EESTI
INFOTEHNOLOOGIA JA
TELEKOMMUNIKATSIOONI
LIIT

Sideosakond
Majandus- ja
Kommunikatsiooniministeerium
Harju 11
15072 TALLINN

Teie 17.01.2017

Meie 02.02.2017 nr 5.1-1/10

Arvamus Euroopa Komisjoni poolt 10.01.2017.
avaldatud e-privaatsuse määruse ettepaneku kohta

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit (edaspidi: ITL) analüüsis Euroopa Komisjoni (edaspidi: EK) poolt 10.01.2017. avalikustatud ettepanekut nr COM(2017) 10 final võtta vastu eraelu puutumatust ning elektroonilist sidet käsitlev määrus (edaspidi: e-privaatsuse määrus). Käesolevaga esitab ITL oma arvamuse e-privaatsuse määruse ettepaneku kohta.
Alustuseks toome välja oma üldisemad seisukohad ning seejärel esitame oma kommentaarid, ettepanekud ja küsimused e-privaatsuse määruse konkreetsete põhjenduspunktide ja artiklite kohta.

1. Kooskõla andmekaitse üldmäärusega ja e-privaatsuse määruse maht

ITL nõustub, et Euroopa Parlamendi ja Nõukogu direktiiv 2002/58/EÜ, milles käsitletakse isikuandmete töötlemist ja eraelu puutumatuse kaitset elektroonilise side sektoris (edaspidi: e-privaatsuse direktiiv) on vaja üle vaadata ning viia kooskõlla Euroopa uue andmekaitse üldmäärusega (General Data Protection Regulation, edaspidi: GDPR). ITL-i hinnangul tuleks seda tehes lähtuda järgmisest:
1) E-privaatsuse määrusega tuleks reguleerida vaid neid spetsiifilisi küsimusi, mida GDPR ei reguleeri. Küsimustes, mida GDPR reguleerib, ei ole vaja kehtestada elektroonilise side sektoris teistest sektoritest rangemat regulatsiooni. See põhjustaks vaid erinevaid tõlgendusi ja õiguslikku ebaselgust, mille tagajärjeks on nii e-privaatsuse määruse kui ka GDPR-i väga erinev rakendamine Euroopa Liidu riikides. See on aga vastuolus digitaalse ühtse turu strateegia suurema eesmärgiga, milleks on õigusaktide harmoniseerimine ja praktikate ühtlustamine.
2) E-privaatsuse direktiivi üle vaatama hakates räägiti sellest, et sellest direktiivist jäetakse välja kõik, mis on GDPR-iga kaetud, mis tähendab, et alles jääb umbes kolm artiklit. Hetkel on EK välja pakkunud e-privaatsuse määruse ettepaneku, mis kordab GDPR-i ning kohati ka laiendab seda. Lisaks on ette nähtud mitu alamakti ning juhised, mille regulatsiooni ulatus on ebaselge ja mis suurendavad regulatsiooni mahtu veelgi.
Sellest tulenevalt oleme seisukohal, et **e-privaatsuse määruse regulatsiooni mahtu tuleb vähendada**. Ettepaneku eesmärgina märgib EK tarbijate kõrgetasemelise kaitsega samaväärsena innovatsioonivõimalusi ettevõtjatele. Ülereguleerimise ning GDPR-i sätete täiendamisega pole võimalik viimati mainitud eesmärki saavutada. E-privaatsuse uus regulatsioon peaks olema lihtsam nii teenuse kasutajatele kui ka pakkujatele.

Kindlasti tuleb üle vaadata ka kavandavate alamaktide maht ning võtta alamaktid vastu vaid küsimustes, kus regulatsioon on hädavajalik, aga küsimust ei ole võimalik reguleerida määruses endas.

2. Regulatsiooni laiendamine uutele teenustele

Üldise kommentaarina märgime veel, et ITL toetab e-privaatsuse määruse laiendamist uutele teenustele nn *over the top* ehk OTT-teenustele (nt Viber, WhatsApp, Facebook Messenger), mis oma olemuse ja kasutajate seisukohast võetuna on nn klassikaliste sideteenuste samaväärsed alternatiivid. Oleme seisukohal, et kõik teenusepakkujad, kes tegutsevad samas sektoris ja pakuvad samalaadseid sõnumside jms teenuseid, mille kasutamisel tekib kaitset vajavaid isikute eraelulisi isikuandmeid, peavad olema e-privaatsuse määrusega ühtemoodi reguleeritud.
Leiame samas, et ühesuguse regulatsiooni rakendamine ei tohi kaasa tuua seda, et OTT teenuseid ja teisi nn uue põlvkonna teenuseid asutakse reguleerima samavõrd rangelt ja liigselt, kui täna reguleeritakse elektroonilise side teenuseid. Selle asemel on vaja hoopis vähendada e-privaatsuse regulatsiooni mahtu viisil, mis võimaldab rakendada samu reegleid ka OTT teenuste suhtes. Lähtuma peab põhimõttest, et innovatsiooni ei tohi takistada ja lämmatada liiga keerulise ning mahuka regulatsiooniga.

3. Määruse jõustumine

Peamine probleem on ITL-i hinnangul e-privaatsuse määruse jõustumise tähtaeg. Nimelt on see planeeritud jõustuma koos GDPR-iga ehk 25.05.2018. See aga tähendab, et eelnõu vastuvõtmise ja selle kohaldamise kohustuse vahele jääb tõenäoliselt liiga vähe aega. Kuna e-privaatsuse määrusega kaasnevad ka rakendusaktid ja juhised, siis on väga keeruline (kui mitte öelda võimatu) seda mõni kuu peale vastuvõtmist rakendama hakata. Samas jäeti näiteks GDPR-i jõustumiseks [rakendamiseks] kaks aastat.
Näitena toome siinkohal sissetulevate kõnede blokeerimise võimaldamise kohustuse (e-privaatsuse määruse artikkel 14), mille täitmiseks on vajalik arendada uus tarkvaraline rakendus. Samamoodi on ettevõtjatel vaja aega, et siduda oma teenustega 6-kuuliste intervallidega korduvad nõusolekuid puudutavad meeldetuletused (e-privaatsuse määruse artikkel 9 lg 3).
ITL on seisukohal, et e-privaatsuse määrus saab jõustuda mitte varem kui vähemalt üks aasta pärast peale selle lõplikku vastuvõtmist. Määruse rakendusaktid ja selle kohta antavad juhised peaksid olema valmis vähemalt 9 kuud enne määruse lõplikku jõustumist. Kui seda ei suudeta tagada, siis tuleks jõustumisaega edasi lükata või võtta e-privaatsuse määrusest kohustusi vähemaks.
Kokkuvõtvalt tuleb tõdeda, et e-privaatsuse määruse praktilise rakendamise küsimused on jäetud läbimõtlemata ja vajalike rakendussätetega piisavalt katmata.

4. Masinatevaheline suhtlus ja asjade internet

E-privaatsuse määruse põhjenduspunkti 12 kohaselt laieneb määrus ka masinatevahelisele (M2M) suhtlusele, mis tähendab, et ka asjade internetile (ingl k *internet of things* ehk IoT). Meie hinnangul peaks sellesse väga ettevaatlikult suhtuma, sest hetkel on tegemist veel suures osas tundmatu valdkonnaga. Liiga varajane regulatiivne sekkumine ohustab selliste uute teenuste arendamist ning kasutuselevõtmist.

Juhime tähelepanu, et andmepõhise majanduse teema on hetkel Euroopa Liidus arutelu all. 10.01.2017 avalikustas Euroopa Komisjon teatise nr COM(2017) 9 final Euroopa andmepõhise majanduse kohta ning ühtlasi avati selle teemaline avalik konsultatsioon.[1] Selle käigus arutatakse järgmisi küsimusi: kes on andmete omanik, andmetele juurdepääs, andmetega seotud vastutus, andmete vaba liikumine jms. Kõik need küsimsued on seega hetkel ebaselged, mis tähendab, et e-privaatsuse määrus hakkaks ettepaneku kohaselt kaitsma protsesse, mis on tegelikult veel välja töötamata.
ITL teeb ettepaneku M2M puudutav e-privaatsuse määruse käsitlusalast välja jätta või M2Mi osas lisada määrusesse sisse erand ehk vähendada oluliselt sellele kohalduva regulatsiooni mahtu. Need isikuandmed, mis vajavad kaitset, peaks olema kaitstud üldise metaandmete regulatsiooni alusel. See tähendab, et kui masinate vahel liigub metaandmeid, mis on seotud konkreetsete isikutega, siis nende osas rakendatakse e-privaatsuse määrust. Kõikide muude võimalike andmete osas, mis masinate vahel liiguvad ning mida ei sa pidada isikuga seotud metaandmeteks, ei tohiks e-privaatsuse määrust rakendada.

5. Avalikud WiFi punktid

E-privaatsuse määruse pp 13 kohaselt rakendub määruses sätestatu ka avalikele internetipunktidele. Leiame, et sellise vastutuse täies ulatuses rakendamine teenuse osutajatele, kelle põhiteenus ei ole internetiühenduse pakkumine, võtab neilt motivatsiooni oma klientidele sellist lisavõimalust pakkuda. Oleme seisukohal, et avalike WiFi punktide pakkujatel peaks olema kohustus informeerida oma kliente oma võrgu privaatsustasemest, aga ei ole mõistlik eeldada, et selliste võrkude privaatsustase on võrreldav elektroonilise sideteenuse osutajate poolt sideteenuse kasutajatele pakutavaga. Kui e-privaatsuse määrusega oleks tagatud eeltoodud info andmine lõppkasutajatele, oleks neil võimalus ise teadlikult otsustada, kas nad soovivad sellistel tingimustel avalikku internetiteenust kasutada või mitte.

6. Nn küpsised (Cookies)

E-privaatsuse määrusest jääb ebaselgeks, kelle vastutus on nn küpsiste nõusolekutega seonduv. Näiteks kas kasutajate nõusolekud võtab vaid veebilehitseja arendaja või millal on veebilehe omanikul õigus nõusolekut uuesti küsida. Samuti soovime selgust küsimuses, kas juhul, kui kasutaja küpsiste kasutamise keelab, ei pea talle võimaldama juurdepääsu veebilehele või peab ta suunama siis alternatiivsele, piiratud võimalustega veebilehele.
Peame positiivseks seda, et e-privaatsuse määruse ettepanekus rõhutatakse, et teenuse kasutajate „üleujutamine“ erinevate nõusolekute küsimistega pole aktsepteeritav. Ka ITL on seisukohal, et regulatsioon peab olema lihtsam nii teenuse kasutajatele kui ka pakkujatele.

7. Sideandmete säilitamine ja kustutamine

E-privaatsuse määruse artikkel 7(3) on ebaselge ning läbimõtlemata. Andmete säilitamise tähtajad on hetkel erinevates Euroopa Liidu liikmesriikides erinevad ning määrusega üritatakse neid lühendada. Samas Eestis tooks selles artiklis sätestatu kindlasti kaasa praeguse elektroonilise side seadusest tuleneva sideandmete säilituskohustuse üheaastase tähtaja pikenemise kolmele aastale, mis on seadusest tulenev nõude aegumistähtaeg, mille jooksul on lõppkasutajal võimalik talle esitatud sideteenuste arvet vaidlustada.

[1] Vt lähemalt: http://europa.eu/rapid/press-release_IP-17-5_en.htm?locale=en

Leiame, et selle tähtaja peab panema vähemalt siseriiklikult selgelt paika, sest vastasel juhul hakkavad erinevad sideettevõtjad seda sätet erinevalt rakendama ehk kehtestama erinevaid tähtaegu pretensioonide esitamise tähtaja kaudu ning tulemuseks on kasutajate jaoks väga ebaselge olukord.

8. Lõpp-kasutajate terminalseadmed

E-privaatsuse määruse artikkel 8 on meie hinnangul e-privaatsuse määruse kõige ebaselgem koht. Selle paremaks tõlgendamiseks ja mõistmiseks tuleks sellele otsesemalt viidata preambula põhjenduspunktides. Praegu jääb täiesti ebaselgeks, milliste põhjenduspunktide kontekstis tuleks artiklit 8 tõlgendada.
Teiseks on see artikkel üldiselt võttes liiga range, kuna kasutuseranditest on välja jäänud praeguse regulatsiooni alusel tunnustatud ja olulised alused. Näiteks tuleb kindlasti lisada teenuse osutaja õigus säilitada ja kasutada neid andmeid ka teenuse kvaliteedi tagamise eesmärgil. Oleks äärmiselt keeruline osutada jätkusuutlikult ja stabiilselt kvaliteetset teenust, kui see on seatud sõltuvusse konkreetse lõppkasutaja nõusoleku olemasolust.
Samuti teeb klientidele pidev kohustuslikult küsitavate nõusolekutega tutvumine terminali kasutamise ebamugavaks, mis viib selleni, et kliendid ei jaksa enam iga üksiku nõusoleku sisusse süüvida ja kõik aktsepteerivad läbi lugemata kõiki küsimusi. See viib just lõppkasutajate „nõusolekute küsimisega üleujutamiseni“, mis ei ole regulatsiooni eesmärk ja mida on Euroopa Komisjon soovinud vältida.
Samuti oleks vaja kiiremas korras artikkel 8 lõikes 4 nimetatud alamakte ning rakendussätteid kohaldamise tähtaja osas, sest ilma nendeta ei ole võimalik selles sättes sisalduvaid kohustusi õigeaegselt ja korrektselt täita.

9. Nõusolek

Me ei pea õigeks e-privaatsuse määruse artiklis 9 sisalduvat kohustust, mille kohaselt peaks teenuse osutaja hakkama kõigile oma klientidele iga kuue kuu tagant meelde tuletama, et kliendil on õigus enda poolt antud nõusolekud tagasi võtta. Sellise kohustuse täitmine tähendaks väga suurt koormust nii sideettevõtjatele kui ka lõppkasutajatele. See oleks klientide „üleujutamine“ tarbetu asjaajamisega. Pealegi pole see absoluutselt vajalik, sest teenuse kasutajad saavad ju nagunii näiteks pakkumisi, mille all on alati toodud link, kus nad saavad oma nõusolekuid muuta.
Seega ei ole vajalik kehtestada eraldi kohustust nõusolekust loobumist meelde tuletada. Siin on ette näha klientide pahameelt kes ei mõista, miks sideettevõtja neid tüütab ja miks nad kord juba antud nõusolekut uuesti andma peavad.
Antud teema on näide ka sellest, kuidas e-privaatsuse määrusega tahetakse minna kaugemale GDPR-i regulatsioonist, kus sellist kohustust ei ole isegi mitte isikuandmete eriliikide suhtes kehtestatud.

10. Sideandmete säilitamisega seotud päringud

E-privaatsuse määruse artikkel 11(2) kohaselt peavad elektroonilise side teenuse osutajad kehtestama sisemised protseduurid, et vastata lõppkasutajate sideandmete juurdepääsuga seotud päringutele. Eestis hoiavad jälitusasutused ise nende andmetega seotud päringute infot. Samuti on Eestis paljudel juhtudel jälitusasutustele avatud elektroonilised otsekanalid nendele andmetele juurdepääsuks, mille mõte ongi selles, et sideettevõtja ise ei näe ega tohigi näha neid päringuid ja andmeid. Seega peaks e-privaatsuse määruse artikkel 11(2) sisalduv jääma kindlasti siseriikliku regulatsiooni objektiks.

Juhime veel tähelepanu sellele, et nimetatud artiklis sisalduva kohustuse mittetäitmine peab e-privaatsuse määruse artikli 24 kohaselt kaasa tooma ka karistuse, mis on efektiivne, proportsionaalne ja hoiatav, samal ajal kui Eestis ei ole selle sisu aktuaalne.
Sideandmete säilitamisega seoses peame äärmiselt oluliseks, et kehtestatakse üheselt mõistetav ja ammendav loetelu andmetest, mida sideettevõtjad peavad säilitama ning nende andmete säilitamise tähtaegadest. Kindlasti tuleb vastutus kehtestada neile ametiisikutele, kes küsivad juurdepääsu sideandmetele. Sideettevõtjaid ei tohi panna järele valvama, kas konkreetsel ametiisikul on õigus küsitavatele andmete juurdepääs saada või mitte kuna selleks puudub neil pädevus.
Kindlasti pooldame, et sideandmete säilitamise ja nendele andmete juurdepääsu tingimused määravad liikmesriigid ise.

11. Numbrinäidu edastamine ja piiramine ning numbriinfokataloogid

Oleme seisukohal, et e-privaatsuse määruse artiklid 12-13 ja 15 tuleks määrusest välja jätta, kuna nende teemade reguleerimiseks õigusaktiga ei ole enam vajadust. Sideteenuste turul ei ole numbrinäidu edastamise ja piiramise ning numbriinfokataloogidega probleeme, mis vajaksid Euroopa Liidu määruse tasemel reguleerimist.
Lisaks juhime tähelepanu, et elektroonilise side seaduse § 108 kohaselt on numbrinäidu kuvamise kohustused tingimusel, et see on tehniliselt võimalik. Hetkel e-privaatsuse määruse eelnõu sellist lisaklauslit ei sisalda, kuigi peaks.
Vastavaid artikleid lugedes tekkis meil ka küsimus, kas need kohustused kehtiksid ka juhul, kui kõne vastuvõtjal on number, aga kõne algatajal ei ole (nt OTT sõnumside teenuse kasutajal ei pruugi olla numbrit).
E-privaatsuse määruse põhjenduspunktis 31 pakutakse välja selgelt liiga keeruline ja koormav regulatsioon numbriinfokataloogide jaoks. Tänapäeval otsivad enamik inimesi esimesena infot Google'ist, kellele ei ole ette kirjutatud, kuidas ja mis alustel ta infot kuvama peab. Juhul, kui tõepoolest peaks kehtestatama numbriinfo teenusepakkujatele niivõrd karmid ja üksikasjalikud kohustused (s.t iga sideteenuse kasutaja õigus ise otsustada, mis andmeid täpselt ja kuidas avaldada tohib) võib olla päris kindel, et Eesti teenuse osutajad lõpetavad sellise teenuse osutamise ära. Kui numbriinfo teenuste teemat tingimata reguleerida tahetakse, siis peab jääma samasugune regulatsioon nagu täna ehk kasutaja võimalus üldiselt öelda, kas ta on oma numbri avalikustamisega nõus või ei ole. Mingisuguseid keerulisemaid skeeme ja tehnilisi lahendusi vähemalt Eesti tingimustes arendama ei hakataks, kuna nende väljatöötamine oleks selle äri mahtusid arvestades majanduslikult ebamõistlik.
Kui suudetakse põhjendada, et numbrinäidu ja numbriinfo kataloogide regulatsioon on siiski jätkuvalt vajalik, võiks need jätta siseriiklikult reguleeritavaks. Kui peetakse vajalikuks siiski ühtset regulatsiooni EL-i tasandil, siis oleks õigem neid küsimusi reguleerida uues sidekoodeksis (Euroopa Komisjoni ettepanek nr COM(2016) 590 final, 14.09.2016), kuna tegemist ei ole isikuandmete kaitse teemaga, vaid pigem tehniliste ja tarbijakaitseliste küsimustega.
Eeltoodu ei puuduta hädaolukorras numbri näitamisega seonduvat ehk e-privaatsuse määruse artikli 13 lõiget 1, mille regulatsioon on muidugi vajalik.

12. Sissetulevate kõnede blokeerimine

Me ei poolda ka e-privaatsuse määruse artikliga 14 kehtestatavat sissetulevate kõnede tasuta blokeerimise kohustust sideettevõtjatele, sest selliseks kohustuslikuks teenuseks puudub vajadus.

Leiame, et tegemist ei ole nii kaaluka küsimusega andmekaitseõiguses, et sideettevõtjad peaksid sellega eraldi tegelema. Praktikas ei pruugi tänapäeval numbrinäit väljendada seda, kust helistatakse, sest erinevate riikide hinnaeristustest tulenevalt muudetakse täiesti massiliselt numbreid.
E-privaatsuse määruse põhjenduspunkti 29 kohaselt on olemas sissetulevate kõnede blokeerimist võimaldav tehnoloogia sideettevõtjatele. Juhime tähelepanu sellele, et tegelikult on turul olemas hoopis piisavalt rakendusi (aplikatsioone), mille klient saab endale alla laadida ning mis võimaldavad teatud kõnesid blokeerida nagu näiteks Truecaller, Whoscall ja CIA. Ei ole mõistlik kohustada sideettevõtjaid tegema kallist süsteemiarendust ning pakkuda selle tulemusel klientidele tasuta teenust, mida kasutaks ilmselt väga vähe kliente. Tegemist on küsimusega, mille turg on juba lahendanud.

13. Turvariskidest teavitamine

E-privaatsuse määruse artikli 17 kohaselt teavituste saatmine on iseenesest sobiv aga meid teeb murelikuks lisatud täiendus, mille kohaselt peab teade sisaldama ka hinnangut potentsiaalsete kulude kohta. Juhime tähelepanu, et see teade tuleb ju klientidele saata **võimalikult kiiresti** ning potentsiaalsete kulude hindamine olukorras, kus turvariski täpsem sisu ja ulatus ei pruugi olla lõpuni selged, kulutab tarbetult aega ning ka kuluhinnang ise saaks olema ettenähtavalt väga oletuslik, ebatäpne ja sellisena kliente pigem segadusse ajav. Seetõttu on meie ettepanek jätta artikli 17 lõpust välja „*including an indication of the lickely costs involved*“.ˇ
Lisaks tekkis meil küsimus seoses sellega, et kuigi e-privaatsuse määruse artikkel 17 räägib konkreetsest (ingl k *particular*) riskist teavitamisest, siis määruse põhjenduspunkti 37 esimese lause kohaselt oleks justkui tegemist kohustusega teavitada lõppkasutajaid ka üldistest turvalisuse tagamise meetoditest. Õigusakti põhjendavas osas ei saa kehtestada täiendavaid kohustusi, mida õigusakti põhiosas ei sisaldu. Seetõttu tuleb see vastuolu kõrvaldada viies põhjenduspunkti teksti kooskõlla regulatsioonis endas sisalduvaga.

14. Järelevalve ja sanktsioonid

Me ei näe vajadust e-privaatsuse määruse V peatükis sisalduvate äärmiselt rangete karistuste järele. Raskemad rikkumised on nagunii kaetud GDPR-i alusel määratavate karistustega.
Leiame, et sellised trahvimäärad on ebamõistlikult kõrged ja ka e-privaatsuse määruse liiga lühike jõustamisaeg tekitab kindlasti probleeme. Sellises olukorras väga suurte trahvimäärade kehtestamine ei ole vastuvõetav.
Nagu me oleme ülalpool välja toonud, on paljud e-privaatsuse määruse sätted äärmiselt segaselt sõnastatud. Kui need võetakse vastu eelnõus oleval kujul ning määruse jõustumisaega ei lükata edasi, siis ei tohi määrus kindlasti sisaldada selliseid trahvimäärasid.

15. Regulatsiooni õigustehniline kvaliteet: vastuolud eelnõu preambula ja põhiosa vahel

Väga tõsine probleem on e-privaatsuse määruse raskesti loetavus. Nimelt on eelnõus justkui kaks eraldiseisvat osa: põhjenduspunktid preambulas ja artiklid põhiosas. Neid on omavahel väga raske seostada. Lugedes jääb mulje, et põhjenduspunktid reguleerivad ka küsimusi, mida määruse põhiosas pole. Seetõttu palume kindlasti e-privaatsuse määrus tervikuna üle vaadata ning põhjendav osa ning põhitekst omavahel paremini kooskõlla viia, et regulatsioonist oleks võimalik üheselt aru saada.

Kokkuvõttes leiame, et e-privaatsuse regulatsiooni kavand tuleb üle vaadata vähendades elektroonilise side spetsiifilist regulatsiooni küsimustes, mis on reguleeritud GDPR-iga. Samuti peame väga oluliseks, et kõik teenusepakkujad, kes tegutsevad samas sektoris ja pakuvad samalaadseid teenuseid, oleksid ühtemoodi reguleeritud.
Lahendamist vajavad kindlasti järgmised olulised küsimused**:**

- **ülereguleerimine,**
- **ebaselgus**
- **liiga lühike jõustumistähtaeg**.

Loodame, et leiate võimaluse arvestada ITL-i ülaltoodud seisukohti e-privaatsuse määruse ettepanekule Eesti riigi positsiooni kujundamisel. Oleme valmis Teiega kohtuma, et oma ettepanekuid täiendavalt selgitada.
Samuti anname teada, et arvestades ettepaneku olulisust ja keerukust ning piiratud ajaraamistikku, vajavad teatud e-privaatsuse määruse sätted põhjalikumat analüüsi. Seega analüüsime e-privaatsuse määrust kindlasti edasi ning esitame vajadusel Majandus- ja Kommunikatsiooniministeeriumile oma täiendavad seisukohad ning ettepanekud.

Lugupidamisega

/allkirjastatud digitaalselt/

Jüri Jõema
Tegevjuht