EESTI ADVOKATUUR
ESTONIAN BAR ASSOCIATION

**Liisa-Ly Pakosta**
Justiits- ja digiminister
Justiitsministeerium
info@justdigi.ee
Raavo.palu@justdigi.ee

Teie 09.12.2024 nr 2-2/3131-1
Meie 03.02.2025 nr 1-8/982-1

**Küberturvalisuse seaduse ja teiste seaduste muutmise seadus (küberturvalisuse 2. direktiivi ülevõtmine)**

Lugupeetud Liisa-Ly Pakosta

Täname, et olete advokatuurile saatnud arvamuse avaldamiseks küberturvalisuse seaduse ja teiste seaduste muutmise seaduse eelnõu. Edastame teile advokatuuri intellektuaalse omandi ja IT-õiguse komisjoni seisukohad eelnõu osas.

## 1. Eelnõu ei vasta HÕNTE nõuetele

### 1.1. Eelnõu kohaldamisala on ebaselge

Õigusselguse[1] huvides peab olema tagatud, et seaduse eelnõus on üheselt ja selgelt sedastatud kohustatud isikud ja puutumust omavad valdkonnad. KüTSi eelnõu kohaldamisala reguleeriv sõnastus on niivõrd ebaselge, et ei ole võimalik aru saada, mis on seadusandja eesmärgiks ning kes ja milliste kriteeriumite alusel on kohustatud isikud.

### 1.2. Eelnõu normatiivtekst ei ole loetav

Eelnõu ei ole kooskõlas HÕNTE § 15 lg-ga 2. Nimelt ei toeta eelnõu ülesehitus ja sõnastus teksti loetavust ja seadusest arusaamist. Antud mahus ülamärgete kasutamine osutab, et põhjendatud on uue KüTSi väljatöötamine. Sarnased teemad on killustatult käsitlemist leidnud erinevates sätetes ja jaotistes. HÕNTE näeb ette, et teemasid tuleb käsitleda eraldi ja vastavasisulised paragrahvid tuleb rühmitada nende sisu järgi peatükkides ja osades (vt HÕNTE § 7 jj).

Eelnõus kasutatud viitamine on ebaselge ja ei taga õigusselgust. Eelnõus on väga suures mahus viiteid Euroopa Liidu õigusaktidele. Kui eelnõu koostajad jäävad seisukohale, et selline viitamine on mõõdapääsmatu, siis tuleb seletuskirjas vastavad viited Euroopa Liidu õigusaktidele sisuliselt lahti seletada.

[1] PS § 13 lg-s 2 toodud õigusselguse põhimõte nõuab, et õigusaktid oleksid sõnastatud piisavalt selgelt ja arusaadavalt, et isikul oleks võimalik piisava tõenäosusega ette näha, milline õiguslik tagajärg kaasneb teatud tegevuse või tegevusetusega (RPJKo 3-4-1-23-15, p 98; 5-19-38/15, p 68; 5-22-4/13, p 62).

### 1.3. Seletuskiri ei vasta HÕNTE nõuetele ja ei täida eesmärki

Seletuskiri ei vasta HÕNTE § 39 jj nõutele. Seletuskiri on küll mahukas aga norme selgitatakse seletuskirjas valikuliselt. Seletuskirjas tuleb eelnõu sätted lahti selgitada ja vajadusel põhistada või näidetega ilmestada. Vältida tuleb formalistlikku käsitlust, kus norm on kopeeritud seletuskirja ja puuduvad igasugused muud selgitused. Lisaks tuleb arvestada, et kui normatiivtekstis on nõnda palju sisemisi viiteid kui ka viiteid teistele õigusaktidele, sh Euroopa Liidu õigusaktidele, siis tuleb seletuskirjas selliste viidete sisu põhjalikult lahti selgitada. Märkida tuleb, et keerulise ülesehituse ja sõnastusega seaduse eelnõu seletuskiri peab toetama normatiivtekstist arusaamist. Kahjuks tuleb möönda, et KüTSi eelnõu seletuskiri ei täida vajaliku abimaterjali rolli.

### 1.4. Mõjude analüüsid on tegemata või mõjusid on käsitletud puudulikult ja ühekülgselt

HÕNTE § 39 sätestab, et seletuskirja eesmärgiks on mh anda ülevaade seaduse jõustumisega kaasnevatest mõjudest. Eelnõu seletuskirjas ei analüüsita kõiki asjakohaseid mõjusid. Käsitlemist leidnud mõjusid on kirjeldatud äärmise pealiskaudsusega ja ainult positiivses võtmes. Kui eelnõuga kasvavad kohustatud isikute arv ja järelevalve mahud ning samuti on ettenähtav mõju kõigile turuosalistele ja lõpptarbijale, siis on küüniline sedastada, et mõjusid ei ole või need on juba direktiivi väljatöötamisel käsitlust leidnud. Eesti poliitikakujundajal ja seadusandjal on kohustus hinnata igakülgselt kõiki mõjusid, mis võivad Eestile osaks langeda.

Soovitused:

1. Viia eelnõu kooskõlla HÕNTE-ga.
2. Kaaluda KüTSi eelnõu uue tervikteksti väljatöötamist.

### 1.5. Ebapiisav kaasamine

Käesoleva eelnõu puudujäägid viitavad üheselt, et poliitikakujundaja ei ole saanud turuosalistelt sisendit. Sellise sisu ja mõjuga õigusaktide väljatöötamisel on oluline kaasata erinevad huvigrupid. Enne eelnõu väljatöötamist peab poliitika olema kujundatud. Ebapiisav kaasamine võib olla juurpõhjuseks, miks eelnõu ei vasta HÕNTE-le.

## 2. Vabariigi Valitsuse pädevus

Eelnõu § 1 lg $1^6$ annab Vabariigi Valitsusele volituse määrata Vabariigi Valitsuse määrusega valdkonna või sektori, milles oleva isiku suhtes kohaldatakse teenuse osutaja kohta sätestatut olenemata tema suurusest vastavalt eelnõu § 1 lg $1^4$ punktides 1, 2, 3 ja 4 kriteeriumitest. Viidatud volitusnormis tuleb konkretiseerida volituse sisu ja ulatust. Nimelt on sedastatud kriteeriumid liiga laiad ning annaksid Vabariigi Valitsusele põhjendamatult suure diskretsioonivabaduse. Seletuskirjas ei ole selgitatud sellise volitusnormi võimalikku negatiivset mõju (nt omavoli, poliitilist kallutatust vms). Nii suure mõjuga ettevõtlusvabadust piirav volitusnorm ei ole põhjendatud. Konkretiseerida tuleb volitusnormi sisu ja ulatust. Täpsustamist vajavad eelkõige kriteeriumid.

Soovitus:

Muuta eelnõu § 1 lg $1^6$ sõnastust selliselt, et Vabariigi Valitsuse volitusnormi sisu ja ulatus on konkretiseeritud täpsustatud kriteeriumitega.

**3. KüTS § 61 lg 3 ja § 184 sõnastust seoses juhtorganite kohustuste ja sunnimeetmetega tuleks muuta**

KüTS § $6^1$ lg-s 3 on sätestatud:

(3) *Teenuse osutaja juhtorgan tagab, et teenuse osutaja töötajad ja ametnikud saavad korrapäraselt sarnaseid koolitusi teemadel, mis on nimetatud käesoleva paragrahvi lõikes 2.“*

Kommenteeritud väljaandes puudub aga selgitus KüTS § $6^1$ lg 3 osas. Täpsemalt, seletuskirjas on välja toodud vaid teenuse osutaja juhtorgan, kui koolituse läbija : *„Taolise koolituse läbija ehk teenuse osutaja juhtorgani liige teab: etc.“.*

Lõike enda tekst hõlmab aga ka teenuse osutaja töötajaid ja ametnikke: *„Teenuse osutaja juhtorgan tagab, et teenuse osutaja töötajad ja ametnikud saavad korrapäraselt sarnaseid koolitusi teemadel, mis on nimetatud käesoleva paragrahvi lõikes 2.“*

NIS2 artikli 2 lg 2 eestikeelses versioonis on sätestatud: „*Liikmesriigid tagavad, et elutähtsate ja oluliste üksuste juhtorganite liikmed on kohustatud läbima korrapäraselt erikoolitusi, ning ergutavad elutähtsaid ja olulisi üksusi pakkuma sarnaseid koolitusi korrapäraselt oma töötajatele, et nad saaksid omandada piisavad teadmised ja oskused, et mõista ja hinnata küberturvalisuse riske ja nende juhtimise tavasid ning nendest tulenevat mõju üksuse osutatavatele teenustele.“*

NIS2 artikli 2 lg 2 ingliskeelses versioonis on sätestatud: *Member States shall ensure that the members of the management bodies of essential and important entities are required to follow training, and shall encourage essential and important entities to offer similar training to their employees on a regular basis, in order that they gain sufficient knowledge and skills to enable them to identify risks and assess cybersecurity risk-management practices and their impact on the services provided by the entity.*

Lause ülesehitusest nähtub, et ergutustööd peab tegema just riik, mitte üksus. Ühtlasi pole võimalik sõnast „ergutama“ lugeda välja teenuse osutaja juhtorgani kohustust, mida peaks trahviga survestama. Mõttekäigu toetuseks räägib ka sõnakasutus *tagavad, et ... on kohustatud vs. ergutavad ... pakkuma; Shall ensure that ... are required vs. shall encourage ... to offer.* Esimene versioon on ilmselgelt karmim kui teine.

Juhtorgani liikmed on kohustatud läbima erikoolitusi, kuid töötajate koolituste osas on rõhk ergutamisel, mitte kohustusel. Seega ei saa töötajate koolituste pakkumist käsitleda juhtorganite kohustusena, mida peaks trahviga survestama.

KüTS § $18^4$ on lausa eraldi mainitud vastutust töötaja koolitamata jätmise osas: *”Kommenteeritava paragrahviga ette heidetav tegu on seotud KüTS §-s $6^1$ sätestatud nõuete rikkumisega, mida teenuse osutaja juhtorgan või juhtorgani liige peab täitma, et tagada KüTSi nõuete täitmine. Näiteks turvameetmete heaks kiitmine, nende järgimise jälgimine ja kontroll, vajalikel erikoolitustel osalemine ning tagada, et teenuse osutaja töötajad ja ametnikud saavad küberturvalisuse valdkonnaga seotud koolitusi.“*

Soovitus:

Muuta KüTS § 61 lg 3 ja § 184 sõnastust, et töötajate koolitamise kohustus ei oleks seotud trahviga, vaid jääks ergutuse tasandile vastavalt NIS2 direktiivi artikli 20 mõttele.

**4. KüTS § 8 lg $4^1$ ja $4^2$ puhul jääb arusaamatuks, miks seadusandja ei kirjuta ümber NIS2 teksti seoses varajase hoiatuse, intsidenditeate, vahearuande ja lõpparuandega**

Eelnõu § 8 lõiked $4^1$ ja $4^2$ käsitlevad varajase hoiatuse, intsidentide teavitamise, vahearuande ja lõpparuande nõudeid. Siiski on arusaamatu, miks seadusandja ei ole ülevõtmisel järginud NIS2 direktiivi teksti võimalikult täpset sõnastust. NIS2 direktiivi eesmärk on tagada ühtne ja harmoneeritud lähenemine liikmesriikides, mistõttu ühtlustatud sõnastuse kasutamine aitaks vältida võimalikke tõlgendamisprobleeme ning tagada õigusselgus.

Seletuskirjas viitab seadusandja sellele, et teavituse liigid on sisu ja tingimuste mõttes erinevad, mistõttu on otsustatud säilitada osaliselt kehtiv õigus (näiteks teavituste tähtaja osas) ja ühtlustada teavituste sisu. Siiski ei ole seletuskirjas selgitatud, miks ei ole direktiivi teksti sõnastust täpsemalt järgitud ning miks valiti selline erinev lähenemine.

Probleemid ja tähelepanekud:

1. Intsidentide teavituse tähtaeg: NIS2 direktiiv sätestab selgelt, et intsidentidest tuleb teavitada hiljemalt 72 tunni jooksul. Eelnõus puudub konkreetne säte selle tähtaja kohta, mis loob õigusselgusetuse ja võib viia tähtajast erinevate tõlgendusteni.

2. Teavituse ulatus ja sisu: Eelnõus on kirjas vaid kohustus esitada teave intsidenti puudutava sisu ja toimumise põhjuste kohta. Samas NIS2 direktiiv nõuab lisaks hinnangut, kas intsident oli ebaseaduslik või pahatahtlik, mis on oluline intsidentide tõsiduse hindamiseks ja riskide maandamiseks. Sellise teabe lisamine aitaks paremini täita direktiivi eesmärke.

3. Varajane hoiatus, vahearuanne ja lõpparuanne: Eelnõu reguleerib teavituste liike, kuid nende sisulised nõuded ja tingimused jäävad ebaselgeks. See jätab liiga palju ruumi tõlgendustele, mis võib viia liikmesriikide praktikas oluliste erinevusteni, mida NIS2 direktiiv just ühtlustada püüab.

Soovitused:

1. Ülevõtmise täpsus: Viia KüTS vastavusse NIS2 direktiiviga, kasutades võimalikult täpselt direktiivi sõnastust. See tagaks õigusselguse ning ühtlustatud praktika nii Eestis kui ka teistes liikmesriikides.

2. Intsidentide teavituse tähtaeg: Lisada eelnõusse selge viide, et intsidentidest tuleb teavitada hiljemalt 72 tunni jooksul vastavalt NIS2 direktiivi nõuetele. See aitab vältida olukordi, kus teavituse õigeaegsuse osas tekivad vaidlused või erisused.

3. Teavituse sisu täiendamine: NIS2 direktiivis nõutud teave, näiteks hinnang intsidentide ebaseaduslikkuse või pahatahtlikkuse kohta, tuleks lisada eelnõusse, et see vastaks direktiivi eesmärgile ja standarditele.

4. Seletuskirja täiendamine: Lisada seletuskirja selgitus, miks on mõni osa direktiivi sõnastusest üle võetud teisiti, kui otsustatakse mitte järgida direktiivi täpset sõnastust. See parandab läbipaistvust ja aitab selgitada seadusandja kaalutlusi.

**5. Ebaselgus juhtorgani definitsiooni osas**

Eelnõu § $6^1$ ja § $18^4$ kasutavad mõistet „juhtorgan“, kuid eelnõu tekstis ega seletuskirjas ei ole täpsustatud, kas see hõlmab juhatust, nõukogu või mõlemat. Eesti õiguses ei ole mõistet „juhtorgan“ iseseisvalt defineeritud; TsÜS eristab eraldi juhatust ja nõukogu (§ 31 lg 1 ja 2). See tekitab tõlgendamisprobleeme, eriti olukordades, kus juhtorgani kohustuste rikkumine toob kaasa rahatrahvi (kavandatav § $18^4$).

Eelnõu § $6^1$ võtab üle NIS2 direktiivi artikli 20, mille ingliskeelses versioonis kasutatakse mõistet „management bodies“. Direktiivi eestikeelses tõlkes on see tõlgitud kui „juhtorganid“, kuid direktiivi sisust tulenevalt viidatakse pigem juhatusele kui organile, kes vastutab igapäevaste juhtimisotsuste, sealhulgas küberturvalisuse meetmete heakskiitmise ja rakendamise jälgimise eest. Direktiivi eesmärk ei tundu hõlmavat nõukogu, kelle roll on järelevalve ja strateegiline suunamine.

Ka eelnõu muud sätted viitavad juhatuse reguleerimisele, näiteks:

- § $6^1$ lõike 2 nõuab juhtorgani liikmelt regulaarsete küberturvalisuse alaste koolituste läbimist. Seda vastutust ja oskuste vajadust seostatakse pigem juhatusega, kes vastutab operatiivjuhtimise eest, mitte nõukoguga, kelle ülesanded on strateegilisemad.
- § 14 lõike 13 punkt 2 kohaselt võib Riigi Infosüsteemi Amet nõuda elutähtsa teenuse osutaja nõukogult või osanikelt juhatuse liikme volituste ajutist peatamist (vt kriitikat selle sätte kohta allpool). Ka sellest haldussunni sättest saab järeldada, et juhtorganiks saab pidada üksnes juhatust.

Soovitus:

Täpsustada eelnõu § $6^1$ ja § $18^4$ sõnastust, et oleks selge, kas „juhtorgan“ viitab ainult juhatusele, nõukogule või mõlemale. Lähtudes direktiivi eesmärgist ja Eesti õiguse kontekstist, oleks asjakohane viidata juhatusele.

**6. Elutähtsa üksuse juhatuse liikmete volituste peatamise menetluse puudulikkus**

Eelnõu § 14 lõike 13 punkti 2 kohaselt võib Riigi Infosüsteemi Amet nõuda ettekirjutusega elutähtsa teenuse osutaja nõukogult või osanikelt juhatuse liikme volituste ajutist peatamist.

Juhatuse liikme volituste peatamise nõue on äärmuslik meede, mis mõjutab otseselt juhatuse liikme õigusi ja ettevõtte juhtimise toimimist. Sellise meetme rakendamine peab olema selgelt põhjendatud ja proportsionaalne, et vältida järelevalveasutuse meelevaldset otsustusõigust ning tagada õigusselgus ja ettevõtjate õiguskindlus.

Esiteks. NIS2 direktiiv ei anna regulaatorile endale pädevust selliste meetmete rakendamiseks. Direktiivi kohaselt saab regulaator üksnes taotleda “asjaomaselt organilt või kohtult” kooskõlas liikmesriigi õigusega, et keelata füüsilisel isikul, kes täidab selles elutähtsas üksuses tegevjuhina või seadusliku esindajana juhtimisülesandeid, selles üksuses ajutiselt juhtimisülesannete täitmine. Seega on eelnõus pakutud lahendus vastuolus direktiiviga.

Teiseks. NIS2 direktiiv nõuab, et "sellise ajutise peatamise või keelu kehtestamise suhtes kohaldatakse kooskõlas liidu õiguse üldpõhimõtete ja hartaga asjakohaseid menetluslikke tagatisi, sealhulgas õigust tõhusale õiguskaitsevahendile ja õiglasele kohtumenetlusele, süütuse presumptsiooni ja kaitseõigust." Eelnõus ja seletuskirjas puudub selgitus nende õigusriiklike menetluslike tagatiste kohaldatavusest juhatuse või nõukogu liikme või osaniku kaitseks. Samuti ei täpsustata, kuidas toimub sellise erandliku ja Eesti õiguskorras ebatavalise meetme kohaldamise menetlus. Mõistlik oleks lähtuda HKMS-s sätestatud haldustoiminguks loa taotlemise regulatsioonist.

Soovitused:

1. Kaaluda, kas juhatuse liikme volituste peatamise meetme kohaldamine on kooskõlas NIS2 direktiiviga ja Põhiseadusega.

2. Täpsustada meetme kohaldamise menetlust tagamaks asjaosalistele õigusriiklikud menetluslikud tagatised.

**7. Eelnõu rakendamise osas puudub õigusselgus**

Eelnõu seletuskirjas on märgitud, et lisanduvatele organisatsioonidele nähakse ette kolmeaastane üleminekuaeg, mille jooksul tuleb oma tegevus viia küberturvalisuse seaduse põhiliste nõuetega kooskõlla. Samas puudub vastav teave seaduse eelnõu tekstis ning viidatud tähtaeg näib tulenevat üksnes rakendusmääruse eelnõust „Vabariigi Valitsuse 9. detsembri 2022. a määruse nr 121 „Võrgu- ja infosüsteemide küberturvalisuse nõuded" muutmine". Viidatud määruse eelnõu käsitleb vaid standardite (E-ITS või ISO/IEC 27001) rakendamise kohustust, kuid küberturvalisuse seaduse eelnõuga kaasnevad täiendavad kohustused mitte ainult uutele vaid ka juba olemasolevatele subjektidele.

Kehtiva küberturvalisuse seaduse kohaselt kohaldatakse seadust teenuse osutajale vaid ulatuses, mis puudutab võrgu- ja infosüsteeme. Eelnõu kohaselt tuleb aga seadusest tulenevaid nõudeid rakendada kogu organisatsioonile tervikuna, mistõttu peaks ilmselt olema üleminekuaeg mitte üksnes uutele subjektidele vaid ka olemasolevatele.

Soovitused:

1. Eelnõus peaks ette nähtud üleminekuaeg kehtima mitte ainult lisanduvatele subjektidele, vaid ka juba olemasolevatele subjektidele.

2. Arvestades, et seaduse eelnõuga laieneb kohustatud subjektide ring, peaks õigusselguse tagamiseks vastav teave uutele subjektidele olema paremini kommunikeeritud, näiteks eelnõu seletuskirja lisatavate täiendavate selgituste kaudu.

Loodame, et Eesti Advokatuuri ettepanekud on abiks ning oleme ka valmis edaspidiseks koostööks.

Lugupidamisega

*allkirjastatud digitaalselt*

Imbi Jürgen
Esimees

Merit Aavekukk-Tamm 6979 253
merit.aavekukk-tamm@advokatuur.ee