

Vabariigi Valitsuse 22. juuni 2006. a määruse nr 140 „Nõuded sideteenuse osutamisele ja sidevõrkude tehnilised nõuded“ ja 11. detsembri 2015. a määruse nr 129 „Vabariigi Valitsuse julgeolekukomisjoni põhimäärus“ muutmise määruse eelnõu seletuskiri

1. Sissejuhatus

Vabariigi Valitsuse 22. juuni 2006. a määruse nr 140 „Nõuded sideteenuse osutamisele ja sidevõrkude tehnilised nõuded“ (edaspidi *VV määrus nr 140*) ning 11. detsembri 2015. a määruse nr 129 „Vabariigi Valitsuse julgeolekukomisjoni põhimäärus“ muutmise eesmärk on kehtestada meetmed üldkasutatava elektroonilise side teenuse (edaspidi: *sideteenus*) ja üldkasutatava elektroonilise side võrgu (edaspidi *sidevõrk*) riigi julgeoleku huvidele vastavuse tagamiseks.

Määrus kehtestatakse elektroonilise side seaduse (edaspidi *ESS*)¹ § 87 lõigete 2– 2² ning riigikaitseaduse² § 4 lõike 2 alusel.

ESS § 87 lõike 2 punkt 4 alusel on Vabariigi Valitsusel volitus, lähtudes ESS § 87 lõikes 1 sätestatud põhimõtetest ja eesmärkidest, kehtestada sidevõrkude tehnilised nõuded ja nõuded sideteenuse osutamisele, kui see on vajalik avaliku korra ja riigi julgeoleku tagamiseks. Käesolevas määruses kehtestatakse ESS § 87 lõike 2 punkt 4 alusel nõuded sideteenuse osutamisele, kuna see on vajalik avaliku korra ja riigi julgeoleku tagamiseks. Selle volitusnormi alusel kehtestatakse nõue, et sideteenuse osutamisel kasutatav riist- ja tarkvara ei tohi ohustada riigi julgeolekut.

ESS § 87 lõiked 2¹ ja 2² jõustusid 30. mail 2020. Nendega anti Vabariigi Valitsusele õigus kehtestada riigi julgeoleku tagamiseks sideettevõtjale kohustus teavitada sidevõrgus kasutatavast riist- ja tarkvarast ning õigus kehtestada riigi julgeoleku tagamiseks sideettevõtjale kohustus taotleda sidevõrgu riist- ja tarkvara kasutamiseks luba. Nende normide alusel kehtestatakse käesoleva määrusega sideettevõtjatele sidevõrgus kasutatava riist- ja tarkvara teavitamise kohustus ning kasutusloa taotlemise kohustus. Keeldu osutada sideteenust kasutades riist- ja tarkvara, mis ohustab riigi julgeolekut, hinnatakse ja kasutamise keeldu rakendatakse riist- ja tarkvara kasutusloa menetluses. Samuti kehtestatakse teavitamise kohustuse kord, asutus, keda tuleb teavitada, ning loa taotlemise kord ja loa andev asutus.

Riigikaitseaduse § 4 lõige 2 sätestab, et Vabariigi Valitsuse julgeolekukomisjon täidab talle julgeolekuasutuste seaduse ja teiste seadustega pandud ning Vabariigi Valitsuse antud ülesandeid. Selle sätte alusel muudetakse käesoleva määrusega Vabariigi Valitsuse julgeolekukomisjoni põhimäärust, kuhu lisatakse paragrahv Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogu (edaspidi küberjulgeoleku nõukogu) kohta.

1.1. Sisukokkuvõte

¹ Elektroonilise side seadus. RT I, 20.05.2020, 34.

² Riigikaitseadus. RT I, 13.03.2019, 147.

Info- ja kommunikatsioonitehnoloogia (edaspidi IKT) on viimaste aastakümnetega kiiresti arenenud. See on muutnud ühiskonna (kaasa arvatud Eesti) sõltuvaks tehnoloogilistest lahendustest. Eestis on 99% avalikest teenustest saadaval interneti kaudu e-teenustena ning võrreldes paljude riikidega on Eesti sõltuvus IKT-st erakordselt suur.

Sidesektor on selles kontekstis baastaristu pakkuja, mis võimaldab digiühiskonnal toimida ja areneda. Sidevõrgu tehnoloogiad on aluseks suurt töökindlust ja usaldusväärsust nõudvates kriitilise tähtsusega valdkondades nagu meditsiinis, transpordis, panganduses, energeetikas ning tõusva trendina robotikas ja tehisintellekti lahendustes. Kuna kõik andmed liiguvad läbi sidevõrkude, omavad sidevõrgud riigi julgeoleku kontekstis järjest olulisemat rolli.

Sidevõrgu tehnoloogiad on digiühiskonnas integreeritud peaaegu kõikidesse süsteemidesse, kaasa arvatud elutähtsatesse teenustesse. Seetõttu tuleb IKT taristut käsitleda fundamentaalselt kriitilise infrastruktuurina. Uute sidevõrkude nagu 5G kasutuselevõtuga kaasneva kiire internetiühenduse kättesaadavuse tõus annab põhjust prognoosida, et nii inimeste kodudes kui ka era- ja avalikus sektoris suureneb järgnevatel aastatel internetiühendusega seadmete hulk olulisel määral. Rahvusvaheline mobiilsideettevõtjate ühendus GSMA hindab, et 2025. aastaks kasvab internetiga ühendatud seadmete arv tänasega võrreldes kolmekordseks ning jõuab ülemaailmselt 25 miljardi seadmeni.³

On paratamatu, et sidevõrkude ning neisse ühendatud seadmete arvu ja olulisuse kasvuga muutub IKT süsteemide manipulatsioonide ja rünnete eest kaitsmine keerukamaks. Keerukust lisavad sagedased tarkvarauuendused ja kriitilised turvapaigad, mille paigaldamisega pole aega oodata. Kaasaegsed seadmed pannakse kokku lugematute spetsialiseerunud ettevõtete komponentidest üle maailma, muutes tarneahela kontrollimise kalliks ning keeruliseks. Limiteeritud kontrollivõimekuse tõttu on seadmete/tehnoloogia tootja usaldamine muutunud kriitiliseks faktoriks. Tehnoloogia tootja pole enam pelgalt seadmete ja tarkvara tarnija, vaid laiemalt tehnoloogilise teenuse pakkuja, kellega ehitatakse üles aastatepikkune koostöösuhe.

Eesti IKT taristu puhul tuleb samuti arvestada riigikaitse aspektiga. Eesti riigikaitse tugineb laia riigikaitse käsitusele ning NATO (Põhja-Atlandi Lepingu Organisatsioon) kollektiivkaitsesele. See tähendab, et riigi kaitsmine ei hõlma üksnes sõjalist riigikaitset, vaid riigi kaitseks peavad valmis olema kõik riigiasutused ja kogu ühiskond.⁴ Riigi tõhus kaitse tagatakse nii sõjaliste kui ka mittesõjaliste võimete, ressursside ja tegevustega avalikust, era- ja kolmandast sektorist. IKT taristu on selles kontekstis oluline riigi ja ühiskonna toimepidevuse tagamiseks ning riigikaitse korraldamiseks. Riskianalüüside koostamisel tuleb seetõttu arvesse võtta Eesti iseseisva kaitsevõime vajadusi ning meie liitlaste hinnanguid ja piiranguid tehnoloogia kasutamise osas. Eesmärk on tagada olukord, kus meie IKT taristu on turvaline ja usaldusväärne nii meie endi kui ka NATO liitlaste silmis.

Võrkude kvaliteedi kindlustamiseks, küberrünnete mõju minimeerimiseks ja poliitiliste manipulatsioonide vältimiseks tuleb tagada, et sidevõrkude rajamine ning nende vahendusel sideteenuste osutamine toimuks turvalise tehnoloogia abil ning usaldusväärse partneri poolt.

³ Global System for Mobile Communications. New GSMA Study: 5G to Account for 15% of Global Mobile Industry by 2025 as 5G Network Launches Accelerate. Pressiteade, 25.02.2019. Kättesaadav: <https://www.gsma.com/newsroom/press-release/new-gsma-study-5g-to-account-for-15-of-global-mobile-industry-by-2025/>.

⁴ Kättesaadav: <https://www.riigikantselei.ee/et/julgeoleku-ja-riigikaitse-koordineerimine>.

Euroopa Komisjon on 5G sidevõrkude turvalisuse osas soovitanud⁵, et liikmesriigid kaaluksid riskide hindamisel nii tehnilisi kui ka muid strateegilisi faktoreid. Tehnilisteks faktoriteks on näiteks turvanõrkused (haavatavused, tagauksed), mida võidakse kasutada küberluureks ning andmete ja süsteemide häirimiseks või hävitamiseks. Muudeks strateegilisteks (usaldusväärsuse) faktoriteks on muu hulgas kolmandate riikide mõju tehnoloogia tootjale, mõjujõuga riigi valitsemisvorm ja julgeolekualaste koostöölepingute ning teiste küberturvalisust ja privaatsust puudutavate lepingute olemasolu või nende puudumine.

Samuti soovitab Euroopa Komisjon pöörata riskianalüüside tegemisel tähelepanu kõikidele sidevõrgu seadmetele ja komponentidele terve elutsükli jooksul. See puudutab kogu riist- ja tarkvara disaini, arendamise, hankimise, rakendamise, opereerimise ja hooldamise faasides.

Euroopa Liidu võrgu- ja infoturbe koostöörühmis on liikmesriigid välja töötanud 5G sidevõrkude riskianalüüsi⁶ ning öelnud, et tuleviku sidevõrgud (5G) mängivad kesket rolli Euroopa Liidu ühiskonna ja majanduse digitaalses transformatsioonis ning seetõttu on 5G sidevõrkude turvalisus kriitilise tähtsusega. Kõige suurema ja tõenäolisema ohuna nähakse Euroopa Liidu väliseid riike, kellel on huvi ja ressursse viia läbi kõrgelt arenenud küberrünnakuid. Eriti ohtlikud on riigid, kellele omistatud küberrünnete ajalugu näitab agressiivse küberprogrammi olemasolu.

Euroopa Liidu koordineeritud riskianalüüsile tuginedes avaldati 2020. aasta jaanuaris Euroopa Liidu riikide ühine meetmepakett 5G võrkude turvalisuse tagamiseks⁷, mis sisaldab strateegilisi ja tehnilisi meetmeid ning neid toetavaid tegevusi, mille rakendamise tulemusena on võimalik riske tulemuslikult maandada ja tagada turvaliste 5G võrkude kasutuselevõtt kogu Euroopa Liidus. Strateegiliste meetmete all soovitatakse muu hulgas suurendada riigi ametiasutuste regulatiivvolitusi, mis võimaldaks neil karmistada mobiilsideoperaatoritele kehtivaid turvanõudeid ning kasutada *ex ante* sekkumise õigust, et piirata, keelata või seada tingimusi tehnoloogia hankimisele, paigaldamisele või kasutamisele. Lisaks soovitatakse hinnata tarnijate⁸ riskiprofiili ja kohaldada asjakohaseid piiranguid kõrge riskiga tarnijate suhtes. 2020. aasta juulis avaldatud Euroopa Liidu ühiste leevendusmeetmete rakendamise aruandest⁹ selgub, et enamik liikmesriikidest on laiendanud või kohe laiendamas riiklike reguleerivate asutuste pädevusi ning mitmed liikmesriigid on juba seadnud piiranguid kõrge riskiga tarnijate tehnoloogia kasutusele.

Ka varasemalt on sideettevõtjatel olnud ESS § 87 lg 1 järgi üldine kohustus arvestada sideteenuse osutamisel avaliku korra ja riigi julgeolekuga. Käesoleva määrusega täpsustatakse, kuidas peavad ettevõtjad riigi julgeoleku huve arvesse võtma.

⁵ ELT L 88, 29.3.2019, lk 42–47. Kättesaadav: <https://eur-lex.europa.eu/legal-content/ET/TXT/?qid=1569311905525&uri=CELEX:32019H0534>.

⁶ Kättesaadav: <https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security>

⁷ Kättesaadav: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_127

⁸ Nii liikmesriikide ühises 5G võrkude turvalisuse meetmepaketis kui ka näiteks Ameerika Ühendriikide ja Eesti vastastiku mõistmise memorandumis 5G turvalisuse teemal on kasutatud inglise keelses tekstis terminit *supplier*, mis on käesolevas seletuskirjas tõlgitud tarnijaks. Samas on tehnoloogiliste ja strateegiliste riskide aspektist oluline eestkätt tootja riskiprofiili hindamine, mitte sellise tarnija riskiprofiili hindamine, kes tootmisprotsessis ei osale ning ei oma pärast sideettevõtjale toote müüki kasutusõigust. Sellest tulenevalt on sissejuhatuses kasutatud laiemat terminit „tarnija“, kuid regulatiivses osas juriidiliselt täpsemat terminit „tootja“.

⁹ Kättesaadav: <https://ec.europa.eu/digital-single-market/en/news/report-member-states-progress-implementing-eu-toolbox-5g-cybersecurity>

Riigi julgeoleku tagamiseks kehtestatakse määrusega nõue, et sideteenuse osutamisel kasutatav riist- ja tarkvara ei tohi ohustada riigi julgeolekut. Ohte riigi julgeolekule käsitletakse kahes grupis: 1) tootja, hooldus- või tugiteenuste pakkuja profiilist tulenevad ohud, mille tõttu on riist- ja tarkvara kasutamine sideteenuse kasutamisel kõrge riskiga ning 2) muud põhjused, millal on riist- ja tarkvara kasutamine ohuks riigi julgeolekule. Muud põhjused puudutavad eelkõige riist- ja tarkvara tehnilisi riske (näiteks riistvara turvaviga), mis ei ole seotud riist- või tarkvara tootja, hooldus- või tugiteenuste pakkuja profiiliga.

Riist- ja tarkvara ohtu riigi julgeolekule hinnatakse riist- ja tarkvara kasutusloa menetluses. Kasutusloa menetluses hindavad julgeolekuasutused, Riigi Infosüsteemi Amet (edaspidi *RIA*) ning küberjulgeoleku nõukogu, kas tegemist on tootja, hooldus- või tugiteenuste pakkuja profiilist tulenevalt kõrge riskiga riist- või tarkvaraga või kas riist- või tarkvara kasutamine võib ohustada riigi julgeolekut muul põhjusel.

Kasutusloa kohustus rakendub riist- ja tarkvarale, mis plaanitakse kasutusele võtta pärast määruse jõustumist ehk eelduslikult pärast 1. novembrit 2020. Kasutusloa taotlus tuleb esitada enne riist- või tarkvara plaanitavat kasutusele võtmist. Sellele üldreeglile on kolm erisust. Esiteks hõlmab kasutusloa kohustus riist- ja tarkvara, mis on kasutusele võetud enne 1. novembrit 2020, kui selles võetakse 5G *non-standalone* (edaspidi 5G NSA) või uuema mobiilsidevõrgu standardi funktsioon kasutusele pärast 1. novembrit 2020. Sellise riist- ja tarkvara kasutusloa taotlus tuleb esitada enne plaanitavat 5G NSA või uuema mobiilsidevõrgu standardi funktsiooni kasutusele võttu. Teiseks, vahemikus 1. november 2020 kuni 1. jaanuar 2029 kasutusele võetava riist- ja tarkvara, millel ei ole kriitilist funktsiooni¹⁰ ega 5G NSA või uuema mobiilsidevõrgu standardi funktsiooni, korral tuleb kasutusloa taotlus esitada hiljemalt 1. juuliks 2029. Kolmandaks, kui riist- või tarkvara on tarvis viivitamata paigaldada küberintsidendi kõrvaldamiseks või selle vahetuks ärahoidmiseks, esitab sideettevõtja kasutusloa taotluse hiljemalt kümnendal tööpäeval pärast riist- või tarkvara paigaldamist, kui üldnormide järgi on riist- ja tarkvaral kasutusloa taotlemise kohustus.

Määrusega seatakse keeld osutada sideteenust kõrge riskiga riist- ja tarkvara kasutades. Keeldu rakendatakse riist- ja tarkvara kasutusloa menetluse kaudu. Kõrge riskiga riist- ja tarkvara on defineeritud tootja, hooldus- või tugiteenuste pakkuja profiili kaudu (vt § 3² lõige 3). Keeld ei hõlma riist- ja tarkvara, mis on kasutusele võetud enne 1. novembrit 2020, välja arvatud juhul, kui sellel on 5G NSA või uuema mobiilsidevõrgu standardi funktsioon. Kui kasutusloa menetluses tuvastatakse, et tegu on kõrge riskiga riist- ja tarkvaraga, ei anta sellele kasutusluba. Kasutusluba antakse teatud tähtajani vaid kahel juhul. Esiteks, kui tegu on 5G NSA või uuema mobiilsidevõrgu standardi funktsiooniga kõrge riskiga riist- ja tarkvaraga, millel ei ole kriitilist funktsiooni, antakse kasutusluba 1. jaanuarini 2024. Teiseks, kui tegu on kõrge riskiga riist- ja tarkvaraga, millel ei ole kriitilist funktsiooni ega 5G NSA või uuema mobiilsidevõrgu standardi funktsiooni, võib seda kasutada 1. jaanuarini 2030, ent korraga antakse kasutusluba kuni 8 aastaks.

¹⁰ Riist- ja tarkvara kriitilised funktsioonid on järgnevad: 1) Euroopa Telekommunikatsiooni Standardite Instituudi standardite kohaselt tuumikvõrgu funktsioon; 2) funktsioon, mille kaudu või mille häirimisel on võimalik mõjutada vähemalt 1000 lõppkasutajat või teise sideettevõtja sidevõrku; 3) funktsioon, mille eesmärk on võimaldada jälitustoimingu teostamist või sõnumi saladuse õiguse piiramist.

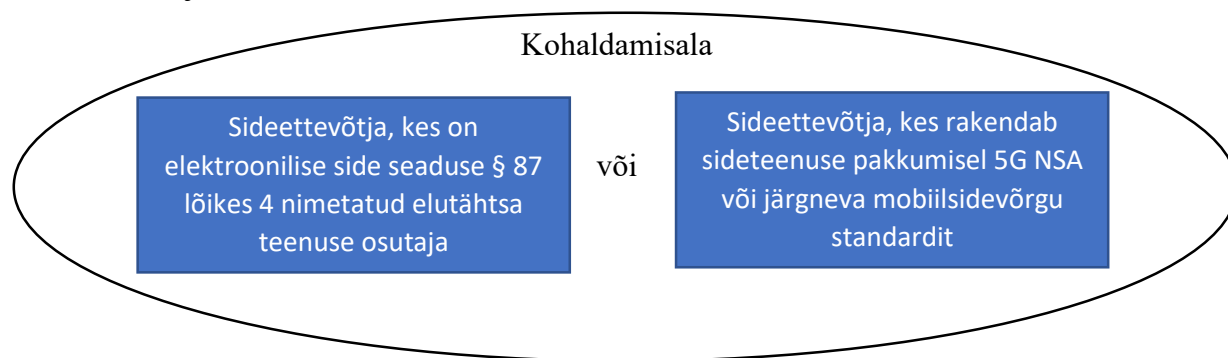
Kui riist- või tarkvara kasutusloa menetluses leitakse, et riist- ja tarkvara võib ohustada riigi julgeolekut muul põhjusel kui tootja, hooldus- või tugiteenuste profiili tõttu, seatakse sellisele riist- või tarkvarale kasutusloas kasutamise tingimused või keeldutakse kasutusloa andmisest.

Riist- ja tarkvara kasutusloa menetluses antakse ettevõtjale arvamuse ja vastuväidete esitamise võimalus ning kaalutakse riist- või tarkvara kasutamise keelamise ja tingimuste seadmise mõju side toimepidevusele, sideturule ja konkurentsile.

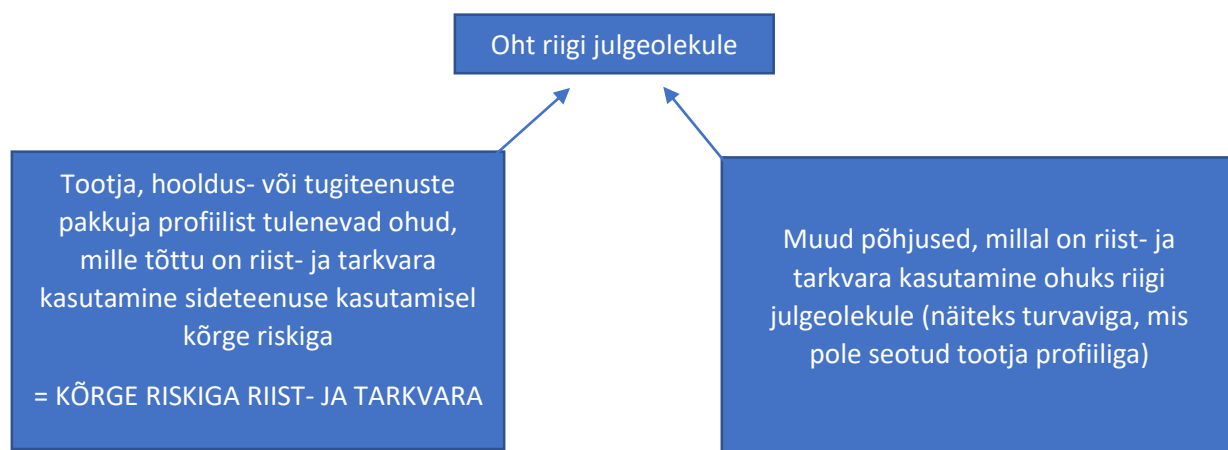
Riist- ja tarkvara kasutusloa väljastab Tarbijakaitse ja Tehnilise Järelevalve Amet (edaspidi ka *TTJA*). Kasutusloa menetluses on arvamuse andjateks julgeolekuasutused ja Riigi Infosüsteemi Amet. Kooskõlastajaks on küberjulgeoleku nõukogu.

Samuti kehtestatakse riigi julgeoleku tagamiseks määrusega sideettevõtjale teavitamiskohustus. Teavitamiskohustus kehtib määruse jõustumisest kogu sidevõrgus kasutatavale riist- ja tarkvarale. Teavituskohustuse kaudu saab riik tervikliku pildi sidevõrkudes kasutuses olevast riist- ja tarkvarast, sealhulgas riist- ja tarkvarast, millele kasutusloa kohustust ei rakendata. Teavitada tuleb iga kalendriaasta 1. märtsiks sidevõrgus vastava aasta 1. jaanuari seisuga kasutatavast riist- ja tarkvarast.

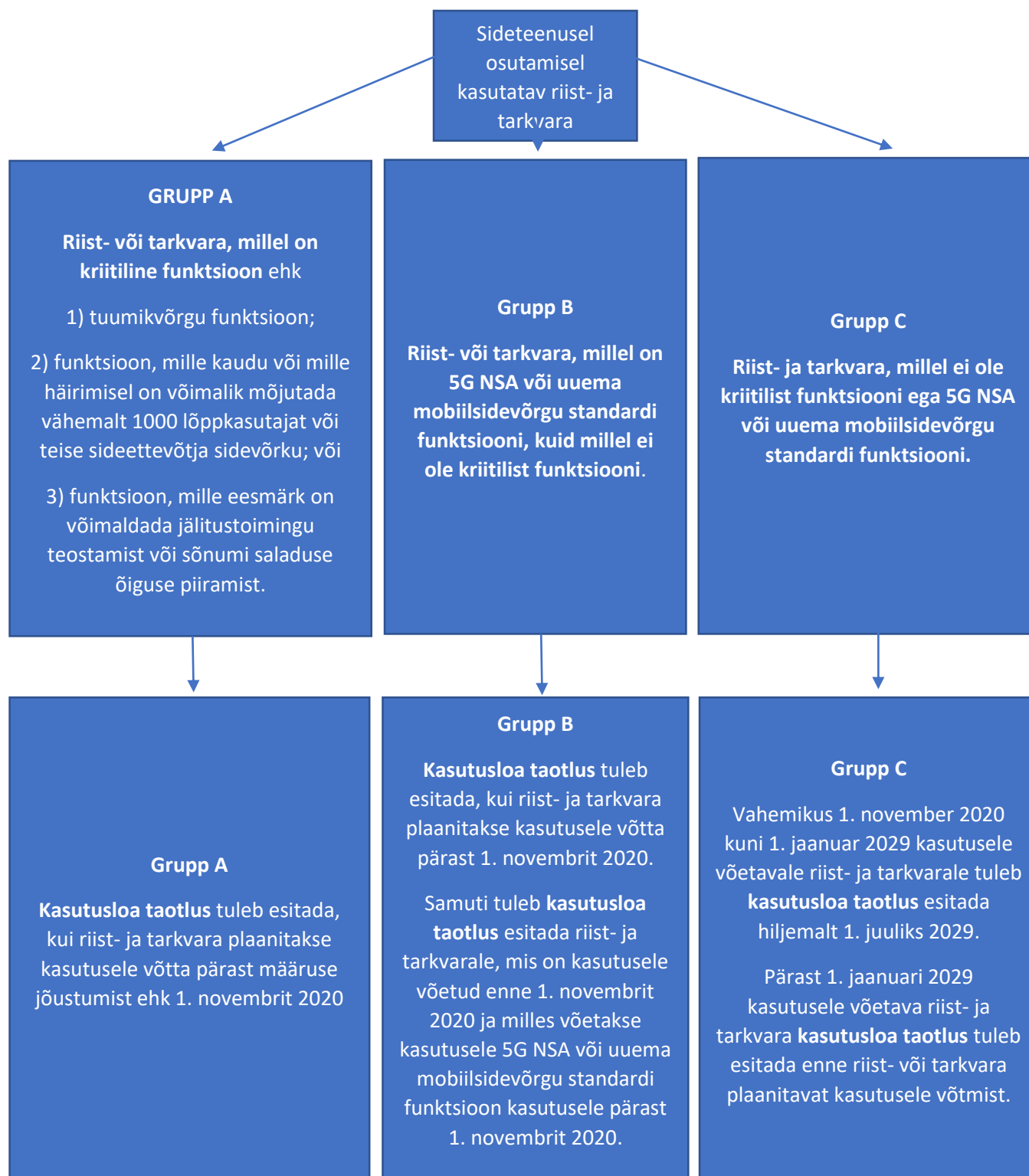
Kokkuvõttev joonis kohaldamisalast:

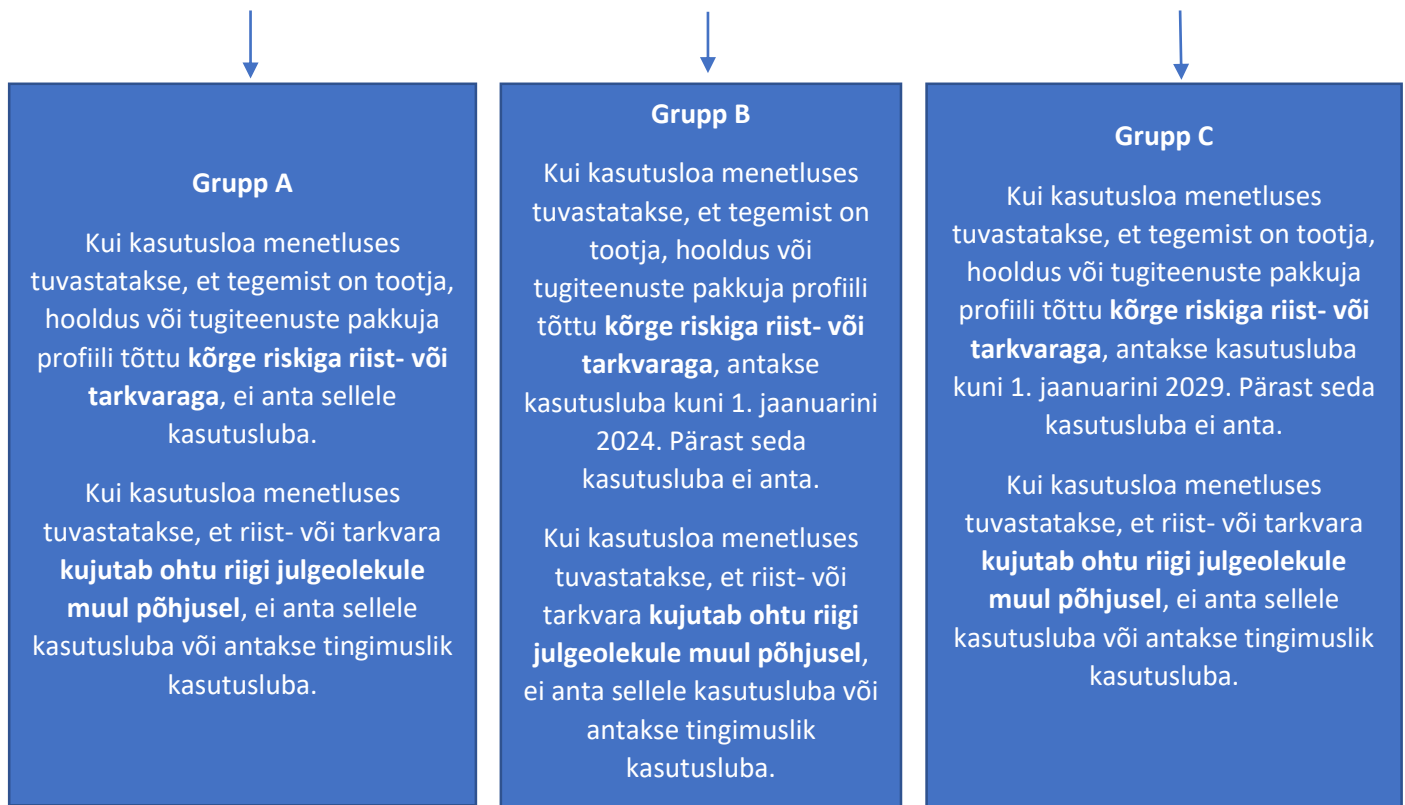


Kokkuvõttev joonis riigi julgeoleku ohugrupidest:



Kokkuvõttev joonis riist- ja tarkvara liikidest kasutusloa kohustuse ning kõrge riskiga riist- ja tarkvara keelu kontekstis:





1.2. Eelnõu ettevalmistaja

Määruse eelnõu on välja töötanud IKT seadmete usaldamise poliitika töörühm, mis moodustati väliskaubandus- ja infotehnoloogiaministri 26.06.2019. a käskkirjaga nr 1.1-1/19-100. Töörühma juhtis Majandus- ja Kommunikatsiooniministeeriumi riigi küberturvalisuse poliitika juht Raul Rikk (tel: 625 6338, e-post: raul.rikk@mkm.ee).

Töörühma koosseisu kuulusid Majandus- ja Kommunikatsiooniministeeriumi, Justiitsministeeriumi, Kaitseministeeriumi, Kaitsepolitseiameti, Kaitseväe, Politsei- ja Piirivalveameti, Registrate ja Infosüsteemide Keskuse, Riigi Infosüsteemi Ameti, Riigi Infokommunikatsiooni SA, Riigikantselei, Siseministeeriumi, Tarbijakaitse ja Tehnilise Järelevalve Ameti, Välisministeeriumi ja Välisluureameti esindajad.

Määruse eelnõu ja seletuskirja on vormistanud Majandus- ja Kommunikatsiooniministeeriumi küberturvalisuse õigusnõunik Kea Kohv (e-post: kea.kohv@mkm.ee), sideosakonna juhataja asetäitja Mart Laas (tel: 625 6441, e-post: mart.laas@mkm.ee) ja peaspetsialist Liisi Moks (tel: 639 7665; e-post: liisi.moks@mkm.ee). Määruse osas tegi juriidilisi ettepanekuid Majandus- ja Kommunikatsiooniministeeriumi õigusnõunik Ave Henberg (tel: 625 6360, e-post: ave.henberg@mkm.ee).

1.3. Märkused

Eelnõu ei ole seotud muu menetluses oleva eelnõu ega Vabariigi Valitsuse tegevusprogrammiga.

2. Eelnõu sisu ja võrdlev analüüs

Määruse eelnõu koosneb kolmest paragrahvist, millest esimene on VV määruse nr 140 muutmine, teine on Vabariigi Valitsuse 11. detsembri 2015. a määruse nr 129 „Vabariigi

Valitsuse julgeolekukomisjoni põhimäärus“ muutmine ning kolmas puudutab määruse jõustumist.

Eelnõu § 1.

Eelnõu § 1 punktiga 1 asendatakse VV määruse nr 140 preambulas sõnad „lõike 2“ sõnadega „lõigete 2–2²“. Muudatus on vajalik, et uuendada VV määruses nr 140 nimetatud ESS volitusnorme (vt pikemalt sissejuhatuses). Lisanduvate volitusnormide alusel kehtestatakse määrusega kasutusloa kohustus ja teavitamiskohustus. Volitusnorm, mille alusel võib seada nõudeid sideteenuse osutamisele, kui see on vajalik avaliku korra ja riigi julgeoleku tagamiseks, sisaldub juba varasemas VV määruses nr 140.

Eelnõu § 1 punktiga 2 muudetakse VV määruse nr 140 §-i 1, millega on sätestatud määruse eesmärk. Paragrahvi 1 tekst muudetakse ja sõnastatakse järgmiselt: „Määrusega kehtestatakse nõuded üldkasutatava elektroonilise side teenuse (edaspidi *sideteenus*) osutamisele ning üldkasutatava elektroonilise side võrkudele (edaspidi *sidevõrk*). Määruse kehtestamise eesmärgiks on elektroonilise side seaduse § 87 lõike 2 punktides 1, 3 ja 4 ning lõigetes 2¹ ja 2² sätestatu reguleerimine.“ Sõnastust muudetakse, kuna võrreldes varasemaga lisanduvad eesmärkidena ESS § 87 lõike 2 punktis 4 sätestatu reguleerimine ehk nõuded avaliku korra ja riigi julgeoleku tagamiseks ning ESS § 87 lõigetes 2¹ ja 2² sätestatu reguleerimine ehk kasutusloa kohustus ja teavitamiskohustus riigi julgeoleku tagamiseks. Võrreldes varasema sõnastusega pole uues sõnastuses kriteeriumit, et nõuded kehtivad vaid sideteenuste osutamisel lõppkasutajatele. Nõuded kehtivad ka sel juhul, kui sideteenust osutatakse teisele sideteenuse osutajale.

Eelnõu § 1 punktiga 3 täiendatakse VV määrust nr 140 uue peatükiga 2¹. Uus peatükk nimega „Nõuded sideteenusele ja sidevõrgule riigi julgeoleku tagamiseks“ koosneb viiest paragrahvist.

Paragrahv 3¹ sätestab nõuete kohaldamisala. **Paragrahv 3¹ lõikega 1** sätestatakse subjektide ring, kellele nõuded kohalduvad. Subjektideks on sideettevõtjad, kes vastavad vähemalt ühele kahest tingimusest: 1) sideettevõtja on ESS § 87 lõikes 4 nimetatud elutähtsa teenuse osutaja või 2) rakendab sideteenuse pakkumisel Euroopa Telekommunikatsiooni Standardite Instituudi viienda või järgneva põlvkonna mobiilsidevõrgu standardeid.

ESS § 87 lõikes 4 nimetatud elutähtsa teenuse osutaja (ETO) on telefoniteenuse, mobiiltelefoniteenuse ja andmesideteenuse osutaja, kelle teenust tarbib vähemalt 10 000 lõppkasutajat. Eestis on selliseid sideettevõtjaid neli. Kolm suuremat on Telia, Elisa ja Tele2. Samuti läheb 10 000 reegli alla STV. Kolme suurima ETO osakaal elektroonilise side turul on ca 95%. Elutähtsa teenuse ja elutähtsa teenuse osutaja mõiste tuleneb hädaolukorra seadusest (edaspidi *HOS*). Elutähtis teenus on teenus, millel on ülekaalukas mõju ühiskonna toimimisele ja mille katkemine ohustab vahetult inimeste elu või tervist või teise elutähtsa teenuse või üldhuviteenuse toimimist. HOS mõistes peab iga valdkonna elutähtsa teenuse osutaja (side mõistes sideettevõtja, kelle teenust tarbib vähemalt 10 000 lõppkasutajat) tagama oma valdkonna elutähtsa teenuse (side mõistes HOS § 36 lõike 1 punktid 5–7 ehk telefoni-, mobiiltelefoni- ja andmesideteenuse) toimepidevuse. Elutähtsa teenuse toimepidevus on teenuse osutaja järjepideva toimimise suutlikkus ja järjepideva toimimise taastamise võime pärast katkestust. Täpsemini, elutähtsa teenuse toimepidevuse tagamine on suunatud sellele, et elutähtis teenus oleks kättesaadav tarbijatele igal ajahetkel, ka hädaolukorra ajal. Selleks peab elutähtsa teenuse osutaja olema võimeline osutama teenust katkematult olenemata olukorrast

ehk omama vastavaid vahendeid, tehnilist ettevalmistust jne ning olema suuteline võimalikult kiiresti taastama teenuse katkematu osutamise.¹¹

Alternatiivina on sideettevõtja nõuete subjekt, kui ta „rakendab sideteenuse pakkumisel Euroopa Telekommunikatsiooni Standardite Instituudi viienda või järgneva põlvkonna mobiilsidevõrgu standardeid“. Tingimus rakendub olenemata sellest, millises sagedusvahemikus sideettevõtja sideteenuse pakkumisel viienda (5G) või järgneva põlvkonna mobiilsidevõrgu standardeid rakendab. Muuhulgas on hõlmatud 3410–3800 MHz, 694-790 MHz, 24,25-27,50 GHz raadiosagedusalad, kus on 5G-d kõige efektiivsem arendada.

Sideteenus on üldkasutatava elektroonilise side teenus. Seda mõistet on avatud ESS-is ning lühendit „sideteenus“ kasutatakse ka kehtivas VV määruses nr 140. ESS § 2 p 68 kohaselt on üldkasutatav elektroonilise side teenus (lühidalt sideteenus) teenus, mida sideettevõtja pakub vastaval sideteenuse turul üldistel alustel kõikidele isikutele, ilma et isikud peaksid vastama mingitele neid teistest sarnastest isikutest eristavatele tunnustele. Teenus on üldkasutatav eelkõige siis, kui selle osutamine on kestev ja järjepidev ning seda pakutakse sisuliselt ühesugustel tingimustel.

Viienda põlvkonna (5G) mobiilsidevõrgu standardi all on mõeldud nii 5G NSA-d kui ka 5G SA-d. 5G NSA (Non Stand Alone – mitte eraldiseisev) all on mõeldud võrke, mille omadused ja funktsioonid on defineeritud standardiga *ETSI (European Telecommunications Standards Institute) TS 123 501 (V15.10.0): "5G; System Architecture for the 5G System (3GPP TS 23.501 version 15.10.0 Release 15"*. 5G SA (Stand Alone – eraldiseisev) all on mõeldud võrke, mille omadused ja funktsioonid on defineeritud standardiga *ETSI TS 123 501 (V16.5.0): „5G; System Architecture for the 5G System (3GPP TS 23.501 version 16.5.0 Release 16)"*. Järgneva põlvkonna all on mõeldud kõiki 5G-le järgnevaid põlvkondi, nt 6G, 7G jne.

Euroopa Telekommunikatsiooni Standardite Instituut (inglise keeles *European Telecommunications Standards Institute*, lühidalt ETSI) tegeleb Euroopas sidealaste standardite väljatöötamisega. Tarbijakaitse ja Tehnilise Järelevalve Amet (edaspidi TTJA) on ETSI täisliige alates aastast 1998. ETSI standardid ja standardikavandid on tasuta saadaval internetist [ETSI Publications](#). ESS § 142 lõikest 2 tuleneb TTJA-le kohustus esitada elektroonilise side alase Euroopa standardiorganisatsiooni standardi Eesti standardiorganisatsioonile Eesti standardiks ülevõtmiseks.

Paragrahv 3¹ lõikega 2 sätestatakse, et peatükis kehtestatud nõudeid ei kohaldata ehitusseadustiku § 61² lõike 1 tähenduses sidevõrgu füüsilise taristu ega võrguelementide osas, mis ei ole võimelised signaale töötleva ega vaja toimimiseks energiat. Selline füüsiline taristu ja võrguelemendid ei kujuta ohtu riigi julgeolekule, mistõttu on need nõuete kohaldamisalast väljas.

Paragrahv 3² reguleerib riigi julgeolekut ohustava riist- ja tarkvara kasutamist sideteenuse osutamisel. **Paragrahv 3² lõikega 1** seatakse sideettevõtjale nõue, et sideteenuse osutamisel kasutatav riist- ja tarkvara ei tohi ohustada riigi julgeolekut. Mõiste „riigi julgeolek“ on sisustatud Riigikogu 2017. a kinnitatud julgeolekupoliitika alustes (edaspidi JPA)¹² ja Vabariigi

¹¹ HOS seletuskiri. Kättesaadav: <https://www.riigikogu.ee/tegevus/eelnoud/eelnou/6e396188-c9c2-4673-9fb6-ad324ec9a36c/Hädaolukorra%20seadus>.

¹² Eesti julgeolekupoliitika alused. Kättesaadav: https://www.riigikantslei.ee/sites/default/files/content-editors/Failid/2017.05.31_jpa_riigikogu.pdf.

Valitsuse poolt kinnitatud riigikaitse arengukavas 2017–2026 (edaspidi *RKAK*)¹³. JPA sätestab Eesti julgeolekupoliitika eesmärgina kindlustada Eesti riigi iseseisvus ja sõltumatus, rahva ja riigi kestmine, territoriaalne terviklikkus, põhiseaduslik kord ja elanikkonna turvalisus. RKAK määrab ühe olulise riigikaitse tegevussuunana riigi ja ühiskonna toimimise mistahes olukorras. See hõlmab elutähtsate teenuste või muude riigikaitse tähenduses oluliste teenuste toimepidevuse tagamist. Sideteenused kuuluvad elutähtsate teenuste hulka ning sidevõrkude rajamine on nendega vahetult seotud.

Laia riigikaitse seisukohast on seega oluline, et riigi ja ühiskonna harjumuspärasest toimimisest tagavate teenuste kasutatavus ei satuks võrguseadmete tarkvaravigade, võimalike tootja poolt tekitatud tehnoloogiliste „tagauste“ või nende vastu suunatud pahatahtlike rünnakute ja manipulatsioonide tõttu ohtu.¹⁴ Samuti on oluline tagada, et sidevõrgud ei oleks monokultuursed (ühe konkreetse tootja tehnoloogiaga üles ehitatud), mis tekitab sõltuvuse antud tootjast ning võimendab selle tootjaga seotud riske.

Määruses käsitletakse ohte riigi julgeolekule kahes grupis: 1) tootja, hooldus- või tugiteenuste pakkuja profiilist tulenevad ohud, mille tõttu on riist- ja tarkvara kasutamine sideteenuse kasutamisel kõrge riskiga (§ 3² lõiked 2-4) ning 2) muud põhjused, millal on riist- ja tarkvara kasutamine ohuks riigi julgeolekule (§ 3² lõige 5). Muud põhjused puudutavad eelkõige riist- ja tarkvara tehnilisi riske (näiteks riistvara turvaviga), mis ei ole seotud riist- või tarkvara tootja, hooldus- või tugiteenuste pakkuja profiiliga.

Paragrahv 3² lõikes 2 sätestatakse, et riigi julgeolekut ohustab kõrge riskiga riist- ja tarkvara kasutamine sideteenuse osutamisel.

Paragrahv 3² lõikes 3 on defineeritud, mis on sidevõrgu kõrge riskiga riist- ja tarkvara. Sidevõrgu kõrge riskiga riist- ja tarkvara on defineeritud riist- ja tarkvara tootja, hooldus- või tugiteenuste pakkuja kaudu. Kui riist- või tarkvara tootja või hooldus- või tugiteenuste pakkuja vastab vähemalt ühele lõikes 3 esitatud 8 punktist, on tegu kõrge riskiga riist- ja tarkvaraga.

Paragrahv 3² lõikes 3 nimetatakse 8 punkti, mis on sarnased Euroopa Liidu liikmesriikide ühises 5G võrkude turvalisuse meetmepaketis ning Ameerika Ühendriikide ja Eesti vastastikuse mõistmise memorandumis kokku lepitud punktidele. Punktid, mida hinnatakse on järgnevad: juriidiline asukoht või peakontor asub väljaspool Euroopa Liidu, Põhja-Atlandi Lepingu Organisatsiooni (NATO) või Majandusliku Koostöö ja Arengu Organisatsiooni (OECD) riike; asub riigis, kus ei kehti demokraatliku õigusriigi põhimõtted või ei austata inimõigusi; allub sõltumatu kohtuliku kontrollita välisriigi valitsusele või julgeolekuasutustele; majandustegevus ei põhine turupõhisel konkurentsil või selleks ei ole loodud tingimusi asukohariigis; asukohariigis ei ole loodud tingimusi intellektuaalomandi õiguste kaitsele; omanike, partnerite ja äriühingute juhtimisstruktuurid ei ole läbipaistvad; rahastamine ei ole läbipaistev ning ei järgi hangete, investeringute ja lepingute vallas parimaid tavasid; võib muul moel kujutada ohtu riigi julgeolekule.

Neid punkte kontrollivad julgeolekuasutused riist- ja tarkvara kasutusloa menetluses. Kasutusloa menetluses saab sideettevõtja kindluse, kas tema riist- või tarkvara on tootja, hooldus- või tugiteenuste pakkuja profiili tõttu kõrge riskiga või mitte. Nimetatud punktid on

¹³ Riigikaitse arengukava 2017–2026. Kättesaadav: https://www.riigikantselei.ee/sites/default/files/content-editors/Failid/rkak_2017_2026_avalik_osa.pdf.

¹⁴ Riigi julgeoleku hindamisest vt ka sisukokkuvõte.

indikaatoriks sideettevõtjale äripartnerite valikul ning võimaldavad täpsemalt mõista, mis aspekte julgeolekuasutused riigi julgeoleku ohu kindlakstegemisel kontrollivad.

Demokraatliku õigusriigi põhimõtte tähendab, et kehtivad sellised õiguse üldpõhimõtted, mida tunnustatakse Euroopa õigusruumis. Õigusriigi all on mõeldud õigusriiki laiemas tähenduses ehk mitte ainult riiki, kus on olemas seadused, vaid on olemas ka põhiõigused, võimude lahusus, sõltumatud kohtud ja seadusi järgiv haldus.¹⁵

Tarnijate riskiprofiili hindamise olulisust on rõhutatud mitmetes EL dokumentides ning ka Ameerika Ühendriikide ja Eesti vastastikuse mõistmise memorandumis 5G turvalisuse teemal¹⁶.

2019. aasta Euroopa Liidu riskianalüüsis toodi välja, et oluline on hinnata iga tehnoloogia tootja riskiprofiili. Muu hulgas tuleb riskianalüüsi kohaselt analüüsida ettevõtete sõltumatust Euroopa Liidu välistest riikidest, et välistada tehnoloogia kaudu poliitiliste huvide realiseerimist. Selleks on vaja arvesse võtta ettevõtte ja valitsuse seoseid, ettevõttele kohaldatavaid õigusakte (kas õigusaktid lähtuvad demokraatlikest printsiipidest ning andmekaitse põhimõtetest), ettevõtte juhtimise läbipaistvust ning kolmandate riikide võimet rakendada ettevõtte üle sunnimehhanisme. Riskianalüüsi olulisim sõnum on see, et IKT kasutamise puhul peab riskide hindamine olema kõikehõlmav, mitte ainult tehniliste aspektide keskne.

2020. aasta jaanuaris avaldatud 5G võrkude turvalisuse meetmepaketi kohaselt võib konkreetsete tarnijate riskiprofiile hinnata mitme teguri põhjal, mis on järgmised:

- tõenäosus, et tarnija tegevusse võib sekkuda ELi mittekuuluv riik. See on 5G-võrkudega seotud mittetehniliste nõrkuste hindamisel üks olulisemaid aspekte. Sellist sekkumist võib muu hulgas hõlbustada nende tegurite olemasolu:
 - tihe seos tarnija ja konkreetse kolmanda riigi valitsuse vahel;
 - kolmanda riigi õigusaktid, eriti kui riigis puudub seadusandlik ja demokraatlik kontrolli- ja tasakaalustussüsteem või kui ELi ja asjaomase riigi vahel ei ole sõlmitud turvalisust või andmekaitset käsitlevaid lepinguid;
 - tarnija ettevõtte omandistruktuur;
 - kolmanda riigi võimalus avaldada mis tahes vormis survet, sealhulgas seoses seadmete valmistamise kohaga;
- tarnija suutlikkus tarned tagada;
- tarnija toodete üldine kvaliteet ja küberturvalisuse tavad, sealhulgas see, mil määral kontrollitakse omaenese tarneahelat ja kas turvalisust peetakse piisavalt oluliseks.

Ameerika Ühendriikide ja Eesti vastastikuse mõistmise memorandumis 5G turvalisuse teemal on öeldud, et pakujate ja tarneahelate hindamine peaks sisaldama järgmisi elemente:

- tarnijad ei peaks alluma välisriikide valitsusele ilma sõltumatu kohtuliku kontrollita;
- rahastamine peaks olema läbipaistev, äripõhine ja järgima hangete, investeringute ja lepingute sõlmimise parimaid tavasid;
- omandiõigus, partnerlussuhted ja ettevõtte juhtimisstruktuurid peaksid olema läbipaistvad;

¹⁵ RKÜKo 12.07.2012, 3-4-1-6-12, p 131; RKPJKo 17.02.2003, 3-4-1-1-03, p 14. Vt ka Põhiseaduse § 10 kommentaare.

¹⁶ Kättesaadav: <https://ee.usembassy.gov/et/ameerika-uhendriikide-ja-eesti-vastastikuse-moistmise-memorandum-5g-turvalisuse-teemal/>

- pühendumus innovaatikale ja intellektuaalomandi õiguste austamine; ja
- peaksid tõendatult kinni õigusriigi põhimõtetest; turvalisest keskkonnast; hoiduksid müügieetika rikkumisest; ning järgiksid turvaliste standardite ja tööstuse parimaid tavasid, et edendada toodete ja teenuste elujõulist ja kindlat pakkumist.

Pidades silmas digiühiskonna arengut ning IKT arengu tõttu muutunud julgeolekuolukorda, on vajalik, et enne sidevõrkude jaoks vajaliku riist- ja tarkvara kasutusele võtmist tagatakse nende kooskõla riigi julgeoleku huvidega. Riigi julgeoleku huvidega kooskõla hindamisel kontrollitakse muu hulgas tarnijate riskiprofiile.

Paragrahv 3² lõikega 4 kehtestatakse keeld osutada sideteenust sidevõrgu kõrge riskiga riist- ja tarkvara vahendusel. Keeldu rakendatakse riist- ja tarkvara kasutusloa menetluse kaudu. Keelu rakendussätted sisalduvad §-is 8¹. Üldreeglina ei hõlma kõrge riskiga riist- ja tarkvara kasutamise keeld riist- ja tarkvara, mis on kasutusele võetud enne määruse jõustumist ehk 1. novembrit 2020. Erandiks on enne määruse jõustumist kasutusele võetud riist- ja tarkvara, millel on 5G NSA või uuema mobiilsidevõrgu standardi funktsioon.

Paragrahv 3² lõikega 5 sätestatakse, et sideteenuse osutamisel kasutatav riist- ja tarkvara võib ohustada riigi julgeolekut ka muul kui lõikes 2 kirjeldatud põhjusel. Tegemist on erinormiga lõike 2 suhtes.

Riist- ja tarkvara kasutamisest tulenevaid ohte riigi julgeolekule eristatakse seega kahes grupis: 1) tootja, hooldus- või tugiteenuste pakkuja profiilist tulenevad ohud, mille tõttu on riist- ja tarkvara kasutamine sideteenuse kasutamisel kõrge riskiga (üldnorm § 3² lõikes 2) ning 2) muud põhjused, millel on riist- ja tarkvara kasutamine ohuks riigi julgeolekule (§ 3² lõige 5). Muud põhjus on näiteks riist- ja tarkvara, mille tootja, hooldus- või tugiteenuse pakkuja ei ole profiili tõttu kõrge riskiga, kuid riistvaras peitub turvaviga, mistõttu on selle kasutamine ohtlik.

Paragrahv 3² lõikega 6 täpsustatakse, et riist- ja tarkvara ohtu riigi julgeolekule hinnatakse ja kasutamise keeldu rakendatakse riist- ja tarkvara kasutusloa menetluses. Kasutusloa menetluses hinnatakse kõrge riskiga riist ja tarkvara puhul vaid ohtu riigi julgeolekule. Kõrge riskiga riist- ja tarkvarale tingimuslikku kasutusluba anda ei saa. Kui kõrge riskiga riist- ja tarkvara kasutamine on lubatud, antakse sellele kasutusluba vastava tähtajani. Kui tegu on 5G NSA või uuema mobiilsidevõrgu standardi funktsiooniga kõrge riskiga riist- ja tarkvaraga, millel ei ole kriitilist funktsiooni, antakse kasutusluba 1. jaanuarini 2024. Kui tegu on kõrge riskiga riist- ja tarkvaraga, millel ei ole kriitilist funktsiooni ega 5G NSA või uuema mobiilsidevõrgu standardi funktsiooni, võib seda kasutada 1. jaanuarini 2030, ent korraga antakse kasutusluba kuni 8 aastaks. Muul juhul kõrge riskiga riist- ja tarkvarale kasutusluba ei anta.

Kui riist- või tarkvara kasutusloa menetluses leitakse, et riist- ja tarkvara võib ohustada riigi julgeolekut muul põhjusel kui tootja, hooldus- või tugiteenuste profiili tõttu, seatakse sellisele riist- või tarkvarale kasutusloas kasutamise tingimused või keeldutakse kasutusloa andmisest.

Kui ohtu riigi julgeolekule riist- või tarkvara kasutusloa menetluses ei tuvastata, antakse riist- või tarkvarale kasutusluba.

Paragrahv 3³ sätestab sideettevõtjale sidevõrgus kasutatavast riist- ja tarkvarast teavitamise kohustuse. **Paragrahv 3³ lõige 1** seab sideettevõtjale kohustada teavitada TTJA-d iga aasta enda sidevõrgus 1. jaanuari seisuga kasutatavast riist- ja tarkvarast. Teavitus tuleb esitada hiljemalt jooksva aasta 1. märtsiks. Teavitama ei pea § 3¹ lõikes 2 nimetatud füüsilisest taristust ega võrguelementidest (vt § 3¹ lõike 2 selgitusi). Teavituse vormi teeb Tarbijakaitse ja Tehnilise

Järelevalve Amet kättesaadavaks oma veebilehel. Selle lõikega sätestatud teavitamiskohustus ei ole sõltuvuses kasutusloa taotlemise kohustusest ehk see rakendub muu hulgas ka selle riist- ja tarkvara osas, mille kohta peab sideettevõtja loa taotlema. Teavitus on vajalik, et anda riigi julgeolekuasutustele ja RIA-le terviklik pilt olulistes sidevõrkudes toimuvast. Sidevõrk on baastaristu, millest sõltuvus ühiskonna digitaliseerumise kasvades tõuseb. Terviklik pilt sidevõrkudest võimaldab hinnata julgeolekuriske laiemalt.

Paragrahv 3³ lõige 2 nimetab teabe, mille peab sideettevõtja teavituskohustust täites esitama. Selleks on riist- ja tarkvara nimetus ja versiooni number; kogus; tootja; omanik; kasutusõiguse lepingu osapooled ja kehtivusaeg, kui riist- ja tarkvara omanik ei ole sideettevõtja; funktsioon sidevõrgus; füüsilise asukoha aadress, mille võib esitada riigi, haldusüksuse, asustusüksuse, aadressiobjekti või muu piirkondliku täpsusega; kasutamise algusaasta ja prognoositav lõpuaasta; kui tegemist on mobiilsidevõrgus kasutatava riist- või tarkvaraga, siis millise mobiilsidevõrgu põlvkonna jaoks riist- või tarkvara töötab.

Tootja on ettevõtte või isik, kes on riist- või tarkvara tootnud.

Kasutuslepingud on võlaõigusseaduse 3. osas sätestatud lepingud, näiteks tasuta kasutamise, üüri-, rendi-, litsentsi-, liisingu- ja laenulepingud. Kõik need on § 3² lõikega 2 punktiga 5 hõlmatud.

Riist- või tarkvara funktsioon on selle konkreetne ülesanne, mida see riist- või tarkvara täidab või peaks täitma. Näiteks: BGP marsruuter, rakendus (ISO/OSI L7) tulemüür, võrgu sissetungi tuvastus (IDS) sensor, IP võrguliikluse peegeldaja jne. Riist- või tarkvaral võib lisaks peamisele ülesandele olla ka teisene ülesanne, näiteks marsruuter võib samaaegselt olla ka sensor, raadiovõrgu pääsupunkt võib samaaegselt olla ka marsruuter jne.

Füüsilise asukoha aadressi võib esitada riigi, haldusüksuse, asustusüksuse, aadressiobjekti või muu piirkondliku täpsusega. Riigi all on mõeldud „Eesti“. Haldusüksus ja asustusüksus on defineeritud Eesti territooriumi haldusjaotuse seaduses (edaspidi *ETHS*). *ETHS* § 2¹ lõige 2 kohaselt on haldusüksus haldusjaotusel põhinev, seaduse ja teiste õigusaktidega kindlaks määratud nime, liigi ja piiridega üksus, mille territooriumi ulatuses teostatakse riiklikku või omavalitsuslikku haldamist. Haldusüksuste nimistu kinnitab ja selles teeb muudatusi Vabariigi Valitsus. Haldusüksuste nimistu on leitav Vabariigi Valituse määrusest „Eesti territooriumi haldusüksuste nimistu kinnitamine“¹⁷. Haldusüksused on maakonnad, vallad ja linnad nagu näiteks Järva maakond, Häädemeeste ja Rakvere. Vald ja linn jagunevad asustusüksusteks. Asustusüksused on asulad, milleks on linnad, külad, alevikud ja alevid.¹⁸ Aadressiobjekt on maaga seotud objekt, millele on määratud aadress või millele aadressi määramise kohustus või võimalus tuleneb õigusaktist.¹⁹ Muu piirkondliku täpsuse all on võimalik ettevõtjal piiritleda asukoht näiteks geograafilise regioonina Põhja-Eesti. Tarkvara puhul on võimalik määrata füüsiline asukoht riistvara kaudu, milles seda tarkvara kasutatakse.

Mobiilsidevõrgu põlvkonnad ehk generatsioonid (G) on näiteks 3G, 4G, 5G. Täpsemalt vt § 3¹ lõike 1 selgitustest.

¹⁷ Eesti territooriumi haldusüksuste nimistu kinnitamine. RT I, 11.11.2017, 1

¹⁸ *ETHS* § 6 lõiked 1-2

¹⁹ Ruumiandmete seadus § 40 lõige 2. RT I, 13.03.2019, 152

Paragrahv 3³ lõige 3 sätestab, et lisaks § 3⁴ lõikes 2 nimetatule esitab sideettevõtja teavituses teabe kellel on peale sideettevõtja administreerimisligipääs sidevõrgu haldusvõrgule ja millised on ligipääsu tingimused isikute lõikes ning sidevõrgu riist- ja tarkvara hooldus- ja tugiteenuste osutajad. Nende punktide puhul küsitakse informatsiooni sidevõrgu üleselt ning seda ei pea esitama riist- ja tarkvara täpsusega.

Haldusvõrgu all mõeldakse sidevõrgu haldusvõrgu määratlust ITU-T soovitusel M.3010 alusel.²⁰ Sellest lähtuvad nii ETSI standardid kui ka 3GPP standardid, sh kõige uuemad neist. Haldusvõrgu ingliskeelne määratlus on järgnev: „3.30 *telecommunications management network: An architecture for management, including planning, provisioning, installation, maintenance, operation and administration of telecommunications equipment, networks and services.*“

Administreerimisligipääs hõlmab näiteks võimalust riist- või tarkvara seadistada ja ümber konfigureerida. Hooldus- ja tugiteenuse osutajad on ettevõtted või isikud, kes pakuvad sideettevõtjale sidevõrgu riist- ja tarkvara hooldamise või tugiteenuseid või mõlemat.

Paragrahv 3³ lõige 4 sätestab, et TTJA registreerib § 3³ lõikes 1 saadud sideettevõtja teavituse ning edastab selle teadmiseks julgeolekuasutustele ja Riigi Infosüsteemi Ametile. Teavituse edastamine on vajalik, kuna julgeolekuasutustel ja Riigi Infosüsteemi Ametil on vajalik olla kursis riigi julgeoleku aspektist olulistest sidevõrkudes toimuvaga (vt ka § 3³ lõige 1 selgitus).

Paragrahviga 3⁴ seatakse sideettevõtjatele sidevõrgu riist- ja tarkvara kasutusloa taotlemise kohustus. **Paragrahv 3⁴ lõikega 1** seatakse sideettevõtjale kohustus esitada TTJA-le enne riist- või tarkvara plaanitavat kasutusele võtmist riist- või tarkvara kasutusloa taotlus. Taotluse vormi teeb Tarbijakaitse ja Tehnilise Järelevalve Amet kättesaadavaks oma veebilehel.

Riistvara või tarkvara kasutusele võtmine on ka riistvara väljavahetamine ning tarkvara uuendamine. Sellisel juhul tuleb esitada kasutusloa taotlus, välja arvatud erandjuhul, mis on sätestatud sama paragrahvi lõikes 4.

Üldreegli kohaselt peab sideettevõtja 1. novembrist 2020 esitama kasutusloa taotluse enne seda, kui ta riist- või tarkvara kasutusele võtab. Määruses ei ole sätestatud täpset aega, kui palju enne planeeritavat kasutusele võtmist sideettevõtja taotluse esitama peab. Oluline on, et sideettevõtja arvestaks kasutusloa taotlemisel ajaga, mis kulub selle menetlemiseks (vt §-id 3⁵ ja 3⁶).

Üldreeglile²¹ on kolm erisust. Esiteks hõlmab kasutusloa kohustus riist- ja tarkvara, mis on kasutusele võetud enne 1. novembrit 2020 ja milles võetakse 5G *non-standalone* (edaspidi 5G NSA) või uuema mobiilsidevõrgu standardi funktsioon kasutusele pärast 1. novembrit 2020. Sellise riist- ja tarkvara kasutusloa taotlus tuleb esitada enne plaanitavat funktsiooni kasutusele võttu. Teiseks, kui tegu on vahemikus 1. november 2020 kuni 1. jaanuar 2029 kasutusele võetava riist- ja tarkvaraga, millel ei ole kriitilist funktsiooni ega 5G NSA või uuema mobiilsidevõrgu standardi funktsiooni, tuleb esitada kasutusloa taotlus hiljemalt 1. juuliks 2029. Kolmandaks, kui riist- või tarkvara on tarvis viivitamata paigaldada küberintsidendi

²⁰ ITU-T Recommendation M.3010 „Principles for a telecommunications management Network“. Kättesaadav ITU kodulehel: <https://www.itu.int/itu-t/recommendations/rec.aspx?rec=4869>

²¹ Üldreegli all on mõeldud eelmainitud reeglit, et taotlus tuleb esitada enne riist- ja tarkvara kasutusele võtmist.

kõrvaldamiseks või selle vahetuks ärahoidmiseks, esitab sideettevõtja kasutusloa taotluse hiljemalt kümnendal tööpäeval pärast riist- või tarkvara paigaldamist.

Kuna sideettevõtja suhtleb juba praegu sideturu reguleerimise ja sageduslubade teemal TTJA-ga, siis on loogiline, et ka sel teemal suhtleb sideettevõtja TTJA-ga, mitte kolme erineva ameti ja küberjulgeoleku nõukoguga. Seetõttu tuleb taotlus esitada TTJA-le.

Paragrahv 3⁴ lõige 2 seab sideettevõtjale kohustuse esitada kasutusloa taotlus sidevõrgu riist- või tarkvara kasutamise lubamiseks hiljemalt kümnendal tööpäeval pärast selle paigaldamist, kui riist- või tarkvara on tarvis viivitamata paigaldada küberintsidendi kõrvaldamiseks või vahetuks ärahoidmiseks. Küberintsidendi all on mõeldud küberturvalisuse seadusega²² defineeritult süsteemis toimuvat sündmust, mis ohustab või kahjustab süsteemi turvalisust.

Paragrahv 3⁴ lõikega 3 kehtestatakse loetelu teabest, mille sideettevõtja peab kasutusloa taotluses esitama. Taotluses peab riist- või tarkvara kohta esitama selle nimetuse ja versiooni numbri; koguse; tootja; omaniku; kasutusõiguse lepingu osapooled ja kehtivusaja, kui riist- ja tarkvara omanik ei ole sideettevõtja; riist- ja tarkvara hooldus- ja tugiteenuste osutaja, kui see pole omanik ega kasutusõiguse omaja; füüsilise asukoha aadressi, mille võib esitada riigi, haldusüksuse, asustusüksuse, aadressiobjekti või muu piirkondliku täpsusega; kasutamise algusaasta ja prognoositav lõpuaasta; kui tegemist on mobiilsidevõrgus kasutatava riist- või tarkvaraga, siis millise mobiilsidevõrgu põlvkonna jaoks riist- või tarkvara töötab; info, kellel on lisaks sideettevõtjale administreerimisligipääs riist- või tarkvarale ning ligipääsu tingimused isikute lõikes. Viimane info peab hõlmama kõiki sideettevõtjale endale Eestis või väljastpoolt Eestit administreerimisligipääsu omavaid isikuid.

Esitatav informatsioon peab olema täielik ehk näiteks, kui on küsitud riist- ja tarkvara hooldus- ja tugiteenuste osutaja, kui tegemist pole omaniku ega kasutusõiguse omajaga, tuleb esitada kõik sellele tingimusele vastavad hooldus- ja tugiteenuste osutajad, kui neid on rohkem kui üks.

Tootja, kasutusõiguse, füüsilise asukoha aadressi, raadiovõrgu ja raadiovõrgu generatsiooni ning administreerimisligipääsu defineerimise kohta vt § 3³ lõigete 2-3 selgitusi.

Asukoha täpsuse saab sideettevõtja ise määratlada olenevalt sellest, kus riist- või tarkvara kasutatakse. Asukoha kirjeldamisel eeldatakse riigi julgeoleku aspektist kõige riskantsemat piirkonda. Seega, kui sideettevõtja kirjeldab füüsilise asukoha riigi täpsusega (Eesti), siis eeldatakse, et seda riist- või tarkvara kasutatakse potentsiaalselt ükskõik kus Eestis. Kui sideettevõtja määratleb füüsilise asukohana näiteks Rapla, siis tähendab see, et ta kasutaks seda riist- või tarkvara ainult Raplas ning sellest lähtutakse ka riigi julgeoleku riskide hindamisel.

Paragrahv 3⁴ lõige 4 sätestab kasutusloa kohustusele erandi. Sideettevõtja lõikes 1 sätestatud kasutusluba taotlemata vahetada välja riistvara ja võtta kasutusele tarkvara uuendused, mille puhul muutub kasutusloas kinnitatud nimetus või versiooni number, eeldusel, et lõikes 2 nimetatud andmed, mille on riist- ja tarkvarale antud kasutusloas kinnitanud Tarbijakaitse ja Tehnilise Järelevalve Amet jäävad samaks.

Erand rakendub ehk uut kasutusluba ei pea taotlema, kui täidetud on kõik järgmised tingimused: 1) riist- või tarkvarale rakenduks ilma selle erandita kasutusloa taotlemise kohustus; 2) tegemist on riistvara väljavahetamise või tarkvara uuendamisega; 3) väljavahetatava riistvara või uuendatava tarkvara osas on kasutusluba olemas; 4) väljavahetamisel või uuendamisel muutub

²² Küberturvalisuse seadus. RT I, 22.05.2018, 1. § 2 p 3.

ainult riist- ja tarkvara nimetus, versiooni number või mõlemad; 5) muud andmed, mille on riist- ja tarkvarale antud kasutusloas kinnitanud Tarbijakaitse ja Tehnilise Järelevalve Amet, jäävad samaks. Erand on loodud selleks, et vältida tarbetut bürokraatiat olukorras, kus risk riigi julgeolekule on minimaalne. Erandi kasutamisel jätkub uuele riist- ja tarkvarale kasutusloa tähtaeg, mis on antud vanale riist- ja tarkvarale (vt § 3⁷ lõige 2).

Paragrahv 3⁴ lõige 5 puudutab uue kasutusloa taotlemist pärast kasutusloa lõppemist. Lõikega sätestatakse, et kui kasutusloa taotluses esitatud riist- või tarkvara andmed on jäänud samaks, võib uue kasutusloa taotluse esitada viitega esialgsele taotlusele koos kinnitusega andmete samaks jäämise kohta. Kui riist- või tarkvara andmed on muutunud, esitatakse uuel taotlusel andmed vastavalt § 3⁴ lõikes 3 sätestatule. Lõige on loodud selleks, et vähendada bürokraatiat olukorras, kus ettevõtja on samad andmed riigile juba esitanud ning vahepeal midagi andmetes muutunud ei ole.

Paragrahvid 3⁵ ja 3⁶ sätestavad kasutusloa taotluse menetlemise ja kooskõlastamise korra, sh tähtajad. Nende paragrahvide järgi on menetluse protsess lihtsustatult järgnev:

- 1) Sideettevõtja saadab taotluse TTJA-le;
- 2) TTJA küsib arvamust Välisluureametilt (VLA), Kaitsepolitseiametilt (KAPO) ja Riigi Infosüsteemi Ametilt (RIA);
- 3) VLA, KAPO ja RIA hindavad riske ja edastavad arvamuse;
- 4) Kui arvamused on positiivsed, annab TTJA haldusaktiga riist- või tarkvarale kasutusloa;
- 5) Kui vähemalt üks arvamustest on negatiivne,
 - a. annab TTJA ettevõtjale arvamuse ja vastuväidete esitamise võimaluse, sh keelu ja tingimuste seadmise mõju kohta,
 - b. ning TTJA saadab taotluse küberjulgeoleku nõukogule;
- 6) Küberjulgeoleku nõukogu kaalutleb riigi julgeoleku aspekti, mõju side toimepidevusele, sideturule ja konkurentsile ning kooskõlastab / seab tingimused / ei kooskõlasta. Samuti annab küberjulgeoleku nõukogu hinnangu kasutusloa tähtajale ehk hindab, kui pikaks ajaks peaks kasutusloa andma.
- 7) TTJA annab haldusakti ning teavitab sellest sideettevõtjat. TTJA haldusakt võib olla taotluse rahuldamine, rahuldamine tingimuslikult või rahuldamata jätmine. Kui tegemist on kõrge riskiga riist- või tarkvaraga, ei saa kasutusloas tingimusi seada, ning on võimalik vaid kasutusloa väljastamine või sellest keeldumine.

Paragrahv 3⁵ lõike 1 kohaselt registreerib TTJA kasutusloa taotluse ja edastab selle viie tööpäeva jooksul arvamuse andmiseks julgeolekuasutustele ja Riigi Infosüsteemi Ametile (RIA). Julgeolekuasutused on julgeolekuasutuste seaduse mõistes Kaitsepolitseiamet (KAPO) ja Välisluureamet (VLA). Julgeolekuasutuste ja RIA arvamust tuleb küsida, kuna TTJA-l puudub nii riigi julgeoleku kui ka küberturvalisuse hindamise pädevus. Seetõttu edastab TTJA sideettevõtja sidevõrgu riist- ja tarkvara taotluse, sh tehnilise dokumentatsiooni, riigi julgeoleku huvidele vastamise kontrollimiseks riigi julgeolekuasutustele ja RIA-le.

Kui ettevõtja taotlus on puudustega, kohaldub haldusmenetluse seadus (edaspidi *HMS*) § 15, mille lõike 2 sätestab, et kui isik jätab koos taotlusega esitamata nõutud andmed või dokumendid või kui taotluses on muid puudusi, määrab haldusorgan taotluse esitajale esimesel võimalusel tähtaja puuduste kõrvaldamiseks, selgitades, et tähtpäevaks puuduste kõrvaldamata jätmisel võib haldusorgan jätta taotluse läbi vaatamata.

Paragrahv 3⁵ lõike 2 kohaselt, kui julgeolekuasutus või Riigi Infosüsteemi Amet leiab, et kasutusloa taotluses nimetatud sidevõrgu riist- või tarkvara on kõrge riskiga riist- või tarkvara või selle kasutamine võib ohustada riigi julgeolekut muul põhjusel, esitab ta oma seadusest tulenevate ülesannete täitmisel kogutud ja töödeldud teabe põhjal kahekümne tööpäeva jooksul põhjendatud arvamuse kasutusloa taotluse kohta. Kui tegemist ei ole kõrge riskiga riist- ja tarkvaraga, vaid see võib ohustada riigi julgeolekut muul põhjusel, esitatakse arvamuses põhjendatud ettepanek vastav riist- või tarkvara kasutamine keelata või seada selle kasutamisele tingimused. Kui vähemalt üks nimetatud asutustest leiab, et on oht riigi julgeolekule, siis kohalduvad §-le 3⁵ järgnevad lõiked ehk kohaldub § 3⁵ lõigetes 3-7 sätestatud menetlus.

Julgeolekuasutuste teabe kogumise ülesanded, milleks on ette nähtud ka ressurss, tulenevad julgeolekuasutuste seaduse (edaspidi *JAS*)²³ §-dest 6 ja 7 ning § 9 alusel VV korraldusega kehtestatud riigi julgeolekuteabe hanke ja analüüsi kavast. Arvamuse andmisel lähtuvad julgeolekuasutused seega olemasolevast teabest.

Paragrahv 3⁵ lõike 3 kohaselt, kui julgeolekuasutus või RIA leidis arvamuses, et taotluses nimetatud riist- või tarkvara võib ohustada riigi julgeolekut, annab TTJA pärast lõikes 2 nimetatud arvamuse andmise tähtaega sideettevõtjale võimaluse esitada kahekümne tööpäeva jooksul vastuväited ja aramus, kuidas mõjutab taotluse rahuldamata jätmine või tingimuste seadmine sideteenuse osutamist.

Paragrahv 3⁵ lõike 4 kohaselt esitab TTJA pärast lõikes 3 nimetatud arvamuse andmise tähtaega esitab sideettevõtja taotluse koos lõigetes 2 ja 3 nimetatud arvamustega kooskõlastamiseks küberjulgeoleku nõukogule.

Paragrahv 3⁶ lõike 5 kohaselt hindab küberjulgeoleku nõukogu, kas kasutusloa taotluses nimetatud sidevõrgu riist- või tarkvara on kõrge riskiga riist- või tarkvara või kas selle kasutamine võib ohustada riigi julgeolekut muul põhjusel. Kui riist- või tarkvara võib ohustada riigi julgeolekut muul põhjusel, hindab küberjulgeoleku nõukogu, millistel tingimustel on riist- või tarkvara võimalik kasutada, ning kaalub riist- või tarkvara kasutamise keelamise ja tingimuste seadmise mõju side toimepidevusele, sideturule ja konkurentsile ning annab hinnangu kasutusloa tähtaja kohta.

Küberjulgeoleku nõukogu hindab riist- ja tarkvara kasutamisest tulenevat ohtu riigi julgeolekule eelkõige julgeolekuasutustelt ning RIA-lt saadud arvamuste põhjal. Seejuures pole küberjulgeoleku nõukogu julgeolekuasutuste ega RIA arvamustega seotud, vaid teeb otsuse kaaludes nii julgeolekuasutuste ja RIA arvamusi kui ka muid aspekte nagu näiteks ettevõtja vastuväited.

Kui tegemist ei ole küberjulgeoleku nõukogu hinnangul kõrge riskiga riist- ja tarkvaraga, vaid see võib ohustada riigi julgeolekut muul põhjusel, kaalutleb küberjulgeoleku nõukogu olukordi, kus riigi julgeoleku huvid, majanduslikud huvid, sideteenuse toimepidevuse tagamine ning muud võimalikud huvid on vastuolulised. Näiteks võib tekkida olukord, kus teatud riist- ja tarkvara kasutamine ei ole julgeolekuasutuste koostatud riskihinnangu järgi turvaline, kuid seda riist- või tarkvara ei ole võimalik sideteenuse toimepidevuse tagamiseks kiiresti välja vahetada.

²³ Julgeolekuasutuste seadus. RT I, 26.05.2020, 10.

Selline olukord nõuab kaalutlemist ning parima võimaliku lahenduse väljatöötamist. TTJA pöördub küberjulgeoleku nõukogu poole kaalutletud ja tasakaalustatud seisukoha küsimiseks.

Kõrge riskiga riist- ja tarkvara tuvastamisel on võimalik määruse kohaselt kasutusloa väljastamine või sellest keeldumine. Tingimuslikku kasutusluba anda pole võimalik. Samuti seab määrus ette, millal peab võib kõrge riskiga riist- ja tarkvara kasutada ja millal ei või. Sellest tuleb lähtuda ka kasutusloa taotluse menetlemisel. Üldreeglina, kui kasutusloa menetluses tuvastatakse, et tegu on kõrge riskiga riist- ja tarkvaraga, ei anta sellele kasutusluba. Kasutusluba antakse teatud tähtajani vaid kahel juhul. Esiteks, kui tegu on 5G NSA või uuema mobiilsidevõrgu standardi funktsiooniga kõrge riskiga riist- ja tarkvaraga, millel ei ole kriitilist funktsiooni, antakse kasutusluba 1. jaanuarini 2024. Teiseks, kui tegu on kõrge riskiga riist- ja tarkvaraga, millel ei ole kriitilist funktsiooni ega 5G NSA või uuema mobiilsidevõrgu standardi funktsiooni, võib seda kasutada 1. jaanuarini 2030, ent korraga antakse kasutusluba kuni 8 aastaks.

Paragrahv 3⁵ lõike 6 kohaselt kooskõlastab küberjulgeoleku nõukogu taotluse või jätab selle põhjendatult kooskõlastamata kolmekümne tööpäeva jooksul pärast § 3⁵ lõikes 4 nimetatud materjalide saamist. Vajadusel võib küberjulgeoleku nõukogu pikendada kooskõlastamise tähtaega kuni viieteistkümne tööpäeva võrra, teavitades sellest Tarbijakaitse ja Tehnilise Järelevalve Ametit.

Paragrahv 3⁵ lõige 7 annab küberjulgeoleku nõukogule võimaluse otsustada tingimusliku kooskõlastuse andmine ning määrata tingimused, mille täitmisel võib riist- ja tarkvara kasutada, kui tegemist on § 3² lõikes 5 nimetatud riist- või tarkvaraga ehk kui riist- või tarkvara ei ole kõrge riskiga riist- või tarkvara, vaid võib ohustada riigi julgeolekut muul põhjusel. Kõrge riskiga riist- ja tarkvarale tingimuslikku kasutusluba väljastada ei saa.

Paragrahv 3⁶ lõike 1 kohaselt otsustab TTJA sideettevõtja taotluse rahuldamise ja kasutusloa väljastamise kolmekümne tööpäeva jooksul pärast selle saamist, kui taotluse suhtes ei ole tarvis läbi viia § 3⁵ lõigetes 3–7 sätestatud menetlust. Paragrahv 3⁵ lõigetes 3–7 kirjeldatud menetlust ei ole vaja läbi viia juhul, kui ükski julgeolekuasutustest ega RIA ei leia, et riist- või tarkvara kujutaks ohtu riigi julgeolekule. Kui üks julgeolekuasutustest või RIA leiab, et on oht riigi julgeolekule, esitab ta TTJA-le § 3⁵ lõikes 2 nimetatud põhjendatud arvamuse ning sellega tekib kohustus läbida § 3⁵ lõigetes 3–7 kirjeldatud menetlus.

Paragrahv 3⁶ lõige 2 sätestab, et kui sideettevõtja taotluse suhtes on tarvis läbi viia § 3⁵ lõigetes 3–7 sätestatud menetlus (mis rakendub siis, kui üks julgeolekuasutustest või RIA näeb ohtu riigi julgeolekule), otsustab TTJA viieteistkümne tööpäeva jooksul pärast § 3⁵ lõikes 6 nimetatud kooskõlastuse saamist sideettevõtja taotluse rahuldamise või rahuldamata jätmise ning kasutusloa väljastamise.

Paragrahv 3⁶ lõike 3 kohaselt taotlus rahuldatakse ja kasutusluba väljastatakse, kui kasutusloa taotluses nimetatud riist- või tarkvara puhul pole alust arvata, et see võib ohustada riigi julgeolekut.

Paragrahv 3⁶ lõike 4 kohaselt ei anta kõrge riskiga riist- ja tarkvarale kasutusluba. Paragrahvi 3² lõikes 5 nimetatud riist- või tarkvarale ei anta kasutusluba või antakse tingimuslik

kasutusluba. Paragrahvi 3² lõikes 5 nimetatud riist- või tarkvara ei ole kõrge riskiga riist- ja tarkvara § 3² lõike 3 definitsiooni kohaselt, kuid võib ohustada riigi julgeolekut muul põhjusel.

TTJA otsus on haldusakt, mida on võimalik vaidlustada halduskohtus. Kohaldub HMS-is haldusakti kohta sätestatu. Näiteks võib TTJA teatud tingimustel haldusakti edasiulatuvalt kehtetuks tunnistada, kui muutuvad haldusakti andmisel aluseks olnud faktilised asjaolud või haldusaktiga seatud tingimusi ei täideta (vt HMS § 66 lõige 2).

TTJA haldusaktis tehtud otsuses on hõlmatud kõik § 3⁴ lg 2 elemendid. Kui ettevõtte soovib muuta näiteks kasutusloaga riist- või tarkvara füüsilist asukohta või hooldusteenuse pakkujat, peab vormistama ka loa muudatuse ja läbima selleks loamenetluse.

Paragrahv 3⁷ sätestab kasutusloa tähtaja. **Paragrahv 3⁸ lõike 1** kohaselt antakse kasutusluba kuni kaheksaks aastaks. Selline norm eksisteerib ka näiteks Prantsuse õiguses²⁴. Kasutusloal on kehtivustähtaeg, kuna aja möödudes võib olukord riigi julgeoleku vaatest muutuda ning võib olla vajalik teha esialgsest erinev otsus.

Paragrahv 3⁷ lõike 2 kohaselt jätkub riistvara väljavahetamisel või tarkvara uuendamisel § 3⁴ lõikes 4 nimetatud juhul uue riist- ja tarkvara kohta väljavahetatud riistvarale või uuendatud tarkvarale varem antud kasutusloa tähtaeg. Kasutusloa tähtaja lõppemisel tuleb kasutuse jätkamiseks taotleda kasutusloa pikendamist. Näiteks kui seadmele on antud luba kehtivusega 8 aastat ning ettevõtja vahetab selle seadme § 3⁴ lõike 4 erandi alusel 7 aasta pärast välja, siis kehtib uuele seadmele luba veel 1 aasta.

Eelnõu § 1 punktiga 3 täiendatakse VV määrust nr 140 §-idega 8¹ ja 8². Tegemist on rakendussätetega. Paragrahv 8¹ puudutab § 3² lõikes 4 sätestatud kõrge riskiga riist- ja tarkvara keelu rakendamist ning § 8² kasutusloa taotlemise kohustuse rakendamist.

Keeld osutada sideteenust kasutades riist- ja tarkvara, mis ohustab riigi julgeolekut, sealhulgas põhjusel, et tegu on kõrge riskiga riist- ja tarkvaraga, rakendub määruse jõustumisel. Samuti rakendub määruse jõustumisel kasutusloa taotlemise kohustus. Rakendussätetega täpsustatakse keelu ja kasutusloa taotlemise kohustuse rakendamist. Seejuures on oluline meeles pidada, et ohtu riigi julgeolekule hinnatakse ning keeldu rakendatakse kasutusloa menetluses.

Nii kõrge riskiga riist- ja tarkvara keelu kui ka kasutusloa taotluse kohustuse rakendamisel on arvestatud tehnoloogiliste riskide maandamist, side toimepidevust, halduskoormust, põhiõiguste riivet, mõju konkurentsile ja sideturule ning kooskõla EL ja NATO liitlaste poliitikaga.

Paragrahvis 8¹ täpsustatakse kõrge riskiga riist- ja tarkvara kasutamise keelu rakendamist.

Paragrahv 8¹ lõike 1 kohaselt ei hõlma § 3² lõikes 4 sätestatud kõrge riskiga riist- ja tarkvara kasutamise keeld riist- ja tarkvara, mis on kasutusele võetud enne 1. novembrit 2020, välja arvatud juhul, kui sellel on 5G NSA või uuema mobiilsidevõrgu standardi funktsioon. Seega

²⁴ 1. augustil 2019 vastu võetud Prantsuse [seadus nr 2019-810](#), mille eesmärk on kaitsta kaitse- ja riiklikke julgeolekuhuve 5G mobiilsidevõrkude kontekstis.

kõik kõrge riskiga riist- ja tarkvara keeluga hõlmatud riist- ja tarkvara on hõlmatud ka kasutusloa kohustusega.

Paragrahv 8¹ lõike 2 kohaselt võib kõrge riskiga 5G NSA või uuema mobiilsidevõrgu standardi funktsiooniga riist- ja tarkvara, millel ei ole kriitilist funktsiooni, kasutada § 3⁴ lõikes 1 nimetatud loa alusel 1. jaanuarini 2024. Kui sellise kõrge riskiga riist- ja tarkvara kohta esitatakse enne 1. jaanuari 2024 kasutusloa taotlus, siis see rahuldatakse ning antakse kasutusluba tähtajani 1. jaanuar 2024. Sel viisil saab sideettevõtja kasutusloa menetluses teada, kas tema riist- või tarkvara on kõrge riskiga ning samas jääb talle üleminekuaeg, et oma tegevuses arvestada, et 1. jaanuarist 2024 ta seda riist- ja tarkvara enam kasutada ei saa.

Paragrahv 8¹ lõike 3 kohaselt võib kõrge riskiga riist- ja tarkvara, millel ei ole kriitilist funktsiooni ega 5G NSA või uuema mobiilsidevõrgu standardi funktsiooni, kasutada § 3⁴ lõikes 1 nimetatud loa alusel 1. jaanuarini 2030. Sarnaselt eelneval lõikega kehtib loogika, et kui sellise kõrge riskiga riist- ja tarkvara kohta esitatakse enne 1. jaanuari 2030 kasutusloa taotlus, siis see rahuldatakse ning antakse kasutusluba tähtajani 1. jaanuar 2030.

Kõrge riskiga riist- ja tarkvara keelu rakendamise puhul on arvestatud nii riigi kui ka ettevõtja huvidega. Kriitiliste funktsioonide puhul erandit ei ole ehk määruse jõustumist on kriitilise funktsiooniga riist- ja tarkvara kasutamise osas keeld. Ülejäänud riist- ja tarkvara puhul on ettevõtjal rohkem aega. 5G NSA või uuema mobiilsidevõrgu standardi funktsiooniga kõrge riskiga riist- ja tarkvara puhul on ettevõtjal üleminekuaeg 1. jaanuarini 2024 ning muu riist- ja tarkvara osas 1. jaanuarini 2030. Üleminekuaeg on vajalik, et kahju sideettevõtjale oleks võimalikult minimaalne. Samas on arvestatud ka riigi julgeoleku huvidega – arvestades 5G kõrgemat kriitilisust, on sellele üleminekuaeg lühem.

Paragrahv 8¹ lõige 4 defineerib riist- ja tarkvara kriitilised funktsioonid, mis on järgnevad:

- 1) Euroopa Telekommunikatsiooni Standardite Instituudi standardite kohaselt tuumikvõrgu funktsioon,
- 2) funktsioon, mille kaudu või mille häirimisel on võimalik mõjutada vähemalt 1000 lõppkasutajat või teise sideettevõtja sidevõrku, või
- 3) funktsioon, mille eesmärk on võimaldada jälitustoimingu teostamist või sõnumi saladuse õiguse piiramist.

Tuumikvõrgu funktsioonideks loetakse määruse kohaselt sellised ETSI standardite kohased funktsioonid, mis on olulised võrgu juhtimise, töö korraldamise, võrgust väljuva informatsiooni- ja andmevahetuse, regulatsioonidest tulenevate nõuete täitmise, kliendiandmete konfidentsiaalsuse või võrgu käideldavuse tagamiseks.

Tuumikvõrgu funktsioonid on ETSI standardite kohaselt juuli 2020 seisuga:

1. Püsi- ja mobiilivõrkude ühisosa:

1.1. Tuumikvõrgu lülituskiht (marsruutimine ja kommuteerimine)

1.1.1. Tuumikvõrgu marsruuterid (*Backbone*, BB) – erinevate alamvõrkude liiklust üle vabariigi IP tasemel marsruutiv kõrgkäideldav võrk

1.1.2. Agregeerivate võrkude marsruuterid (*Aggregation Routers*, MGW) – piirkondlikku võrguliiklust IP tasemel marsruutiv kõrgkäideldav võrk

- 1.1.3. Teiste sidevõrkudega liidestuvad ruuterid (*Edge Routers*, BNG)-
- 1.2. Tuumikvõrgu teenuste kiht
 - 1.2.1. Teenusruuterid (*Service Routers*, SR) - kliendiühenduse IP taseme, kliendiühenduse reguleerimise ning pääsureeglite kehtestamise funktsionaalsus. Siin määratakse vastavalt andmebaasides sisalduvale infole kliendiühenduste alla/üleslaadimise kiirused ja teenuseprofiilidega määratud piirangud ja kvaliteediparameetrid
 - 1.2.2. Võrguteenused, teenuste haldus, näiteks võrguga ühendatud abonentide kiiruse piiramine, pakettide filtreerimine ja liikluse prioriteetide seadmine (sh autentimis- ja autoriseerimissüsteemid (AAA), *Radius*)
 - 1.2.3. Tulemüürid, kaitse teenustõkke rünnakute (DDoS) vastu, võrgu turbeseadmed ja teenused
 - 1.2.4. Sidevõrgu tööd toetavad süsteemid ja teenused - DHCP, DNS, NTP, PTP
 - 1.2.5. Sidevõrgus tuumikvõrgu tööd juhtiv ja korraldav süsteem OSS (*Operational Support System*)
 - 1.2.6. IMS – Kõneside. *IP Multimedia subsystem*
- 1.3. Tuumikvõrgu teenuste osutamiseks vajalik infrastruktuuri kiht
 - 1.3.1. Teenuste hulgitootmist võimaldavad virtualiseerimiskeskonnad tarkvara ja serveritega (NFVI)
- 1.4. Tuumikvõrgu halduskiht (võrgujuhtimissüsteemid)
 - 1.4.1. Teenuste ja võrgu seiresüsteemid
 - 1.4.2. OOB - out of band management
 - 1.4.3. Teenuste ja seadmete provisioneerimissüsteemid (*Network Activation Systems*)

2. 4G tuumikvõrgud:

- 2.1. *Home Subscriber Server* (HSS)
- 2.2. *Packet Gateway* (PGW)
- 2.3. *Policy and Charging Rules Function* (PCRF)
- 2.4. *Mobility Management Entity* (MME)
- 2.5. *Serving Gateway* (SGW).

3. 5G tuumikvõrgud:

- 3.1. *NSSF – Network Slice Selection Function*
- 3.2. *NEF – Network Exposure Function*
- 3.3. *NRF – Network Repository Function*
- 3.4. *PCF – Policy Control Function*
- 3.5. *UDM – User Data Management*
- 3.6. *AF – Application Function*
- 3.7. *AUSF – Authentication Server Function*
- 3.8. *AMF – Access ja Mobility Management Function*
- 3.9. *SMF – Session Management Function*
- 3.10. *SMSF – Short Message Service Function*
- 3.11. *UPF – User Plane Function*
- 3.12. *CHF – Charging Function*
- 3.13. *W-AGF – Wireline Access Gateway Function*
- 3.14. *NWDAF – Network Data Analytic Function*
- 3.15. *5G-EIR – 5G Equipment Identity Register*

- 3.16. UDR – *Unified Data Repository*
- 3.17. UDSF – *Unstructured Data Storage Function*
- 3.18. N3IWF – *Non-3GPP InterWorking Function*
- 3.19. TNGF – *Trusted Non-3GPP Gateway Function*
- 3.20. TWIF – *Trusted WLAN Interworking Function*
- 3.21. SEPP – *Security Edge Protection Proxy*
- 3.22. I-NEF – *Intermediate NEF*
- 3.23. SCP – *Service Communication Proxy*

Uued standardid ja nendel põhinevad tuumikvõrgu funktsioonid avaldatakse ETSI kodulehel.²⁵ Eelnev nimekiri on toodud näitena ega ole kõikehõlmav. Lähtuda tuleb ETSI kodulehel avaldatud tuumikvõrgu funktsioonidest.

Sidevõrkude areng on dünaamiline protsess, kus pidevalt lisanduvad uued tehnoloogiad, võimalused ning ka potentsiaalsed ohud. Lisaks senini kasutatud liigitamisele tuumikvõrguks, transportvõrguks ning juurdepääsuvõrguks on kaasaegsetes telekommunikatsioonivõrkudes järjest kasvav spetsiifilise tarkvara, riistvara ning funktsioonide kogum, mis on võrgu tööks vähemalt sama olulised kui klassikalised tuumikvõrgu komponendid, st mõjutavad sidevõrgu terviku toimimist.

Samas omavad erinevad sidevõrgud oma erinevates kihtides eri funktsioone ning esineb olukordi, kus sama termini või lühendiga tähistatakse sisuliselt erinevaid asju. Samal terminil võib olla erinevaid tähendusi või sama nimega funktsioon, mis võib üheaegselt asuda nii tuumikvõrgus kui ka vähem kriitilises võrgu osas, näiteks kohaliku tähtsusega tugijaamas. Kui funktsioon on eeltoodud ETSI standardite kohaselt kirjeldatud kui tuumikvõrgu funktsioon, kuid töötab lisaks tuumikvõrgule ka muus võrgu osas, näiteks juurdepääsuvõrgus, ning omab seal üksnes piiratud lokaalset mõju, ei ole sel juhul väljaspool tuumikvõrku tegemist tuumikvõrgu funktsiooniga.

Tuumikvõrgu funktsioonidega võrdväärse olulisusega on sellised funktsioonid, mille kaudu või mille häirimisel on võimalik mõjutada teenusepakkuja võrku rohkem kui lokaalselt ehk mille kaudu või mille häirimisel on võimalik mõjutada vähemalt 1000 lõppkasutajat või teise sideettevõtja sidevõrku. Samuti on tuumikvõrgu funktsioonidega võrdväärse olulisusega funktsioonid, mis võimaldavad jälitustoimingu teostamist või sõnumi saladuse õiguse piiramist.

Jälitustoiming on kriminaalmenetluse seadustiku § 126¹ lõike 1 kohaselt isikuandmete töötlemine seaduses sätestatud ülesande täitmiseks eesmärgiga varjata andmete töötlemise fakti ja sisu andmesubjekti ees. ESS § 113 lõike 1 kohaselt peab sideettevõtja võimaldama jälitus- või julgeolekuasutusele juurdepääsu sidevõrgule vastavalt jälitustoimingu teostamiseks või sõnumi saladuse õiguse piiramiseks. Funktsioonide all, mis võimaldavad jälitustoimingu teostamist või sõnumi saladuse õiguse piiramist, on mõeldud *lawful interception* (LI) funktsioone. LI standardid on kättesaadavad ETSI kodulehel.

Paragrahv 8² puudutab kasutusloa kohustuse rakendamist.

Kasutusloa kohustus rakendub koos määruse jõustumisega. Üldreeglina tuleb kasutusloba taotleda riist- ja tarkvarale, mis plaanitakse kasutusele võtta pärast määruse jõustumist ehk 1.

²⁵ Kättesaadav: <https://www.etsi.org/>

novembrit 2020. Kasutusloa taotlus tuleb esitada enne riist- või tarkvara plaanitavat kasutusele võtmist. Sellele üldreeglile on kolm erisust, millest üks sisaldub põhiregulatsioonis ning puudutab juhtumit, kus riist- või tarkvara on tarvis viivitamata paigaldada küberintsidendi kõrvaldamiseks või selle vahetuks ärahoidmiseks. Teised kaks erisust on sätestatud § 8² lõigetes 1 ja 2.

Paragrahv 8² lõike 1 kohaselt hõlmab kasutusloa taotlemise kohustus riist- ja tarkvara, mis on kasutusele võetud enne 1. novembrit 2020 ja milles võetakse 5G NSA või uuema mobiilsidevõrgu standardi funktsioon kasutusele pärast 1. novembrit 2020. Sellise riist- ja tarkvara kasutusloa taotlus tuleb esitada enne plaanitavat 5G NSA või uuema mobiilsidevõrgu standardi funktsiooni kasutusele võtmist.

Säte on vajalik, kuna riigi julgeoleku tagamiseks on oluline, et riske riigi julgeolekule oleks võimalik maandada ka sellisel juhul, kui enne määruse jõustumist on kasutusele võetud kõrge riskiga riist- ja tarkvara ning sellele tehakse pärast määruse jõustumist tarkvarauuendus, mille puhul tarkvara ei ole kõrge riskiga. Riigile on julgeoleku aspektist oluline, et sidevõrk oleks 5G osas 1. jaanuarist 2024 kõrge riskiga riist- ja tarkvarast vaba.

Kuna lõige hõlmab olemasoleva riist- ja tarkvara, mis on juba kasutusele võetud, täpsustatakse, et kasutusloa tuleb esitada enne funktsiooni kasutusele võttu.

Paragrahv 8² lõike 2 kohaselt tuleb vahemikus 1. november 2020 kuni 1. jaanuar 2029 kasutusele võetava riist- ja tarkvara, millel ei ole kriitilist funktsiooni ega 5G NSA või uuema mobiilsidevõrgu standardi funktsiooni, kasutusloa taotlus esitada hiljemalt 1. juuliks 2029.

Säte on vajalik, et anda sideettevõtjale üleminekuaeg sellise kõrge riskiga riist- ja tarkvara osas, mis ei ole niivõrd kriitiline erinevalt kriitilise funktsiooniga riist- ja tarkvarast ning riist- ja tarkvarast, millel on 5G NSA või uuema mobiilsidevõrgu standardi funktsioon.

Eelnõu §-ga 2 täiendatakse Vabariigi Valitsuse 11. detsembri 2015. a määrust nr 129 „Vabariigi Valitsuse julgeolekukomisjoni põhimäärus“ §-ga 7¹, mille pealkiri on „Küberjulgeoleku nõukogu“. Paragrahv koosneb kaheksast lõikest.

Paragrahv 7¹ lõige 1 sätestab, et Vabariigi Valitsuse julgeolekukomisjoni juures tegutseb küberjulgeoleku nõukogu. Praktikas on Vabariigi Valitsuse julgeolekukomisjoni (lühidalt *komisjoni*) juures küberjulgeoleku nõukogu tegutsenud aastast 2009. Seni on küberjulgeoleku nõukogu kehtestatud Vabariigi Valitsuse julgeolekukomisjoni põhimääruse § 8 lõike 1 alusel ning nõukogu on tegutsenud nõukogu töökorra alusel. Muudatusega tuuakse küberjulgeoleku nõukogu alus Vabariigi Valitsuse julgeolekukomisjoni põhimäärusesse.

Paragrahv 7¹ lõige 2 sätestab küberjulgeoleku nõukogu pädevuse ja ülesanded. Lõike kohaselt küberjulgeoleku nõukogu: annab suuniseid küberjulgeoleku poliitika kujundamiseks; võtab seisukohti küberjulgeoleku valdkonda puudutavate plaanide kohta; kooskõlastab sideettevõtja taotluses nimetatud riist- ja tarkvara kasutamise vastavuse riigi julgeolekuhuvidele; täidab teisi komisjoni antud ülesandeid.

Sideettevõtja taotluses nimetatud riist- ja tarkvara kasutamise vastavuse koostööstamine riigi julgeolekuhuvidel võib seisneda ka tingimuste määramises.

Paragrahv 7¹ lõike 3 kohaselt on küberjulgeoleku nõukogul sideettevõtja taotluses nimetatud riist- ja tarkvara kasutamise riigi julgeolekuhuvidel vastavuse koostööstamisel haldusmenetluse seaduses haldusorganile antud õigused ja kohustused.

Paragrahv 7¹ lõike 4 sätestab küberjulgeoleku nõukogu liikmed. Nendeks on Haridus ja Teadusministeeriumi, Justiitsministeeriumi, Kaitseministeeriumi, Rahandusministeeriumi, Siseministeeriumi, Välisministeeriumi, Majandus- ja Kommunikatsiooniministeeriumi kantsler, Majandus- ja Kommunikatsiooniministeeriumi side eest vastutav asekanter, Majandus- ja Kommunikatsiooniministeeriumi riigi küberturvalisuse poliitika juht, Riigikantselei julgeoleku ja riigikaitse koordinatsioonibüroo direktor, Politsei- ja Piirivalveameti, Kaitsepolitseiameti, Välisluureameti, Tarbijakaitse ja Tehnilise Järelevalve Ameti, Andmekaitse Inspeksiooni ja Riigi Infosüsteemi Ameti peadirektor, Riigi Infosüsteemi Ameti küberturvalisuse eest vastutav peadirektori asetäitja, Kaitseväge peastaabi ülem, Kaitseleidi ülem ja riigi peaprokurör. Liikmeid on seega 17 asutusest. Neist 15 asutust on ka varasemalt olnud nõukogu koosseisus. Varasemast uued asutused on TTJA ning AKI (Andmekaitse Inspeksioon). TTJA lisandub, kuna nõukogu hakkab tegema otsuseid sidevõrkude turvalisuse küsimustes, kus TTJA osalus nende otsuste tegemisel on vajalik nii nende kompetentsi tõttu sidevaldkonnas kui ka nende koordineeriva ja infovaldaja rolli tõttu sidevõrkude turvalisuse loamenetluses. AKI lisandub, kuna küberturvalisuse küsimused on sageli tihedalt seotud andmekaitsega ning AKI pädevus andmekaitse valdkonnas võimaldab nõukogul teha privaatsusõiguse ja andmekaitseõiguse aspektidest teadlikumaid otsuseid. Igale liikmele määrab vastav asutus asendusliikme. Asendusliikmete määramine on vajalik, et tagada nõukogu töövõime.

Paragrahv 7¹ lõike 5 sätestab, et küberjulgeoleku nõukogu on otsustusvõimeline, kui koosolekust võtab osa vähemalt kaks kolmandikku nõukogu koosseisust. See säte on vajalik, et tagada nõukogu liikmete osalus koosolekul ning otsuste koostööstala võimalikult paljude nõukogude liikmete arvamusega.

Paragrahv 7¹ lõike 6 kohaselt tehakse küberjulgeoleku nõukogu otsused koosolekul osalevate liikmete häälteenamusega. Häälte võrdsel jagunemisel on otsustav koosoleku juhataja hääle.

Paragrahv 7¹ lõike 7 kohaselt kutsab küberjulgeoleku nõukogu koosolekuid kokku ja juhatab nõukogu esimees, kelleks on Majandus- ja Kommunikatsiooniministeeriumi kantsler või tema määratud isik. Selline kord on kehtinud ka varasemalt.

Paragrahv 7¹ lõike 8 sätestab, et küberjulgeoleku nõukogu töökorra, liikmed ja asendusliikmed kinnitab komisjon.

Eelnõu § 3 sätestab määruse jõustumise. Määrus jõustub 1. novembril 2020.

3. Eelnõu vastavus Euroopa Liidu õigusele

Eelnõul ei ole puutumust Euroopa Liidu õigusega.

4. Määruse mõjud

4.1. Sotsiaalne, sealhulgas demograafiline mõju

Määruse muudatusega ei kaasne sotsiaalseid ega demograafilisi mõjusid.

4.2. Mõju riigi julgeolekule ja välissuhetele

Määrusega kaasneb positiivne mõju riigi julgeolekule ja välissuhetele. Eelnõu abil tagatakse, et rajatavad sidevõrgud ei kujutaks ohtu riigi julgeolekule laia riigikaitse põhimõtete tähenduses, hõlmates seejuures ka riigi kriitilist infrastruktuuri ja elutähtsaid teenuseid.

Uute tehnoloogiate tingimusteta lubamine Eesti sidetaristusse võib tuua kaasa negatiivseid tagajärgi, mis puudutavad nii era- kui avalikku sektorit ja riigi majandusruumi toimimist tervikuna. Riigil on kohustus tagada, et sidevõrgud rajataks usaldusväärsele tehnoloogiale, mille kasutamine ei too kaasa olukorda, kus riik ei saa tagada oma kodanikele põhiõiguste- ja vabaduste, sh privaatsuse, sõnumisaladuse ja intellektuaalse omandi kaitset. Kõrge riskiga tehnoloogiast tulenevate julgeolekuriskide realiseerumise korral on kõige nõrgemas positsioonis just lõpptarbijatest tavalised elanikud, kes ei saa olukorras, kus sidevõrgud on ebausaldusväärset või kergesti haavatavalt rajatud, iseenda küberturvalisuse tagamiseks midagi ette võtta.

Riigikaitse perspektiivist on äärmiselt oluline, et sidevõrkudes kasutatavat tehnoloogiat toodaksid usaldusväärsed ettevõtted, kes ei oleks manipuleeritavad ning keda usaldaksid meie Euroopa Liidu ja NATO liitlased. On oluline, et Eesti sidevõrke ei rajataks kõrge riskiga tehnoloogiaga, mille kaudu on tõenäoline riigikaitseks kasutatavate süsteemide halvamine või mille kasutamist liitlasriigid ei aktsepteeri ja mis võiks seeläbi kaasa tuua viivitusi või takistusi kriitilise tähtsusega infovahetuses ja riigikaitse tegevuses.

Euroopa Liidu liikmesriigid on jõudnud ühiselt seisukohale, et IKT riskide hindamisel tuleb arvesse võtta kõiki aspekte – nii tehnilisi kui ka mittetehnilisi.²⁶ Liikmesriikide ühises riskianalüüsis tõdetakse, et tuleviku sidevõrkude (sh 5G) kontekstis on kõige suuremaks ohuks Euroopa Liidu välised ebademokraatlikud riigid, kellel on huvi ja võimekus ellu viia küberrünnakuid ning kes omavad mõjuvõimu enda jurisdiktsioonis asuvate ettevõtete üle. Seetõttu on oluline rakendada liikmesriikides protseduure, mis võimaldaksid hinnata tehnoloogia tootja riskiprofiili ning vältida kõrge riskiga tarnijate mõju.

4.3. Majanduslik mõju

Eelnõuga ei teki riigile, kohalikele omavalitsustele ega ka sideteenuste lõppkasutajatele vältimatuid kulusid.

Sideettevõtjate jaoks võivad eelnõuga kaasneda kulud, kui rikutakse määrusega seatud kohustusi, näiteks jäetakse riist- või tarkvara osas luba taotlemata. Teavitamiskohustuse ja loakohustuse täitmisega tõuseb sideettevõtjate halduskoormus, mistõttu võib kaasneda tööjõukulu kasv.

Samuti võivad sideettevõtjale kaasneda kulud, kui juba kasutusel olev riist- ja tarkvara sobib 5G NSA ja uuema põlvkonna mobiilside funktsioonide kasutamiseks, kuid osutub kõrge riskiga

²⁶ EU2019FI. Member states publish report on EU-coordinated risk assessment of 5G network security. 09.10.2019. Kättesaadav: https://eu2019.fi/en/article/-/asset_publisher/member-states-publish-a-report-on-eu-coordinated-risk-assessment-of-5g-networks-security.

riist- ja tarkvaraks. See tähendab, et ettevõtja võib antud riistvara kasutada vanema põlvkonna teenuste pakkumiseks, kuid 5G NSA ja uuemate funktsioonide kasutamiseks peab soetama riist- ja tarkvara, mis ei ole kõrge riskiga. Sideettevõtjate võimalike kuluste vähendamine on üks aspektidest, millega on arvestatud kasutusloa kohustuse ja kõrge riskiga riist- ja tarkvara keelu rakendamisel. Loakohustus kriitiliste funktsioonide osas ei too sideettevõtjatele kulusid, kuna selles osas ei ole teadaolevalt kasutuses riist- ja tarkvara, mille oleks tootnud kõrge riskiga tootja. 5G NSA ja uuema mobiilsidevõrgu standardi funktsioonidega kõrge riskiga riist- ja tarkvara on lubatud kasutada 1. jaanuarini 2024. Seega saab vahepealsel perioodil (kasutusloa kohustuse rakendumise ja 1. jaanuari 2024 vahel) ettevõtja kasutusloa menetluse kaudu teada, kas tema riist- ja tarkvara kujutab ohtu riigi julgeolekule. Enne 1. jaanuari 2024 on tal võimalik riist- ja tarkvara kasutada, kui see on kõrge riskiga. Tegemist on seega üleminekuperioodiga, mis võimaldab ettevõtjal kulusid vähendada ja tegevust ette planeerida. Ülejäänud kasutusele võetava riist- ja tarkvara osas on üleminekuperiood pikem (1. jaanuarini 2030), et sideettevõtja saaks oma tegevuses loakohustuse rakendamisega ette arvestada ning võimalikke tulevasi kulusid minimeerida, kuna praegu on nendes osades kasutusel ka kõrge riskiga tootjate riist- ja tarkvara.

Sideettevõtjad, kes on määruse kohaldamisalas, peavad sidevõrkude rajamisel arvestama määrusest tulenevate kohustustega. Seetõttu ei ole võimalik välistada olukorda, et lahendused, mida ettevõtja oleks loa taotlemise kohustuse puudumisel majanduslikult kõige soodsamate tingimuste tõttu eelistanud, ei pruugi riigi julgeolekuhuvide seisukohalt sidevõrgu rajamiseks sobida ning valida tuleb mõni muu tehnoloogia pakkuja.

4.4. Mõju riigiasutuste ja kohaliku omavalitsuse asutuste korraldusele

Määrus omab mõju MKM haldusala eelarvele, kuna määruse rakendamiseks on vaja luua üks uus töökoht. Tegemist on sidevõrgu riist- ja tarkvara hindamisega riigi julgeoleku seisukohast, mille osas täna TTJA-l pädevus puudub. Lisandub töökoormus menetluste näol (dokumentide kontroll, otsuste ettevalmistamine, töö koordineerimine osapoolte vahel jne) ning vajalik on sisuline panustamine küberjulgeoleku nõukogu töösse.

Julgeolekuasutuste, Riigi Infosüsteemi Ameti ja küberjulgeoleku nõukogu töökoormus suureneb. Selle mõju suurus on seotud TTJA loamenetluse käigus arvamuste / ettepanekute küsimise ja nendega kaasnevate dokumentide hulgaga, mida ei saa täpselt ette ennustada.

5. Määruse rakendamiseks vajalikud kulutused ja määruse rakendamise eeldatavad tulud

Määruse rakendamisega on vaja suurendada MKM haldusala eelarvet ühe inimese palgakulu võrra, milleks hinnanguliselt on kalendriaastas koos kõikide maksudega 32 112,00 eurot.

Käesoleva määruse rakendamisega ei kaasne otseseid tulusid riigieelarvesse.

6. Määruse jõustumine

Määrus jõustub 1. novembril 2020.

7. Eelnõu kooskõlastamine, huvirühmade kaasamine ja avalik konsultatsioon

Eelnõu esitatakse kooskõlastamisele eelnõude infosüsteemi (EIS) kaudu Justiitsministeeriumile, Siseministeeriumile, Kaitseministeeriumile, Rahandusministeeriumile,

Riigikantseleile ja Välisministeeriumile ning arvamuse avaldamiseks Eesti Infotehnoloogia ja Telekommunikatsiooni Liidule.

Määruse eelnõu sisu on pidevalt arutatud ning seeläbi täiendatud IKT seadmete usaldamise poliitika töörühma koosolekutel (vt seletuskirja punkt 1.2). Määruse eelnõu kontseptsiooni on tutvustatud Vabariigi Valitsuse julgeolekukomisjoni küberjulgeoleku nõukogule ning määruse eelnõule on oma toetuse andnud Vabariigi Valitsuse julgeolekukomisjon.

Sideettevõtjaid, kellele kaasneb määrusega kohustusi, on järjepidevalt kaasatud, sealhulgas määruse kontseptsiooni loomise protsessi ning määruse eelnõu mustandi tagasisidestamisel. Määruse eelnõus on muu hulgas arvestatud sideettevõtjate tagasisidet tehnoloogilistest aspektidest, näiteks loakohustuse alla minevate funktsioonide defineerimisel. Samuti on kohtunud ning määruse kontseptsiooni tutvustatud selleks soovi avaldanud sidevõrkudes kasutatava riist- ja tarkvara tootja Huaweiiga.

Avalik konsultatsioon sideettevõtjatega toimub eelnõu ametliku kooskõlastamisega samaaegselt.