägib Euroopa Komisjoni rakendusaktist, mis ei pruugi olla eelnõuga kooskõlas ning kohustab teenuse osutajad sel juhul järgima nimetatud rakendusakti.
Vastuseks eelnõu koostajate küsimusele seletuskirjas (lk 87) anname teada, et see säte ega selle eesmärk ei ole arusaadav. Miks peaks üldse tekkima olukord, et Eestis kehtestatakse riigi poolt määrus, mis on vastuolus EL-i rakendusaktiga?
Samuti on äärmiselt ebaproportsionaalne panna vastutus kohustatud isikutele ehk teenuse osutajale tuvastamaks vastuolusid määruse ja rakendusakti vahel.

ITL-i ettepanek: vaadata selle sätte sõnastus üle ning jätta sellest välja teenuse osutajate kohustus erinevaid õigusakte omavahel võrrelda ja hinnata kumba täita.
ITL-i täiendavad kommentaarid, küsimused ja ettepanekud eelnõu konkreetsete sätete ja seletuskirja osas leiate käesoleva kirja lisast.

7. NIS2 direktiivi ja DORA määruse kattuvuse regulatiivne lahendus

Eelnõus ei adresseerita turuosaliste poolt tõstatatud murekohta seoses finantssektori digitaalse tegevuskerksuse ehk DORA määrusega (EL-i määrus 2022/2554). Praegu pole selgelt määratletud, kas NIS2 direktiivi kohuslased, kes osutavad krediidiasutustele teenuseid kriitilise või olulise funktsiooni osas, peavad lisaks NIS2 direktiivile tõendama ka DORA-le vastavust ning kuuluma DORA järelevalve alla. See tekitab dubleerivat halduskoormust.

ITL-i ettepanek: Käsitleda KÜTS-is kui üldseaduses seda teemat, et vältida dubleerivat halduskoormust ning tagada sujuvam nõuetele vastavuse tagamine. Oluline on keskenduda:

- topelt nõuete vähendamisele, võimaldades lihtsustatud tõendamist;
- koordineeritud järelevalvele, et vältida ebavajalikku bürokraatiat ja tagada tõhusam regulatiivne järelevalve.

Eelnõuga jääb lahtiseks ka küsimus, et kas krediidiasutused peavad tagama vastavuse DORA kui otsekohalduva määruse nõuetele ning ka Eestis kehtiva KüTS-i nõuetele. Ehk kas läbima peab lisaks Finantsinspektsiooni auditeerimisele ka E-ITS auditi või saama ISO27001 sertifikaadi või loetakse ka DORA alusel tehtav audit samaväärseks nii nagu täna E-ITS ja ISO27001 on alternatiivid. Hetkel peab teenuse osutaja justkui ise võrdluse tegema (eelnõu § 1 punktiga 4 muudetav KüTS § 1 lg 4), kas otsekohalduva määrusega on kohustused täidetud või mitte. Samal ajal on teada, et nii nagu E-ITS ja ISO ei ole identse sõnastusega, ei ole seda ka DORA (kuigi sarnane), ometi on E-ITS ja ISO õigusakti tasemel loetud võrdsustatuks. Ebaselgeks jääb, kes ja kuidas ikkagi vastavust hindab ja kontrollib, millises osas kattub ja millises osas mitte, milliseid nõudeid tuleb täita otsekohalduvast määrusest ja milliseid KüTS-ist.

Lõpetuseks tõdeme, et meie poolt välja toodud eelnõu probleemid on tingitud sellest, et eelnõu osas ei ole viidud läbi eelkonsultatsioone ega tehtud mõjuanalüüsi. Eelnõu ei arvestada riigis püsitatud eesmärki vähendada bürokraatiat ja halduskoormust ning iga uue õigusaktiga ka millestki vanast loobuda.
Loodame, et leiate võimaluse tagasisidet arvestada ja võtta NIS2 direktiiv Eesti õigusesse üle selliselt, et tagatud on riskipõhisus ja proportsionaalsus ning küberturvalisuse valdkonna areng. Soovitame ülevõtmisel arvestada ka seda, mis moodi võetakse NIS2 direktiivi üle teistes liikmesriikides, kus räägitakse palju rohkem ettevõtete konkurentsivõimest ja nende enda rollist küberturvalisuse tagamisel. Riigi roll on seejuures pakkuda ettevõtetele nõustamist ja tõhusaid koostöömehhanisme.
Eesti on mõõtnud juba alates 2008. aastast kriitilise infrastruktuuri vastupanu rünnetele. Seetõttu võiks eeldada, et Eesti riigil on olemas hea tervikpilt olukorrast ning sellest lähtuvalt saab ka sõnastada, mis probleemi eelnõuga lahendatakse. Kooskõlastusele saadetud eelnõu versioon aga jätab mulje nagu seni oleks kõik valesti olnud ja valdkond vajab põhjalikku uuendust, sealjuures teenuste kirjeldusest ja kohustatud üksustest ei ole võimalik üheselt järeldada, kellele või millele need kohalduvad Eesti kontekstis.
Teeme Justiits- ja Digiministeeriumile ettepaneku korraldada ITL-iga kohtumine, et arutada meie poolt eelnõus tõstatutud murekohti ning välja pakutud lahendusi. Samuti **palume selle eelnõu menetlusega mitte kiirustada.** Eelnõu kokku kirjutamiseks võttis riik kaks aastat aega pärast NIS2 direktiivi vastuvõtmist. Nüüd on vaja aega ka selle huvigruppidega läbi arutamiseks ning eelnõu mõjude ja rakendatavuse analüüsiks. Tegemist on olulise valdkonnaga ja suure mõjuga eelnõuga.

Lugupidamisega

/allkirjastatud digitaalselt/

Doris Põld
Tegevjuht

LISA 10 lehel

Keilin Tammepärg, keilin.tammeparg@itl.ee

ESTONIAN ASSOCIATION OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

EESTI
INFOTEHNOLOOGIA JA
TELEKOMMUNIKATSIOONI
LIIT

Lisa: täiendavad kommentaarid, küsimused ja ettepanekud eelnõu sätete ning seletuskirja kohta

1) Eelnõu § 1 p 1 – KüTS § 1 lg 1^1 ja eelnõu § § p 7 – KüTS § 2 p 1^1

Üksus terminina on antud kontekstis kasutamiseks võõras ja pigem kasutatakse seda militaarvaldkonnas. Eesti keeles oleme harjunud ettevõtete/äriühingute ja (riigi/KOV) asutustega. Teeme ettepaneku kasutada Eestis kasutusel olevaid mõisteid, nii on selgem kõigile, sh kohustatud subjektidele.

Variant on kaaluda ka hädaolukorra seaduse analoogiat. Seal nimetatakse elutähtsa teenuse osutajatena juriidilised isikud, kelle pädevuses on seaduses nimetatud elutähtsa teenuse osutamine (HOS § 38 lg 1).

Segadust tekitab ka see, et KüTS § 1 lg 1^1 kohaselt on üksus ettevõtte, hiljem eelnõus ka avaliku sektori asutus. Samuti jääb lõpuni arusaamatuks füüsilise isiku hõlmamine üksuse definitsiooniga. Kas mõeldud on füüsilisest isikust ettevõtet? Sest füüsilist isiku ju ei asutata.

Seonduva teemana kordame veel, et kuigi eelnõu koostajad on suuliselt selgitanud, et teenuse osutaja ongi üksus, siis eelnõust see ei nähtu.

2) Eelnõu § 1 p 1 – KüTS § 1 lg 1^2

Palusite eelnõu seletuskirjas tagasisidet, kas sõnastused on arusaadavad või vajavad täpsustamist. ITL-i tagasiside on, et sõnastused ei ole arusaadavad ja vajavad kindlasti täpsustamist.

Teeme ettepaneku sõnastada subjektide loetelu lühemalt, selgemalt ja üheselt arusaadavalt.

EL-i õigusele viitavatesse punktidesse on vaja sisulist eesti keelset mõistet, nt punktides 5 ja 6.

Punkti 34 (interneti vahetuspunkti teenuse osutaja) tõlge on ebaõnnestunud (vrdl. *telephone exchange* - kas see on telefoni vahetus?). Siin aitaks seaduses ingliskeelse termini kasutamine. IXP on üldiselt igale eksperdile mõistetav.

Punkti 35 puhul on raske mõista sõnastust, kus on kaks korda järjest sõna süsteem - domeeninimesüsteemide süsteemi teenuse osutaja.

Punkti 36 (pilvandmetöötlusteenuse osutaja) puhul palume selgitada, kas see kohaldub ka vahendusteenuse osutajale.

Punkt 38 (sisulevivõrguteenuse osutaja) ei ole arusaadav. Kirjelduse järgi oleks tegemist justkui võrguomanikuga, kuid sisulevi viitab sisule või vahendamisele. Teeme ettepaneku seda punkti täpsustada (samuti ka KüTS § 2 punkti 7^2), et see pole side, TV või raadioteenus (seletuskirjas hetkel on täpsustus). Samuti teeme ettepaneku lisada ingliskeelse termini "*Content Delivery Network* - CDN", et oleks arusaadavam. Kindlasti aitaks kaasa ka see, kui nimetada ära, kes need (5) ettevõtet on, kes eelnõu koostajate hinnangul selle sätte alla lähevad.

Punkt 39 (hallatud teenuse osutaja) on kõige arusaamatum üksuse kategooria, millest tõesti ei saa aru, keda mõeldud on. Seletuskirja sõnastuse kohaselt võiks sellesse kategooriasse kuuluda väga paljud erinevad ettevõtted. Seletuskirjas pakutakse, et neid võiks olla 20 tükki.

Palun kirjutage eelnõus lahti, milliste teenuste osutajatega tegemist on ning kuidas on vastutus jagunenud, kui vahendatakse kellegi teise toodet/teenust.

Vastavalt vaja üle vaadata ka eelnõu § 1 p 14 – KüTS § 2 p 11.

Punkti 40 (hallatud turbeteenuse osutaja) tekib kõigepealt küsimus, miks see eraldi välja toodud on, kui eelmine mõiste – hallatud teenuse osutaja – katab ka selle kategooria. Või need ikkagi ei kattu? Näiteks võib turbeteenus võib olla ka sisse ostetud infoturbejuhi teenus, mis ei sobi KüTS § 2 p11 definitsiooniga.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Termini sisu jääb arusaamatuks. Näiteks kas mõeldud on vahendajaid või kedagi muud? Vahendajate puhul võib olla oluline, et kas vahendaja saab ise midagi teha või üldse sekkuda, kui tegemist on valmistootega. Vahendustegevuse juures on oluline ka küsimus, kas tegemist põhitegevuse või kõrvaltegevusega. Teisel juhul võivad kohustused olla ettevõtte jaoks ebaproportsionaalselt suured.
Sarnaselt vaja üle vaadata ka eelnõu § 1 p 14 – KüTS § 2 p 12.
Punkti 47 (Eurostati klassifikaatori NACE Revision 2 C jao jaotistes 26, 27, 28, 29 ja 30 osutatud majandustegevusega tegelev ettevõtja) osas teeme ettepaneku lisada sisu ehk mis majandustegevusele need punktid viitavad.

3) Eelnõu § 1 p 1 – KüTS § 1 lg 1[3]

Punkti 1 (üldkasutatava elektroonilise side võrgu pakkuja) puhul juhime tähelepanu, et Elektroonilise side seaduses (ESS § 2 p 66) kasutatakse terminit võrguteenuse pakkuja. See vastab Direktiivi (EL) 2018/1972 artikli 2 punktile 2 mis tõepoolest kasutab terminit „elektroonilise side võrgu pakkumine“. Seega teeme ettepaneku mitte luua uut terminit vaid võtta ESS-ist õige sisuga termin.
Neid ettevõtteid on kindlasti rohkem kui 4, kuna siia alla lähevad muuhulgas ka kõik riigiabi eest ehitatud sidetaristu (nt optikakiu) pakkujad.
Punkti 2 (üldkasutatava elektroonilise side teenuse osutaja) kohta on samasugune kommentaar – neid ettevõtteid on kindlasti rohkem kui 4. Õige numbri saab Tarbijakaitse ja Tehnilise Järelevalve Ametilt. ITL-ile teadaolevalt on neid ettevõtteid üle 200. Teeme ettepaneku lisada antud mõiste definitsioon, mis on elektroonilise side seaduses.
Eelnõu § 1 punktiga 16 KüTS-i lisatava § 3 lg 1^2 punkt 9 räägivad “elektroonilise side võrgu ja elektroonilise side teenuse **pakkujast**”. Pakkuja mõistet pole aga defineeritud . Samuti kasutatakse vahepeal mõistet “elektroonilise side teenuse **osutaja**”. Jääb selgusetuks mis vahe on osutajal ja pakkujal KüTS-i tähenduses.
Meile teadaolevalt kasutatakse võlaõigusseaduses ja tarbijakaitseseaduses lähenemist, et pakkuja on see, kel on teenus olemas, kuid kes seda veel ei osuta. Ehk õigem oleks kasutada mõistet teenuse osutaja.
Punkti 3 (usaldusteenuse osutaja) osas tekkis küsimus, kuidas on hinnatatud, et esialgselt usaldusteenuseid osutajaid on 28 tk. Millistel allikatel see informatsioon tugineb? Taaskord oleks abiks avalik nimekiri, keda eelnõu koostajad selle kategooria alla liigitaksid. Siiski peab eelnõu tekst ka olema piisavalt selge selles osas, et kohustatud isik ise ka aru saaks, kas on kohuslane või ei.
Punkti 5 (domeeninimede registreerimise teenuseid osutav üksus) osas märgime, et registripidajaid on www.internet.ee andmetel 51 (seletuskirjas 10).

4) Eelnõu § 1 p 1 – KüTS § 1 lg 1[4]

Kas üksus käesolevas paragrahvis on ainult ettevõte või ka avaliku sektori asutus?
Punkt 2 - miks siin kasutatakse sõna “häire”? Pigem see on ikka küberintsident (mille mõiste sees on häire). NIS2 direktiivi artikkel 2 lg 2 punkt c kasutab sõna “distruption” mis on pigem “teenuse häirimine”, mitte “häire” (ingl.k “alert”). Häire on küll NIS2 tõlkes, aga pole korrektne.
Punkti 2 osas võiks pigem olla sõnatus „on oluline mõju“, mitte „võib olla“.
Punkti 3 osas sarnaselt „võib tuua“ asendada „toob kaasa“.
Punkti 4 osas jääb ebaselgeks, milline on kriitilise tähtsuse tuvastamise metoodika.

5) Eelnõu § 1 p 1 – KüTS § 1 lg 1^5
Normitehniline märkus, et saatelauses piisab viitest KüTS § 1 lõikele 1^4, ei näe vajadust nimetada kõiki selle alapunkte (1-4).

6) Eelnõu § 1 p 2 – KüTS § 1 lg 2^1
Küsimus: Keda on selle sättega mõeldud – millise asutuse kohta see reaalses elus käib?

7) Eelnõu § 1 p 5 – KüTS § 1 lg 4^1
Õigusselguse mõttes asendaks sõna "võib" sõnaga "peab".

8) Eelnõu § 1 p 6 – KüTS § 1^1
Kuna seadus on ülimuslik, siis kas teenuselepingu sätted, mille kohaselt toimuksid teenuse pakkujaga võimalikud vaidlused Eesti Vabariigi kohtusüsteemis, muutuksid kehtetuks, kui teenuse pakkuja asub nt Leedus?
Hea oleks selgemaks saada ka, mida tähendab KüTS § 1^1 lg 3 p 1 "peamine tegevuskoht ..., kus turvameetmeid käsitlevad otsused valdavalt tehakse." Tekib küsimus mis laadi otsused – kas strateegilised, operatiivsed? Kelle otsused?

9) Eelnõu § 1 p 7 – KüTS § 2 p 1^2
Siin on huvitav lähenemine, kus terminis sätestatakse KüTS § 1 lg 1^3 punktis 7 nimetatud asutused. Miks need ei saa olla seal, kus sätestatakse, et regulatsioon laieneb neile? Teeme ettepaneku lisada siia viide, mitte korrata loetelu.

10) Eelnõu § 1 p 7 – KüTS § 2 p 1^4
Tegemist on olulise muudatusega, sest esmakordselt defineeritakse Eesti õiguses küberturvalisus. Kahjuks on seda tehtud viitega EL-i õigusele. Teeme ettepaneku see mõiste eelnõus avada, sest viide EL-i määrusele ei taga õigusselgust.

11) Eelnõu § 1 p 9 – KüTS § 2 p 3^3
Teeme ettepaneku sõnastada „risk" järgmiselt: 1) vaatlusaluse ohu potentsiaal ära kasutada mingi vara või vararühma nõrkusi ja tekitada seeläbi kahju; 2) võimalus, et küberintsidendi läbi tekib kahju või tõrge, väljendatakse kahju ulatuse mõju hinnangu ja realiseerumise esinemise võimalikkuse kombineeritud näitajana.
Ehk aitaks KÜTS-i kontekstis selgusele kaasa ka see, kui sõna risk juures kasutada eristumiseks mingit täiendavat sõna?
Kummaline konstruktsioon eelnõus sisalduva selgituse puhul on „häire võimekus". Kas see on eesti keeles "häire (mis pole ka õige sõna) tekkimise võimalus". Või siis sündmuse? Pigem on tegu ohuga küberintsidendist tekkivale kahjule, kas teenuse katkemisest või toimimisest tingituna või juurdepääsu piiramisest.

12) Eelnõu § 1 p 9 – KüTS § 2 p 3^4
Siia on vaja mõistet, mitte viidet määrusele.

13) Eelnõu § 1 p 9 – KüTS § 2 p 3^5
Eelnõus peab olema eristatavad ja arusaadav, milline on küberoht ja milline on oluline küberoht.
Seletuskirjast ei tule välja selle mõiste täpsustus ehk milline on „tõsine mõju" ja milline on „märkimisväärne rahaline kahju". On oluline, et selline osa oleks toodud välja seletuskirjas, nt tõsine

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

mõju on kui süsteem maas oleks on nii pikk või mõjutab sellisel hulgal isikud või kaasneb märkimisväärne kahju, mis on aastakäibes selline protsent.
ITL-i ettepanek on seega seda mõistet täpsustada. Äkki läbi mõju (lõppkasutajate arv vmt).

14) Eelnõu § 1 p 9 – KüTS § 2 p 3^6
NIS2 direktiivi artikkel 6 punkt 15 kasutab siinkohas sõna „vulnerability". Selgitame, et "vulnerability" ja "weakness" mõistetel tehakse infoturbes sageli sisulist vahet ja „vulnerability" tähenduses on kasutusel ikkagi "haavatavus" ja "weakness" on "nõrkus". Teeme ettepaneku sisustada see mõiste järgmiselt: (Võiks kasutada nt ISO27001 sõnastust) vara või meetme nõrk koht, mille saab ära kasutada üks või mitu ohtu.

15) Eelnõu § 1 p 9 – KüTS § 2 punktid 3^7 - 3^9
Teeme ettepaneku defineerida need terminid Eesti õigusaktide mõistete pinnalt, mitte ainult viidata EL-i määrusele.

16) Eelnõu § 1 p 11 – KüTS § 2 punktid 4^6 ja 4^7
Toetame nende mõistete puhul viitamist EL-i õigusaktidele ning teeme ettepaneku lisada viide ka eIDAS 2 määrusele (määrus nr 2024/1183).

17) Eelnõu § 1 p 12 – KüTS § 2 p 6
Siia on vaja mõistet, mitte viidet EL-i määrusele.

18) Eelnõu § 1 p 13 – KüTS § 2 p 7^4
Teeme ettepaneku „on mõeldud" asendada konkreetsema sõnastusega („on"). Lisaks kaaluda loetelu vormistamist punktidena.

19) Eelnõu § 1 p 14 – KüTS § 2 p 10
Siin jääb arusaamatuks, kas mõeldakse elektroonilise side teenust (elektroonilise side seadus (ESS) § 2 p 6) või üldkasutatavat elektroonilise side teenust (ESS § 2 p 68). Seletuskiri viitab üldkasutatavale teenusele. Tegu on olulise erinevusega, mistõttu palume seda täpsustada.
Kui tegu pole üldkasutatava elektroonilise side teenusega, siis läheksid ka näiteks ettevõtete sisesed sidevõrgud (milles ei osutata üldkasutatavat teenust igaühele, kes tahab tüüptingimustel kättesaadavat teenust) KüTS-i regulatsiooni alla.

20) Eelnõu § 1 p 14 – KüTS § 2 p 13
Mõiste sisu ei vasta Eesti teadus- ja arendustegevuse seaduse § 3 lõikele 1. Tegemist on küll NIS2 direktiivi artikkel 6 punkti 41 otse ülevõtmisega. Samas sisu tundub olevat Eesti teadus-ja arendustegevuse seaduse mõttes eraõiguslik teadusarendusasutus (aga ei ole ka).

21) Eelnõu § 1 p 16 – KüTS § 3 lg 2 p 10
250+ töötajat ja bilansimaht on üle 43 mln euro või aastakäive üle 50 mln euro tähendab suurettevõtet. Sättes viidatakse keskmise suurusega ettevõtjale ning bilansimahud ja käibed on veel omakorda sassi läinud. Ehk siin on vasturääkivusi rohkem kui üks.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

22) Eelnõu § 1 p 19 – KüTS § 3 lg 3[1]

Sätet lugedes tekkisid järgmised küsimused:

- Punkti 3 puhul jääb arusaamatuks, mida tähendab asjakohasel juhul. Seletuskirjas lk 73 öeldakse, et seda ei pea kõik üksused esitama. Kes siis peab?
  Sama kommentaar eelnõu § 1 p 21 – KüTS § 4 lg 1 p 2 kohta.
- Kas vastava teemal teeb teenuse osutajale esmase päringu RIA? Kui jah, siis millal vastav päring tehakse? Kui ei, siis kuidas see protsess ette näeb? Milline on vastamise tähtaja pikkus?
- Mida mõistetakse IP aadresside vahemiku all ja mis on selle eesmärk?

Juhime veel tähelepanu, et seletuskirjas lk 145 viidatud once only põhimõte ehk ühekordne teavitus IT-lahenduse/digitaalse teenuse kaudu peaks olema prioriteet. Kindlasti on ka oluline, et andmeid, mis ükskõik millisel riigiasutusel olemas on, ei tohi uuesti küsida. Praegu jääb seletuskirjast mulje, et kõik on väga lahtine. Kas see on tõesti nii?

23) Eelnõu § 1 p 19 – KüTS § 3 lg 3[4]

Selle sätte eesmärk jääb arusaamatuks. Sõnastuse kohaselt võivad üksused juhinduda viidatud suunistest, kuid võivad ka mitte. Oluline on selgelt aru saada, millest juhinduda tuleb ja mis on otsekohalduv.
Sama kommentaar eelnõu § 1 p 21 – KüTS § 4 lg 1[4] kohta.

24) Eelnõu § 1 p 22 – KüTS § 5 lg 1

Esimese lause teine pool (alates komast) vajab grammatiliselt üle vaatamist. Samas – kas seda lause teist poolt on üldse vaja eelnõus sätestada?

25) Eelnõu § 1 p 22 – KüTS § 5 lg 3 p 3

Teeme ettepaneku lisada sättesse lühend CSIRT.

26) Eelnõu § 1 p 22 – KüTS § 5 lg 5

Mis on „ajaomastele teenustele“ ja „asjakohasel juhul“ tegelik sisu?
Punkti 15 osas on vajalik selle kontrollimise dokumenteerimine või logimine. Selline kontroll peab olema kokkulepitud tegevus, mis ei sea ohtu teenust ning viiakse läbi ikkagi teenuse osutaja teadmisel.

27) Eelnõu § 1 p 23 – KüTS § 5[2] lg-d 2 ja 3

Õigusselguse mõttes ei ole selline edasivolitamine mõistlik. Jääb arusaamatuks, miks minister volitab täitevasutuse edasi volitama.
Teeme ettepaneku fikseerida koheselt ja ilma edasi volitamiseta asutuse, kes on vastav pädev asutus. Juhul, kui seda ei soovita teha, siis palume selgitada, miks soovitakse see pädev astus osaliselt lahtiseks jätta ja kuidas isikuid teavitataks, kui asutus muutub.

28) Eelnõu § 1 p 24 – KüTS § 6[1]

Esimene küsimus on, kes on juhtorgan antud sätte mõttes. Kas nõukogu, juhatus või ainult juhatuse esimees? Kui lähtuda äriseadustiku definitsioonist, siis juhtorgan osaühingu ja aktsiaseltsi puhul on juhatus. Et kas siis on mõeldud, et kogu juhatus peab tagasi astuma? Palume täpsustada seda eelnõus. Teiseks palume punkt 2 osas täpsustada, et kui spetsiifilisel tasemel peab juhtorgan turvameetmed heaks kiitma. Võib eeldada, et enamik ettevõtete juhatusi ei oma piisavaid pädevusi, et otsustada ega mõista konkreetseid turvameetmeid (nt mis protokolle, krüpteerimismeetodeid vm) kasutada.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Lisaks: NIS2 direktiivis räägitakse hoopis "riskijuhtimismeetmetest", mis erinevad turvameetmetest. Eelnõu peab lähtuma direktiivist, mitte laiendama kohustusi.
Kolmandaks on vaja selgust, kes hindab, milline koolitus on piisav selle nõude täitmiseks. Tegemist on kohustusega, mille rikkumisel ootab ees vastutus.
Seletuskirjas palutakse tagasisidet, kas peaks määratlema ka nende koolituste tegemise välp ehk mis aja tagant tuleks taolisi koolitusi teha. Leiame, et teatav miinimumnõue selles korrapärasuses peaks olema, sest kord 10 aasta jooksul pole piisav. Teadlikkus küberriskidest on organisatsioonides madal ja neisse riskidesse kiputakse suhtuma üleolekuga. Vt ka käesoleva kirja II osa punkti 5.

29) Eelnõu § 1 p 26 – KüTS § 7 lg 2
Siin vajab sätte algus korrigeerimist, sest sätestab, et muudetakse selle lõike punkte 1-3, kuid tegelikult tekitatakse 14 punkti.
Teeme ettepaneku tõlkida turvameetmete nimekiri täpselt NIS2 direktiivist, praegu on tekitatud meetmeid juurde sõnastuste muudatustega. Isegi kui need on väikesed ning sisuliselt on proovitud osa teemasid lahti lüüa eraldi punktideks.
Punkti 9 osas kommenteerime, et küberhügieen ei ole ametikult kasutatav termin. Selle välja toomine eelnõus on täiesti ebamõistlik. Mis asi see on? Selle sõna võiks üldse välja jätta. Organisatsioonid on erineval tasemel. Hakata küberturvalisuse teenust pakkuvates organisatsioonides regulaarseid hügieenikoolitusi tegema ei tundu eriti mõistlik.
Punktide 10 ja 13 osas on taas küsimus, mis on „asjakohane juht". See tuleb siduda riski kaalutlemisega. Punkt 13 valgub üsna laiali – et on justkui turvaline ja siis ebaturvaline(?) lahendus ja siis peaks asjakohasel juhul valima turvalise ja mitteasjakohasel ebaturvalise?

30) Eelnõu § 1 p 27 – KüTS § 7 lg 2^1
Kaitsetarve ei ole üldiselt mõistetav termin. Teeme ettepaneku selle ja teised E-ITS standardis kasutatavad ja ainult E-ITS sõnastikus defineeritud spetsiifilised mõisted eelnõust välja jätta.

31) Eelnõu § 1 p 29 – KüTS § 8 lg 1
Kui teenuse osutaja on MSSP (Managed Security Service Provider), kes osutab teenust KüTS subjektidele, siis kes sel juhul on kohustatud isik? Kas MSSP või klient, kellega intsident aset leidis?

32) Eelnõu § 1 p 31 – KüTS § 8 lg 2
Siin ja KüTS § 8 lg 3 on oluline küberintsident. Umbes sama on terminites KüTs § 2 p 3^1 ulatuslik küberintsident. Kas need on ühe tähendusega või erinevad mõisted?

33) Eelnõu § 1 p 33 – KüTS § 8 lg 4^1
Punkti 1 kohaselt tuleb anda teavet "turvarikkemärgi" kohta. Kas see on üldtuntud termin ega vaja seletust või võiks selle ikkagi lahti seletada? Mujal eelnõus seda ei esine.
NIS2 direktiivi eesti keelses versioonis on see artikkel 23 lg 4 punkti b viimane sõna „turvarikke indikaator" (ingl. k: the indicators of compromise). Sama NIS2 direktiivi põhjenduspunkt 102. Mis on selle tegelik sisu?

34) Eelnõu § 1 p 33 – KüTS § 8 lg 4^2
Vahearuande küsimine on RIA võimalus ehk puudub selgus, millal RIA võib vahearuannet küsida. Mingil liiga varasel hetkel (näiteks poliitilise surve tõttu) võib vahearuande nõudmine võtta ära aja küberintsidendi lahendajalt. Seletuskiri lk 89 tähtaega ei määratle, kas see on siis organisatsiooni enda otsustada?

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Ebaselgus on veel suurem kui küsitakse “täiendavat teavet”. Mis on see “asjakohane juht”, kui seda küsitakse?
Arusaamatuks jääb ka mis on vahearuande eesmärk. Kas RIA soov olla lihtsalt kursis või aidata lahendada? On vist olnud juhtumeid kus RIA ei vaja vahearuannet aga seda küsib ootamatult Vabariigi Valitsus. Teeme ettepaneku kaaluda, kas vahearuanne on põhjendatud pigem ulatusliku mõjuga, mitte olulise mõjuga intsidendi korral. Kui need on erinevad, vt ka p 32.

35) Eelnõu § 1 p 35 – KüTS § 8 lg 7
Kui teenuse osutaja on MSSP (hallatud turbeteenuse osutaja), kes osutab teenust KüTS subjektidele, siis kes sel juhul on kohustatud isik?
Kui teenuse osutaja on MSSP siis toob see kaasa dubleerivad tegevused ning lisapersonali palkamise aruannete koostamiseks, mis omakorda tõstab teenuse hinda klientidele. Lisaks moonutab dubleeriv andmete edastamine tegelikku statistikat.
Ehk see säte illustreerib, et kohustused ja vastused hallatud teenuse osutaja vaatest vajavad selgitamist. Lisaks tekib küsimus, kui vahendajaid on mitu.

36) Eelnõu § 1 p 39 – KüTS § 8^1
Säte reguleerib vabatahtlikku teavitamist. Leiame, et seaduse tasemel kehtestada, et võib teavitada, tundub kummaline. RIA võib seda soovi korral oma kodulehel reklaamida ja luua vastava kanali.
Lg 1 osas palume täpsustada, kas tegemist on intsidentidega, mis ei ole KüTS § 8 all toodud.
Lg 2 sätestab, et anonüümsus on tagatud üksnes avalikult. Lause esimene pool on eksitav jättes mulje, et ka RIA-le saab esitada anonüümselt ilma, et nemadki isikut teaksid.

37) Eelnõu § 1 p 41 – KüTS § 12 lg 3^1
Sättest jääb mulje nagu RIA ise ei võiks abi pakkuda. Kas see on nii?
Siit sättest on puudu NIS2 direktiivi artikkel 23 lõikes 5 veel sätestatud pädeva asutuse (st. RIA) kohustus “anda nõu, kuidas toimida” ja “ka juhiseid olulisest intsidendist õiguskaitseasutuste teavitamiseks“.

38) Eelnõu § 1 p 41 – KüTS § 12 lg 3^2
Millisel juhul eelistatakse ametlikku teavitamist vabatahtlikule?
Selle sätte mõte jääb arusaamatuks, viites on midagi valesti.

39) Eelnõu § 1 p 44 – KüTS § 12 lg 5
Antud juhul võetakse NIS2 säte üle kitsamalt ja subjektide jaoks piiravamalt. NIS2 direktiivi artikkel 2 lg 13 kohaselt võib vahetada ainult teavet, mis on teabevahetuse eesmärgi seisukohast oluline ja proportsionaalne. Teabevahetuse puhul tuleb säilitada asjaomase teabe konfidentsiaalsus ning kaitsta asjaomaste üksuste turvalisust ja ärihuve. Palume need samad põhimõtted viia eelnõuga sisse ka KüTS-i.

40) Eelnõu § 1 p 49 – KüTS § 13^3
See säte on ebamäärane ja jääb ebaselgeks. Küsimus on kas valitsus kehtestab nõuded protsessidele v.a. siis kui on olemas õigusakt, protsessid töötab välja teenuse osutaja või protsessid sertifitseeritakse. Tundub, et viga on eestikeelses tõlkes ja NIS2 direktiivi mõte on selles, et võib nõuda teenuses kasutatavate teenuseosutaja enda või kolmanda isiku loodud IKT toote, teenuse jms sertifitseerimist EL küberturvalisuse skeemide kohaselt.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee

Üldisem küsimus on, et kas lisaks nendele KüTS-i skeemidele on lubatud ka muudel alustel sarnased sertifitseerimisskeemid? Näiteks siseriiklikult meil lubatud EITS-i ja ISO järgi auditeerimine, ISO-t sertifitseeritakse. Kas nõutakse neile lisaks?
Siin tuleb lisada ka täpsustus, et kui on teenuseosutaja valdkonna spetsiifiline sertifitseerimisskeem, siis aktsepteeritakse seda ja ei tohi nõuda midagi sinna otsa. Näiteks eIDAS alusel või rahvusvaheliste standardite alusel sertifitseeritakse kvalifitseeritud usaldusteenuse osutajaid. Praegu nähakse vaeva, et viia nõudeid NIS2 direktiiviga kooskõlla.

41) Eelnõu § 1 p 52 – KüTS § 14 lg 6
Tegemist on ebaselge sättega, mis ütleb, et üldreeglina kasutakse seda või teist. Mõistlik oleks selgelt väljendada, millistel juhtudel (subjektide osas) on järelevalve ennetav ja millistel juhtudel järelkontrollina. Punkt 1 ja 4 annavad justkui täitsa vaba tõlgenduse, kelle juurde kontrollima minna, küll põhjenduse leiab.

42) Eelnõu § 1 p 52 – KüTS § 14 lg 7
Eelnõus ega NIS2 direktiivis ei ole defineeritud ega loetletud, mis on olulised nõuded (ja mis on siis mitte olulised nõuded). Kust seda teada saaks? Kes neid hindab?

43) Eelnõu § 1 p 52 – KüTS § 14 lg 8
Siduvate juhiste andmist ei ole reguleeritud. Siin on "siduv juhis" üks ja ainus kord eelnõus ja selle andmist ei ole reguleeritud. KüTS §12 lg 3^1 on "suunised". Seletuskirja kohaselt võetakse üle NIS2 direktiivi artikkel 32 lg 7 punti a alapunktid i-v, kus on tõesti kirjas juhised.
Samas KüTS §14 lg 9 kohta on seletuskirjas (lk. 94): Kui mingis NIS2 direktiivi sättes on kasutatud sõnastust „korraldus" või „siduvad juhised", siis eelnõus on selle all mõeldud ettekirjutust.
Ehk see säte vajab selgitust ja igal juhul tuleb saada selgeks mis (siduv juhis, suunis, …) on õigusakt või ühekordne haldusakt. Siduv juhis ei ole vist Eesti õiguses kasutusel?

44) Eelnõu § 1 p 52 – KüTS § 14 lg 9
Punkt 2 sihipäraste turvaauditite puhul võiks olla ka eelnõus toodud ära, et kui palju RIA peab teenuse osutajat sellest soovist audit läbi viia ette teavitama. Samuti tuleb teenuse osutajat teavitada, et kes viib auditi läbi ja teenuse osutajale peab jääma võimalus esitada auditi läbiviijale põhjendatud vastuväiteid.
Punkti 2 osas tekib ka küsimus, mis on muu riskialane teave.
Punktis 3 tekitab küsimusi „vajaduse korral" - millise või kelle vajaduse?
Milles seisnevad punktis 3 nimetatud "turvalisuse kontrollid"?
Punktis 10 on kasutuses vastavushaldur, mille mõiste on E-ITS-I rollisõnastikus, kuid seaduses defineerimata. ITL-i ettepanek on E-ITS spetsiifilisi mõisteid eelnõus mitte kasutada.

45) Eelnõu § 1 p 52 – KüTS § 14 lg 10
Teeme ettepaneku punkt 4 eelnõust eemaldada. Juhime tähelepanu, et NIS2 direktiivi ülevõtmisega ei ole kohustust kehtestada kulude katmise osa, eriti tehes seda täiesti põhjendamatult.
Lisaks ei nähtu seletuskirjast, mis väljamineku see võib põhjustada ja kokkuvõtlikult jääb üldine mulje, et sellega soovitaks luua olukord, kus ISO 27001 teed läinud isikute/asutuste osas tekiks olukord, kus on võimalik auditeerida KüTS eelnõu 7 lõikes 2 ja 2^1 toodud E-ITS meetmeid ja selle eest peaks tasuma isik/asutus ise.

Palume selgitada selle punkti eesmärki ja muuta see selliselt, et RIA-l on enne auditi tellimist selgituskohustus, miks seda tehakse ning see selgituskohustus täpselt lahti kirjutada ka seletuskirjas, et oleks kohuslastele arusaadav. Lisaks tuua välja ka aeg, mille jooksul on võimalik esitada vastulauseid.

46) Eelnõu § 1 p 55 – KüTS § 17^3

Lg 6 osas palutakse seletuskirjas tagasisidet, kas kommenteeritava lõike puhul on vaja ka sätestada, et teise riigi pädeva asutuse töötaja võib kasutada KüTSis sätestatud meetmeid, mida saab eelnõu tulemusena kasutada ainult Riigi Infosüsteemi Amet või piisab sellest, et vastavad volitused on ja jäävad ainult Riigi Infosüsteemi Ametile? Kui ootus on, et teise riigi pädev asutus võiks kasutada ka KüTS-is sätestatud meetmeid, siis kas ta võiks kasutada kõiki meetmeid või osasid neist – viimase variandi korral, milliseid meetmeid?

ITL-i liikmed ei kujuta hästi ette seda halduskoormuse kasvu, kui neid ametkondi (ja seda rahvusvaheliselt) lisandub, kellel on õigus auditeerida ja küsida aruandeid ning trahvida ka veel. Samuti puudub Eesti ettevõttel teadmine sellest, kas välismaine asutus on tegelikult ikka ka riigiasutus ja mis pädevused tal oma riigiski on.

47) Eelnõu § 1 p 56 – KüTS § 17^4

See pealkiri on vale. Tegu on volitustega teha koostööd erinevate osapoolte ja ametkondadega. Omaette küsimus on, kas see paragrahv on üldse seaduses kajastatav teema või peaks see olema Vabariigi Valitsuse määruse tase. Või ei vaja see üldse reguleerimist õigusaktiga?

Lõike 2 osas tekitab küsimusi see, et teabevahetus on ette nähtud ainult ETO-dega. Aga teised üksused, kellel on intsident vms?

48) Eelnõu § 1 p 56 – KüTS § 17^5

Jääb arusaamatuks, miks eraettevõtete omavahelisi kokkuleppeid peab seaduses reguleerima - miks kirjutada seadusesse, et teenuse osutajad ja muud isikud võivad infot vahetada. Meil on lepinguvabadus. Riigi/KOV asutustel võib küll mingi akti tasemel olla antud õigus teavet vahetada, kuid kas seda reguleerida käesoleva eelnõuga?

Infovahetamine sõltub ettevõttest ja tema riskide hindamisest, millist infot saab ja peab vahetama, millist mitte (konfidentsiaalne, ärisaladus, toimepidevuse vaatest kõrge riskitasemega info)

Punkti 5 alusel tuleb lausa RIA-t teavitada teabevahetuse kokkuleppega ühinemisest või sellest taganemisest. Kui see oleks konkreetsete ettevõtete vahel, siis miks peaks sellest RIA-t teavitama?

49) Eelnõu § 1 p 56 – KüTS § 17^6

Kas vastastikuse hindamise niivõrd detailne reguleerimine seaduse tasemel on vajalik?

Lõike 4 osas - kas edasivolitamine on lubatav ja vajalik? Kui volitada siis saab seda teha minister.

Seletuskirja lk 146 öeldakse, et pole otsustatud, kas Eesti soovib selles osaleda. Leiame, et võiks aru saada, kas on seda vaja või mitte. Variant oleks ka eelnõus sätestada, kes seda otsustab või kirjutada hetkel lühidalt, et vajadusel määratakse need siseriiklikult vastavalt NIS2 direktiivi artiklile 19 ja praegu jätta välja.

50) Eelnõu § 1 p 60 – KüTS § 19 lg 4

Kui KüTS §-des 18^2 –18^6 sätestatud väärtegude kohtuväline menetleja on RIA, siis kas § 19 lõikest 2 võib järeldada, et 18^2 ja 18^3 sätestatud väärtegu menetletakse ainult isikuandmete kaitse seaduse alusel (3 aastat aegumistähtaeg seal juba kirjas) või mõlema alusel ja kas trahvid ja aegumine käivad ühe või mõlema seaduse järgi?

51) Eelnõu § 1 p 61 – KüTS § 20

Seletuskirjas palutakse tagasisidet, kas eelnõuga ette nähtud tähtajad on arusaadavad ning selged või tuleks nende sisu ja tingimusi muuta ehk et mis tähtajaks või millistest tingimustest lähtuvalt tuleks vastavad tähtajad kindlaks määrata.

Jääb arusaamatuks, miks seotakse jõustumised erinevate sätete jõustumisega olukorras, kus kõik need sätted jõustuvad ühel kuupäeval ehk seaduse jõustumisel, vt eelnõu § 11.

52) SK lk 3

Seletuskirja kohaselt nähakse ette KÜTS-i jõustamiseks toetus uutele subjektidele EL taasterahastust (uusi subjekte on umbes 2000). Samas jääb ebaselgeks, kuna seletuskirjas ei ole välja toodud, kas rahastust võib laiendada ka alltöövõtjatele. Näiteks on palju ettevõtteid, mis peavad KüTS-i nõudeid järgima läbi KüTS-i kohuslasele teenuse osutamise.

Selleks, et KüTS kohuslane ei peaks loobuma oma koostööpartnerist, kes peab vastama samadele tingimustele, siis teeme ettepaneku vastavat toetust ka neile laieneda läbi KüTS-i kohuslase taotluse. See kergendaks oluliselt ka KüTS-i kohuslaste olukorda ning ei tekiks üksustes olukorda, et üksused ei saa kasutada teatud teenuseid, kuna need ei ole seadusega vastavuses. Läbi selle toetaks riik erinevaid teenuse osutajaid ja ettevõtteid ning tagaks pakutavate teenuse turvalisuse.

ESTONIAN ASSOCIATION OF INFORMATION
TECHNOLOGY AND TELECOMMUNICATIONS
Lõõtsa 2b, 11415 Tallinn, Estonia
+372 617 7145
info@itl.ee / www.itl.ee