

Kriminaalmenetluse seadustiku, väärteomenetluse seadustiku, elektroonilise side seaduse ja teiste seaduste muutmise seaduse eelnõu seletuskirja juurde

Lisa

Märkuste arvestamise ja mitteamrvestamise tabel

Märkuse esitaja/märkuse sisu	Märkusega arvestamine/mitteamrvestamine
Andmekaitse Inspeksioon	
1. Seoses andmesubjekti õiguste piiramise regulatsiooni täpsustamise vajadusega jääme oma 16.09.2025 arvamuse nr 2.3-4/25/2674-2 punktis 1 toodu juurde. ESS §-ga 112 seonduvalt on jäänud täielikult tähelepanuta andmesubjekti õiguste piiramise osa (sõltuvalt menetluse liigist kas IKÜM art 23 lg 2 ja IKS § 24 lg 2). Kavandatav ESS § 111¹ lg 1 p 2 kohustab sideettevõtjad säilitama andmeid lisaks kohtueelsele menetlusele ka PPA ettekirjutuse alusel ehk sisuliselt haldusmenetluses. ESS § 112 lg 3 kohaselt säilitatakse järelepärimisi ja logifaile kaks aastat. Tehtud järelepärimiste õiguspärasuse tagamise ja nii järelepärimiste, järelepärimiste alusel antud teabe kui logifailide säilitamise kohustus on järelepärimise esitajal. Lahtiseks jääb olukord, kuidas ja mida peaks sideettevõtja vastama inimesele, kes teeb sideettevõtjale IKÜM art 15 taotluse, et saada teavet oma isikuandmete töötlemise kohta. Praktikas küsivad andmesubjektid välja ka logiandmeid, et veenduda oma isikuandmete töötlemise seaduslikkuses. Sideettevõtja on kohustatud selle teabe väljastama, kui puuduvad alused sellele teabele juurdepääsu piiramiseks. Mis omakorda tähendab seda, et juhul, kui selline andmesubjekti kaebus jõuab inspeksiooni menetlusse ja regulatsioon jääb selliseks nagu hetkel kavandatud, oleme sunnitud kohustama sideettevõtjaid logid väljastama. Sideettevõtjad koguvad ja säilitavad andmeid omal algatusel enda süsteemides ärilisel eesmärgil. Samuti peab sideettevõtja andmetöötlejana tagama oma süsteemide turvalisuse ja toiminguid niikuinii logima st sideettevõtja säilitab logisid muuhulgas ka enda poolt seatud eesmärkidel. Kavandatav ESS (ega ka praegu kehtiv redaktsioon) ei sätesta sideettevõtjale selget alust ja kohustust logisid (sisuliselt päringu toimumise fakti) salajas hoida. Ebaselge on ka see, kas sideettevõtja on enda süsteemis järelepärimisega seotud logisid pidades logide suhtes vastutav töötleja või volitatud töötleja ning kuivõrd saab sideettevõtja tugineda KrMS § 214 lg-le 1 kui asuda seisukohale, et sideettevõtja peaks olema siiski vastutav töötleja (selles osas on inspeksioonil halduskohtus pooleli ka üks kohtuvaidlus, kus see ongi segadust tekitanud).	ANTUD SELGITUS Nõustume märkusega, et isikute teavitamise regulatsioon ei ole hetkel täiesti selge. Samas rõhutame, et see ei ole ESS vaid eriseaduste, sh KrMS reguleerimisala küsimus ning teavitamine erinevatest päringutest ning isiku tutvustamine kogutud andmetega on horisontaalne küsimus ning ei puuduta ainult sideandmete päringuid. Seetõttu leiame, et vajalik oleks terviklik lahendus, samuti et need küsimused vajaksid eraldi arutelu ja vajadusel eraldi eelnõus käsitlemist.

	Seetõttu ongi vajalik õigusselguse ja andmesubjekti põhiõiguste tagamiseks eelnõus selgelt ja üheselt arusaadavalt reguleerida olukorrad juhuks, kus on vajalik andmesubjekti õigusi piirata.	
2.	Kavandatud ESS § 112 lg 1 sätestab, et sättes nimetatud järelepärimise sideettevõtjale võib teha kirjaliku lepingu alusel pideva elektroonilise ühenduse kaudu. Sama regulatsioon kehtib ka praegu, kuid siin tuleks täiendavalt täpsustada, et sõlmida tuleb mitte lihtsalt leping vaid just IKÜM art 28 lg 3 või IKS § 30 kohane leping. Seletuskirjas ei ole avatud, mis lepingut silmas on peetud. Sellise andmetöötluslepingu sõlmimise kohustus peaks olema seaduses täpsemalt reguleeritud, sest praegu pole selge, millises andmekaitseõiguslikus rollis sideettevõtja päringute vahendamise ja sellega kaasneva logimise vaates on st kas sideettevõtjat tuleks teatud andmetöötlustoimingute puhul käsitleda volitatud töötajana või vastutava töötajana. Sellise andmetöötluslepingu täpsem regulatsioon võimaldaks osaliselt lahendada ka eelmises punktis kirjeldatud olukorda.	ANTUD SELGITUS Vastavalt kehtivale õigusele võib sideettevõtjale esitada päringuid ning muuhulgas võib päringute esitamise ja nende vastamise tagada lepingu alusel pideva elektroonilise ühenduse kaudu. Eelnõu seda põhimõtet ei muuda. Samas leiame, et kuna eelnõuga muudetakse sideandmete säilitamise ning ka nende juurdepääsu, siis selles valguses vajavad ülevaatamist ka sõlmitud lepingud. Lisaks on vajalik hinnata, et kes on selle elektroonilise ühenduse vastutav töötaja.
Kaitsepolitseiamet		
1.	Kehtiva õiguse kohaselt käsitletakse sideandmete elektroonilise side seaduse (ESS) § 111 ¹ lõigetes 2 (telefon- ja mobiiltelefoni teenuse andmed) ja 3 (internetiühenduse ja elektronposti andmed) loetletud andmeid, mida sideettevõtjad peavad riigi jaoks säilitama. Rõhutame, et tegemist on side tehniliste ehk metaandmetega, mis kirjeldavad sideühenduse toimumist, mitte kõne, sõnumi või muu kommunikatsiooni sisu. Samuti ei tähenda nende andmete kasutamine reaajas jälgimist, vaid tegemist on nõ ajalooliste andmetega, mis võimaldavad analüüsida juba toimunud side sündmusi tagantjärele. Sideandmed hõlmavad muu hulgas: • infot selle kohta, kelle vahel side toimus (näiteks telefoninumbrid, IP-aadressid); • side alguse ja lõpu aega ning kestust; • kasutatud sidekanalit (kas tegemist on kõne, SMS, andmeside, internetiteenusega); • sidepidamiseks kasutatud seadme või ühenduse tehnilisi tunnuseid; • seadme või ühenduse ligikaudset asukohta side toimumise hetkel. Õigusselguse ja Euroopa Kohtu ning Riigikohtu praktika ühetaoliseks rakendamiseks on vaja selgelt eristada: a) lõppkasutaja tuvastamist võimaldavaid andmeid ehk subscriber data – lihtsustatult öeldes on tegemist lepinguliste andmetega, kust nähtuvad telefoni või internetiühenduse	ARVESTATUD Kasutatud terminoloogia on ühtlustatud. Euroopa Kohus on siinkohal öelnud (liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18) punkt 157 jj, et lausuline ja üldine andmete säilitamine on lubatud üksnes kasutaja identiteediga seotud andmete ulatuses helistaja tuvastamiseks.

	teenuse numbriga ja seadme omaniku andmed või muud tunnused; b) liiklusandmeid ehk traffic data – lihtsustatult öeldes on tegemist andmetega, kust nähtub, mis ajal konkreetne number helistas teisele numbrile; c) asukohaandmeid ehk location data – lihtsustatult öeldes on tegemist kärkeinfoga, kust selgub, millise mobiilimasti piirkonnas kõne alustati. Kui kehtiv ESS käsitleb sideandmetena ka lepingulisi andmeid ehk telefoninumbriga ja omanikku, siis Euroopa Kohus ei ole selliste andmete säilitamise ja kasutamise kohta etteheiteid teinud. Euroopa Kohus käsitleb üksnes liiklus- ja asukohaandmete säilitamist ja kasutamist. Seetõttu toetame eelnõuga kavandatud ESS §-s 111² sätestatud lõppkasutaja tuvastamiseks vajalike andmete eraldi reguleerimist, kuid vastav paragrahv peab võimaldama ka kõne või sõnumi vastuvõtja isikuandmete tuvastamist. Ei saa tekkida olukorda, kus pädev asutus saab õiguslikult tuvastada ainult helistaja telefoninumbri omanikku, kuid ei saa kontrollida, kellele kuulub kõnet või sõnumit vastuvõttev number. Samuti leiame, et ESS-is ja kriminaalmenetluse seadustikus (KrMS) tuleb sideandmete kontekstis kasutada ühesuguseid termineid. Kehtivas KrMS § 90¹ lõikes 1 ja eelnõus KrMS § 90¹ pealkirjas kasutatakse sõnastust „identifitseerimistunnustega seotud andmed“. Seevastu kavandatud ESS muudatustes on kasutusel „lõppkasutaja tuvastamiseks vajalikud andmed“. Olukorras, kus mõeldakse samu andmeid, tuleb terminid ühtlustada. Kaitsepolitseiameti ettepanek on kasutada „lõppkasutaja tuvastamiseks vajalikud andmed“.	
2.	Kaitsepolitseiamet on seisukohal, et Eesti Vabariigi põhiseaduse (PS) ja Euroopa Liidu aluslepingu artikli 4 lõikega 2 („riigi julgeoleku kaitse on iga liikmesriigi ainuvastutuses“) on kooskõlas sideoperaatorite poolt kõigi nende klientide ja teenuse kasutajate sideandmete (nii kliendi andmed kui liiklus- ja asukohaandmed) üldine ja ühetaoline säilitamine. Põhiõiguste kaitse kontekstis on oluline reguleerida nendele andmetele juurdepääs, sest üksnes sideandmete analüüsist on võimalik teha järeldusi isiku suhtluse kohta. Olukorras, kus sideandmeid säilitavad sideettevõtted enda süsteemides ja riigi poolt neid ei töödeldaks, on põhiõiguste riive minimaalne ning võimalike kuritarvituste vältimiseks peavad sideettevõtted järgima e-privatsuse direktiivis sätestatud nõudeid (direktiiv 2002/58/EÜ, artiklid 4–6, 9). Leiame, et Eesti Vabariigi iseseisvus, sõltumatus ja territoriaalne terviklikkus on ülekaalukad põhjendused, et tagada üldine ja ühetaoline sideandmete olemasolu. Euroopa Kohus on 2020. aasta lahendis La Quadrature du Net jt (C-511/18, C-512/18 ja C-520/18) leidnud, et riigi julgeoleku kaitse eesmärgil on kooskõlas seadusandlikud meetmed, kus	ARVESTATUD Täiendav alus sideandmete säilitamiseks riigi julgeoleku tagamise eesmärgil on eelnõu teksti lisatud. Siiski peame vajalikuks märkida, et kuna tegemist ajutise iseloomuga meetmega, siis ei peaks Vabariigi Valitsuse korralduse kehtivus olema kolm aastat ning piisaks ka lühemast tähtajast. Samuti märgime, et juhul kui tegemist ei ole lühiajalise kohustusega, siis ei saa seda anda korraldusega, vaid tuleb anda määrusega.

	elektroonilise side teenuse osutajatele tehakse ettekirjutus säilitada liiklus – ja asukohaandmeid üldiselt ja vahet tegemata olukordades, kus asjaomane liikmesriik seisab silmitsi riigi julgeolekut ähvardava suure ohuga, mis osutub tõeliseks ja vahetuks või ettearvatavaks (p 168). Taoline kohtu seisukoht ei arvesta aga Venemaa Föderatsiooni (VF) sõjalisest doktriinist tulenevate pikaajaliste eesmärkidega. Tuleb arvestada, et VF on varasemalt initsieerinud mitmeid mõjutustegevuse operatsioone (sh erinevad katsed mõjutada valimistulemusi) ja agressiooni rünnakuid (nt Gruusia 2008, Ukraina 2014), mis 24.02.2022 eskaleerus Ukrainas täiemahuliseks sõjategevuseks ja kestab jätkuvalt. Olukorras, kus VF on sõjaliselt rünnanud Ukrainat ja pannud toime erinevaid hübriidrünnakuid Euroopas, on äärmiselt oluline mõista, et VF-ist lähtuv oht on pikaajaline, kus kasutatakse erinevaid meetodeid oma eesmärkide saavutamiseks. Eesti julgeolekupoliitika alustes¹ on märgitud, et VF on Eestile ja Euroopale eksistentsiaalne oht. Kaitsepolitseiameti ülesanne on kaitsta Eesti põhiseaduslikku korda ja julgeolekut ning nende ülesannete täitmiseks on vaja tagada ühetaoline ja üldine sideandmete olemasolu. Igasugune muude kriteeriumite alusel, nt geograafilised piirkonnad, isikute või ametialade loetelude põhine andmete säilitamine läheb meie hinnangul vastuollu PS §-s 12 sätestatud võrdsuse põhimõttega. Ühtlasi annab nõ sihistatud või geograafiline säilitamine vaenulikule välisriigile võimaluse planeerida enda tegevusi selliselt, et nende tegevused ei jääks sideandmete säilitamise kohustuse alla. Juhul, kui seadusandja soov on loobuda seadusest tulenevast üldisest sideandmete säilitamiskohustusest ja kehtestada riigi julgeoleku eesmärgil andmete säilitamine Vabariigi Valitsuse korraldusega (eelnõu ESS § 111³), on kaitsepolitsei ettepanek sätestada vastava Vabariigi Valitsuse korralduse tähtajaks kaks aastat, mida on võimalik kahe aasta kaupa pikendada. Eesti julgeolekukeskkonda hindab kõige kõrgemal tasemel Riigikogu heakskiiduga dokument Eesti julgeolekupoliitika alused. Dokumendi julgeolekukeskkonna kirjeldus tugineb mh julgeolekuasutuste ohuhinnangutele, mida on viimastel aastatel koostatud kahe-kolme aastase välbaga. Meie hinnangul annab 2-aastane tähtaeg ka sideettevõtetele kindluse, et nad ei pea näiteks iga 3 või 6 kuu tagant tegema arendusi, mis on seotud andmete säilitamise ja mitte- säilitamise sisse-välja lülitamisega. Tuleb arvestada, et tekkinud kulud kantakse edasi riigile.	
3.	Kaitsepolitseiamet on seisukohal, et uurimisasutused ei tohiks sideandmete puhul kuritegevuse vastases võitluses sõltuda sideettevõtete ärielistest eesmärkidest. Tuleb arvestada, et sideettevõtete äriks ei ole andmete säilitamine, mistõttu seadusest tuleneva kohustuse puudumisel ei pruugita enam andmeid säilitada või säilitatakse oluliselt vähem andmeid ja	ARVESTATUD Täiendav alus sideandmete säilitamiseks raske kuritegevuse vastu võitlemise eesmärgil on eelnõu teksti lisatud.

lühema tähtaja jooksul. Samuti tuleb arvestada, et Eestis on kolm suuremat sideettevõtet, kelle peakontorid ei asu Eestis. Seadusest tuleneva andmete säilitamise kohustuse puudumine annab peakontoritele võimaluse kulude kokkuhoiu eesmärgil loobuda ärilistel eesmärkidel andmete säilitamisest. Samuti on oht, et erinevad ettevõtted säilitavad erinevaid andmeid ning erineva tähtaja jooksul. Taoline killustatud lahendus ei taga uurimisasutustele süütegude menetlemiseks ja tõendamiseks vajalikke andmeid. Seeläbi ei kannata mitte ainult kurjategijate tabamine, vaid kahjustada saavad ka kannatanute õigused, sest tulevikus võib teatud kuritegude lahendamine ja süüdlaste tabamine sõltuda sellest, millise sideettevõtte klient oli kahtlustatav ja/või kannatanu. Kaitsepolitseiameti hinnangul läheb taoline olukord vastuollu PS §-s 12 sätestatud võrdsuse põhimõttega. Seetõttu teeme ettepaneku kehtestada ESS-s ka kuritegevuse vastase võitluse eesmärgil sideandmete säilitamise kohustus. Raske kuritegevuse vastase võitluse eesmärgil andmete säilitamist võimaldavad ka Euroopa Kohtu otsused. Ka eelnevalt viidatud 2020. aasta lahendis La Quadrature du Net jt leidis kohus, et lubatud on: „seadusandlikud meetmed, mis näevad ette riigi julgeoleku kaitsmise, raskete kuritegude vastu võitlemise ja avalikku julgeolekut ähvardava suure ohu ennetamise eesmärgil liiklus- ja asukohaandmete eesmärgipärase säilitamise, mis on objektiivsete ja mittediskrimineerivate asjaolude alusel piiritletud vastavalt andmesubjektide kategooriatele või geograafilise kriteeriumi põhjal ja ajaliselt piiratud tingimata vajalikkuga, kuid mida on võimalik pikendada“ (p 168). Kaitsepolitseiamet on seisukohal, et raske kuritegevuse vastase võitluse eesmärgil tuleb liiklus- ja asukohaandmeid säilitada järgmiste kriteeriumite põhjal: 1) Eesti riigipiiri piirkonnas (kuni 10 km) ja saartel asuvate tugijaamade leviala andmed; 2) riigikaitseobjektide ja teatud elutähtsate teenuste osutajate piirkonnas asuvate tugijaamade leviala andmed; 3) kuritegevuse statistika alusel põhjendatud piirkonnas asuvate tugijaamade leviala andmed; 4) anonüümse ettemakstud kõnekaardi sideteenuse andmed; 5) välisriigi abonendi rändlusteenuse kasutaja andmed. Punktides 1–3 nimetatud kriteeriumid määratakse kindlaks Politsei- ja Piirivalveameti ja Kaitsepolitseiameti või siseministri ettepanekul Vabariigi Valitsuse poolt ning punktides 4 ja 5 nimetatud andmete puhul kehtib seadusest tulenev kohustus. Kaitsepolitseiameti hinnangul on raske kuritegevuse vastase võitluse eesmärgil sideandmete säilitamiseks ja kasutamiseks õigusliku aluse loomine suurema ühiskondliku hüvega kui näiteks eelnõus sätestatud andmete säilitamine konkreetse menetluse tarbeks (§ 111¹).	
---	--

4.	Arvamuse avaldamiseks saadetud eelnõu versioonis ei ole enam sätteid, mis reguleerisid, kellele peavad sideettevõtted andmeid edastama. Kuigi päringute õiguspärasuse eest vastutab päringu tegija, on õigusselguse huvides põhjendatud sätestada ESS-s asutused, kellele sideettevõtte peab andmeid avaldama. Pädevate asutuste välja toomine ESS-s annab sideettevõtetele selguse, kes ja mis seaduse kohaselt võivad neilt andmeid pärida. Samasugune põhimõte on kirjas krediitiasutuste seaduses (KAS § 88). Arvestades asutuste ülesandeid ja sideandmete olulisust nende ülesannete täitmisel, tuleks ESS-s kindlasti sätestada teabe andmise kohustus: 1) uurimisasutusele, järelevalveasutusele, prokuratuurile ja kohtule kriminaalmenetluse seadustiku kohaselt; 2) julgeolekuasutusele julgeolekuasutuste seaduses sätestatud ülesannete täitmiseks ning riigisaladuse ja salastatud välisteabe seaduses nimetatud julgeolekukontrolli teostamiseks; 3) kohtule kohtumenetlust reguleerivates seadustes ettenähtud juhtudel ja korras. Kokkuvõttes oleme seisukohal, et arvamuse avaldamiseks saadetud eelnõu vajab oluliselt muutmist ja täiendamist. Arvestades kohtupraktikast tulenevaid piiranguid sideandmete kasutamisele kriminaalmenetlustes on ennekõike vaja kiiret lahendust, et sideandmeid oleks võimalik tõendada kriminaalmenetlustes kasutada.	ARVESTATUD Eelnõus nähakse ette loetelu asutustest, kellele sideettevõtjad peavad andmeid esitama. Leiame, et julgeolekukontrolli teostamise alused vastav regulatsioon vajab tervikuna korrastamist. Seega, hetkel ei ole võimalik sellisel kujul andmete töötlemist toetada.
Riigikohus		
1.	KrMS § 90¹ pealkirja muutmise vajadus jääb arusaamatuks. Paragrahvi pealkirja kehtivas redaktsioonis nähakse ette andmete nõudmine sideettevõtjalt. Missuguseid andmeid selle sätte alusel nõuda saab, selgub sätte sisust, pealkirja koormamine konkreetsete andmeliikide nimetustega ei ole vajalik. Lisaks kõneldakse uue redaktsiooni pealkirjas „identifitseerimistunnustega seotud andmetest“, eelnõuga loodav ESS § 111² räägib aga „lõppkasutaja tuvastamiseks vajalikest andmetest“. Tarbetu segaduse vältimiseks peaks mõistekasutus erinevates seadustes olema järjepidev. Ekslik on eelnõu seletuskirjas (lk 5) väljendatud arusaam, et KrMS § 215 alusel saab menetleja esitada päringuid mingite „muude andmete“ – eelnõu konteksti arvestades ilmselt ikka sideandmete – osas, mis ei ole hõlmatud KrMS §-ga 90¹. KrMS §-d 32 ja 215 ei anna uurimisasutustele juurdepääsu andmetele, mille nõudmist ja väljastamist piiravad muud õigusnormid (vt nt RKKK 08.06.2026, 1-22-7314/268, p 22). Sideandmete kriminaalmenetluses tõendamise eesmärgil välja nõudmist reguleerib ammendavalt KrMS § 90¹.	ARVESTATUD Terminite kasutus on eelnõus ühtlustatud. Selgitame, et sideettevõtjal on lisaks otseselt sideteenuse osutamisel tekkivatele või loodavatele andmetele ka muid andmeid, millele juurdepääsu seadus ei piira. Seega leiame, et sellistele andmetele juurdepääs on jätkuvalt tagatud KrMS §-dega 32 ja 215.
2.	ESS-i praegu kehtiv redaktsioon ärilisel eesmärgil säilitatavate andmete mõistet ei sisalda, see termin on kasutusele võetud	ARVESTATUD

	kohtupraktika järgi. Eelnõus ja seletuskirjas kasutatakse vaheldumisi määratlusi „ärilisel eesmärgil töödeldavad andmed“ ja „ärilisel eesmärgil säilitatavad andmed“, selgitamata täpselt nende vahekorda ja võimalikku erinevust. Seaduse süstemaatikat järgides mõeldakse ärilisel eesmärgil säilitatavate (ja töödeldavate?) andmete all ilmselt ESS § 102 lg-s 1 nimetatud teavet. See, et menetleja saaks KrMS § 90¹ lg 2 alusel nõuda just ESS § 102 lg-s 1 loetletud andmeid, on võimalik järeldada ESS-ist viiteliselt erinevate sätete koosmõjus ja eelnõu seletuskirja abil. Seaduse kesksed mõisted tuleks hilisemate vaidluste vältimiseks defineerida siiski seaduses, kuna seletuskirjal ei ole seadusjõudu. Õeldut tuleks silmas pidada ka KrMS § 90¹ lg 2 muutmisel, kuna eelnõu tekstist jääb lõppastmes selgusetuks, missugust teavet selle normi alusel sideettevõtjalt ikkagi nõuda saab – kas üksnes ESS § 102 lg-s 1 loetletud andmeid või lisaks ka eelnõu kohases ESS § 111¹ lg 1 p-s 1 nimetatud ehk prokuratuuri määruse alusel säilitatavaid andmeid. Kui eelnõu jõustuks praeguses sõnastuses (välja saaks nõuda vaid ärilisel eesmärgil säilitatavaid andmeid), siis oleks välistatud ESS § 111 alusel säilitatud andmete väljanõudmine. Eelnõust ja seletuskirjast ei ole üheselt selge seegi, kas tegelik eesmärk on võimaldada KrMS § 90¹ lg 2 alusel välja nõuda ka ESS § 111¹ lg 2 p-de 2 ja 3 alusel (st seoses kõrgendatud või vahetu ohuga PPA või julgeolekuasutuse ettekirjutusel) säilitatavat teavet (vt ka allpool märkust eelnõu § 3 p 7 kohta). Kui KrMS § 90¹ lg 2 peaks sõnastatama nii, et välja saab nõuda just ESS § 111¹ lg 2 p 1 alusel säilitatavat teavet, siis tuleb teadvustada järgmist: juhul kui näiteks isikuvastase, riigivastase või üldohtliku kuriteo puhul on menetluse algjärgus palunud sideettevõtjalt andmete säilitamist PPA või julgeolekuasutus p-de 2 või 3 alusel ja mitte prokuratuur p 1 alusel ning andmete ärilisel eesmärgil säilitamise aeg on möödas, siis ei pruugi saada seda teavet hiljem kriminaalasjas tõendina kasutada. Normitehniliselt oleks korrektne lg 2 teine lause sõnastada sarnaselt KrMS teiste normidega (nt KrMS § 12 lg 2, § 55 lg 1, § 268 lg 2), kus kohtumenetluses esitatud taotluse või lahendatava küsimuse otsustab kohus poolte taotlusel või omal algatusel.	Eelnõud on täpsustatud ja teksti ühtlustatud. Päringuid on võimalik esitada nii ärilisel eesmärgil säilitatud andmete kui ka andmete kohta, mille osas seadus näeb ette säilitamise.
3.	Kehtiv VTMS § 31² lg 2 lubab vääртеomenetluses teha sideandmete <i>üksikpäringu</i> (ühe sideseansi andmed). Muudetud lõige eelnõus räägib üldiselt mistahes ärilisel eesmärgil säilitatavatest andmetest. Miks on plaanis kaotada üksikpäringu tingimus, seletuskirjast ei nähtu (vrd ESS § 1141: tsiviilkohtumenetluses üksikpäring jääb). VTMS § 31² lg 3 uus sõnastus säilitab küll vältimatu vajaduse nõude, aga asendab üksikpäringu kitsenduse vääртеo eest ettenähtud sanktsiooni ülemmääraga. Puudub igasugune selgitus ja mõjuanalüüs selle	ANTUD SELGITUS Eelnõud on täpsustatud ning välja on jäetud lävend, mis on seotud sanktsiooni ülemmääraga. Üksikpäringu nõue on jäetud välja, kuna praktikas on see osutunud liiga piiravaks.

	kohta, milline (sh kui ulatuslik) on pakutud muudatuse praktiline mõju sideandmete päringute tegemisele, vastavus tegelikule tõendamisvajadusele ning kooskõla EL õigusega.	Samas nähakse KrMS eeskujul ette ultima ratio nõue ning vajadus hinnata kohtu poolt päringu põhjendatust arvestades ühtlasi kõne all oleva väärteto laadi ja raskust.
3.	Eelnõus pakutud kujul ESS § 111² (lõppkasutaja tuvastamiseks vajalike andmete säilitamine) sätestamist on põhjendatud mh viitega RKKKo 1-24-4898 p-le 29. Siinkohal peame vajalikuks juhtida eelnõu väljatöötaja tähelepanu sellele, et Riigikohus väljendas nimetatud seisukohta konkreetse kriminaalasja tehiohusid arvestades. Kas igal konkreetsel juhul on tegu EK praktika mõttes üksnes lõppkasutaja identiteedi-, mitte tavapäraste liiklusandmetega, sõltub andmete olemusest, mahust jm kaasuse asjaoludest. Lisaks on EK praktika pidevas arengus, näiteks on sideettevõtjalt IP-aadresside küsimise ja süütoemenetluses kasutamise lubatavuse teemaga seotud pooleliolev eelotsusetaotlus asjas nr C-427/25 (Uffida). Loodava ESS §-ga 111³ nähakse ette andmete säilitamine riigi julgeoleku tagamise eesmärgil. ESS 111³ lg 6 sätestab, et selle paragrahvi alusel säilitatavaid andmeid võib (sideettevõtja?) avaldada üksnes julgeolekuasutusele julgeolekuasutuste seaduses sätestatud alustel ja korras. Eelnõu seletuskiri (lk 8) aga jätab lahtiseks, mida tähendab see, et ESS § 111³ alusel säilitatavad andmed on <i>eelkõige</i> seotud julgeolekuasutuste ülesannete täitmisega. Eelnõu ega seletuskiri ei anna selget vastust küsimusele, kas julgeolekuolekukaalutlustel säilitatavad sideandmed võivad jõuda tõendina kriminaalmenetlusse näiteks KrMS § 63 lg 1¹ kaudu. Samuti vajaks läbimõtlemist ja selgitamist ESS § 111³ lg 6 seos JAS §-ga 32.	ANTUD SELGITUS Käesoleva eelnõu puhul on lähtutud EL Kohtu praktikast, mille kohaselt on lubatud üldiselt ja ühetaoliselt säilitada lõppkasutaja tuvastamist võimaldavaid andmeid ning IP-aadresse (C-470/21). EL Kohus on muuhulgas oma otsustes ka öelnud, et juhul, kui andmeid on säilitatud riigi julgeoleku tagamise eesmärgil, siis nende kasutamine kuritegevuse vastu võitlemisel ei ole lubatud.
Prokuratuur		
1.	Küsimus selles, millisel moel on sideandmete kasutamine tõendina võimalik kriminaalmenetluses, on seadusandja valik. Prokuratuur toetab eelnõu edasist menetlemist, kuivõrd juba prokuratuurile kooskõlastamiseks edastatud eelnõus sätestatu lahendab olulisi menetluspraktikas tõusetunud vaidlusküsimusi. Siiski palume sideandmete tõendina kasutamise küsimuse reguleerimisel kaaluda ka küsimust, kas juba olemasoleva eelnõuga tuleks täiendavalt sätestada sideandmete säilitamise kohustus raske kuritegevuse vastaseks võitluseks. Nii võib olukord, kus kriminaalmenetluses saab tõendina kasutada vaid ärilisel eesmärgil säilitatud sideandmeid luua olulisi riske kuritegevuse vastaseks võitluseks ning tuua kaasa olukorra, kus raskete kuritegude osas tõendite kogumine on oluliselt raskendatud või koguni välistatud. Prokuratuurile teadaolevalt on näiteks Siseministeerium ning Politsei- ja Piirivalveamet kooskõlastamiseks saadetud eelnõu	ARVESTATUD Täiendav alus sideandmete säilitamiseks raske kuritegevuse vastu võitlemise eesmärgil on eelnõu teksti lisatud.

	väljatöötamisega seotud aruteludel pakkunud välja ESS §111³ sõnastuses, mis tagaks võimaluse säilitada sideandmeid raske kuritegevusega võitluse eesmärgil arvesse võttes KrMS §126² loetletud kuritegevuse kataloogi. Selliselt väljapakutud eelnõu sõnastuses nähakse ette võimalust säilitada selliste kuritegudega võitlemise eesmärgil sideandmeid geograafiliste piirkondade määramise põhimõttel ning Eestis rändlusteenust kasutavate abonentidega seotud andmete säilitamise läbi. Euroopa Kohtu lahendiga kooskõlas oleva aluse loomist sideandmete säilitamiseks raske kuritegevuse vastaseks võitluseks toetab ka prokuratuur. Alternatiivina eelnevale toetab prokuratuur ka eelnõus väljapakutud sideandmete kiirsäilitamise regulatsiooni loomist.	
2.	Prokuratuur juhib tähelepanu järgnevale. Eelnõus märgitu kohaselt muudetakse KrMS § 901 lg 2 järgnevalt: „Elektroonilise side teenuse osutamisega seotud ärilisel eesmärgil säilitatavate andmete, mida ei ole nimetatud käesoleva paragrahvi lõikes 1, kohta võib elektroonilise side ettevõtjale teha päringu kohtueelses menetluses prokuratuuri taotlusel ja eeluurimiskohtuniku loal. Kohtumenetluses võib vastava päringu teha kohus.”. Eelnõu väljatöötamise faasis oli kõnealune säte sõnastatud nii: „Elektroonilise side seaduses sätestatud andmeliiklusandmete kohta võib elektroonilise side ettevõtjale teha päringu kohtueelses menetluses prokuratuuri taotlusel ja eeluurimiskohtuniku loal. Kohtumenetluses võib vastava päringu teha kohus.” Nagu eelnevalt märgitud leiab prokuratuur, et ka käesoleva eelnõu jõustamise järel vajatakse jätkuvalt sideandmete säilitamiskohustuse kehtestamist kriminaalmenetluste tagamiseks. Seetõttu oleks otstarbekas ka KrMS § 90¹ lg 2 sõnastamine varasemalt väljapakutud sõnastuses. Samuti ei saa täielikult välistada võimalust, et ka KrMS §90¹ lg 2 tuginedes on vajalik tõendina kasutada selliseid sideandmeid, mida säilitatakse Euroopa Kohtu lahenditega lubatud piirides riigi poolt pandud säilitamiskohustuse alusel.	ARVESTATUD Eelnõu teksti sõnastust on muudetud.
3.	Prokuratuur peab vajalikuks tõstatada küsimuse ka selles, kas internetiteenuse osutamisega seotud sideandmete säilitamiskohustuse kitsendamine eelnõus väljapakutud viisil on põhjendatud. Mõistetavalt ei pruugi kõikide kõnealuste teenuste kohta andmete säilitamine olla käesoleval ajal tehnika arengu tõttu asjakohane. Eelnõus väljapakutud ESS § 111² lg 2 sõnastusest nähtub, et tulevikus säilitatakse internetiteenuse osutamisega seotud andmeid praegusega võrreldes märgatavalt üldisemas mahus. Eelnõus väljapakutud sõnastusega säilitatakse internetiteenusega seotud andmetena järgmiseid andmeid: 1. Kasutajatunnused	ANTUD SELGITUS Eelnõu näeb ette üldise ja ühetaolise säilitamiskohustuse lõppkasutaja tuvastamist võimaldavate andmete ning IP-aadresside osas. Kuna osa varasemalt ESS §-s 111¹ loetletud andmeid loetakse liiklusandmeteks, siis selles osas enam üldist ja ühetaolist säilitamiskohustust ei jää ning nende andmete säilitamine on

	2. Kliendi andmed koos temale side toimumise ajal eraldatud avaliku Interneti-protokolli aadressi ja lähtepordi, kasutajatunnuse või numbriga. Hetkel kehtiva ESS kohaselt kogutakse internetiteenusega seoses järgmiseid andmeid: „Interneti-seansi alguse ja lõpu kuupäev ning kellaaeg konkreetse ajavööndi järgi koos Interneti-protokolli aadressiga, mille on kasutajale eraldanud Interneti-teenuse osutaja, ja kasutajatunnusega“. On küsitav, kas viidatud kehtivas ESS loetletud andmete näol on tegemist selliste andmesideliikluse või asukohaandmetega, millede säilitamise Euroopa Kohtu praktika välistab. Küll ei nähtu väljapakutud eelnõu sõnastusest, kas ka tulevikus on internetiteenuse osutajalt võimalik saada kõiki kehtiva korra järgi säilitatavaid andmeid ning vastuseta jääb küsimus, kas eelnõuga pandav säilitamiskohustus võib kaasa tuua olukorra, kus internetiteenuse osutamisega seoses säilivad andmed nii üldistatud tasemel (nt internetiseansi täpse toimumisaja määratluseta), et selliste andmete kasutamiseväärtus on küsitav. Kui koos kasutajaandmetega säilitatakse säilitamiskohustuse raames ka nt internetiseansi aega määratleda aitavaid andmeid, ei saa tegemist olla aga selliste andmetega, mida saaks eelnõus väljapakutud sõnastuses kasutada tõendina kriminaalmenetluses, kuivõrd tegemist poleks siis mitte pelgalt ärilisel eesmärgil säilitatavate andmetega, vaid säilitamiskohustuse tõttu säilitatud teabega, mille kasutamiseks KrMS § 90¹ lg 2 väljapakutud sõnastuses volitust ei anna.	võimalik ESS-s sätestatud täiendavatel alustel. KrMS sõnastust on muudetud ning võimalik on kasutada nii ärilisel eesmärgil säilitatud andmeid kui ka andmeid, kus nähakse ette säilitamine.
4.	Eelnõus sätestatu kohaselt on võimalik julgeoleku tagamiseks andmeid säilitada kuni 6 kuud. Arvestades prokuratuuri menetluslikku kogemust riigi julgeolekuga seotud kuritegude menetlemisel leiab prokuratuur, et eelnõus väljapakutud aeg võib ka julgeoleku eesmärgil andmete säilitamiseks olla liiga lühike. Kehtiva regulatsiooni kohaselt säilitatakse sideandmeid ka julgeoleku tagamiseks vähemalt 12 kuud.	ARVESTATUD
Tarbijakaitse ja Tehnilise Järelevalve Amet		
1.	Eelnõuga planeeritakse muuta elektroonilise side seaduses (edaspidi ESS) sätestatud side teenuse kasutaja tuvastamiseks vajalikke andmete säilitamise ja väljastamise nõudeid. TTJA teostab ESS § 133 lg 1 kohaselt kehtestatud nõuete täitmise üle järelevalvet. Eeltoodud põhjusel peame oluliseks, et eelnõus kehtestatud nõuded (sh säilitamisele kuuluvate andmete loetelu) oleksid selged ja ühetaoliselt mõistetavad. Eelnõuga kavandatavas ESS §-s 111² loetletakse telefoni- ja mobiiltelefoniteenuse osutamisel säilitamisele kuuluvad andmed. ESS §-s 111² lg 1 p 1 kohaselt esineb säilitamiskohustus muu hulgas sõnumi edastajat või helistajat tuvastada võimaldavate andmete osas (sealhulgas kuulub säilitamisele sõnumi edastaja või helistaja ees- ja	ANTUD SELGITUS Leiame, et selguse huvides on vajalik eristada sõnumi saatjat ja helistajat, et tagada vastavus EL Kohtu praktikale, mis välistab vastuvõtja andmete säilitamise. Eesmärk on siiski lõppkasutaja tuvastamine, mitte konkreetse sõnumi saatja või helistaja isik.

	perekonnanimi, number, kasutajatunnus, elektronposti aadress või aadress). Leiame, et antud sõnastuse puhul on oluline tähele panna, et sõnumi edastajaks või helistajaks ei pruugi olla sideteenuse klient, kelle andmeid teenuseosutaja tavapäraselt töötleb. Helistaja isiku tuvastamine eeldaks kõne sisu (hääle või vestluse) töötlemist, mis ei näi olevat eelnõu eesmärk. Seetõttu teeme õigusselguse tagamiseks ettepaneku muuta ESS §-s 111² lg 1 p 1 sõnastust selliselt, et säilitamiskohustus oleks seotud telefoni- ja mobiiltelefoniteenuse klienti tuvastada võimaldavate andmetega.	
--	---	--

Eesti Infotehnoloogia ja Telekommunikatsiooni Liit

1.	Eelnõu on liiga keeruline ja praktikas raskesti ellu viidav: Eelnõu eesmärk on tagada Eesti õiguse kooskõla Euroopa Liidu õigusega ja leida tasakaal isikute privaatsusõiguse ja olulistel eesmärkidel sideandmete riigiasutuste poolt kasutamise vahel. Selleks on kavas loobuda senisest üldisest ja ühetaolisest säilitamiskohustusest ja sideandmete säilitamise ning väljastamise nõudeid vähendada. Kooskõlastamisele esitatud eelnõuga on liigutud vastupidisesse suunda: sellesse on sisse kirjutatud väga palju erinevaid ja uusi sideandmete säilitamise ja väljastamise aluseid, mida eelnõu varasemates versioonides ei olnud. See ei ole vastuvõetav lahendus ja lähenemisviis, kuna tähendab ühtlasi, et uue toimiva lahenduseni jõudmine võtab veel väga kaua aega. Niivõrd keeruka lähenemise ellu rakendamine kujuneks väga ressursimahukaks nii ajaliselt kui ka kulude vaatest. Eelnõu reguleerib elektroonilise side teenuse osutamisega seotud andmete säilitamist. Lõppkasutaja tuvastamise puhul eristatakse telefoni- ja mobiiltelefoniteenuse osutaja poolt säilitavaid andmeid ning internetiühenduse ja masinatevahelise side teenuse osutaja poolt säilitatavaid andmeid. Selgitame, et eelnõus pakutud erinevad kihilised sideandmete säilitamised on võimalikud vaid mobiilside teenuste puhul. Neid kohustusi ei ole võimalik täita fikseeritud sideteenuseid pakkudes. Ka senistes aruteludes on käsitletud vaid mobiilsideteenuseid. Seda eristust on väga oluline silmas pidada ning eelnõu tuleb sellest lähtudes üle vaadata. Oleme seisukohal, et Eesti riik vajab tekkinud olukorra lahendamiseks oluliselt kiiremat ja lihtsamat lahendust kui hetkel eelnõus ette nähtud, et sideandmeid oleks võimalik õiguspäraselt kriminaalmenetluses kasutada. Kui kehtestada kõik need erinevad säilitamise alused, mida eelnõu ette näeb ja mida on juurde pakutud, siis tegelikkuses põhjustame suured arendus- ja halduskulud ja suurendame halduskoormust, aga sideandmete säilitamine printsipi ei muutu oluliselt vähemaks.	ANTUD SELGITUS Eelnõu väljatöötamisel on lähtutud nii EL Kohtu kui ka Riigikohtu praktikast ning nende poolt seatud tingimustest. Kuna nimetatud kohtupraktika seab suhteliselt kitsad tingimused sideandmete säilitamise osas, siis peame nendest lähtuma ka seadusemuudatuste juures. Kuna senine üldine ja ühetaoline säilitamiskohustus ei ole lubatud, siis selle asemel oleme eelnõus ette näinud täiendavad alused sideandmete säilitamiseks, mis vastavad ühelt poolt kohtupraktikale ning teiselt poolt vajadustele tagada riigi julgeolek ning võidelda raske kuritegevuse vastu. Eelnõus sätestatud säilitamiskohustus saab kehtida vaid andmete osas, mis sideettevõtjatel on olemas. Nõustume, et eelnõus sätestatud säilitamiskohustusega kaasnevad täiendavad kulud. Sellega seoses nähakse eelnõus ka ette, et sihistatud säilitamisega seonduvad kulud kaetakse riigieelarvest.
----	--	--

2.	Peame kõige olulisemaks, et Eesti sideandmete uus regulatsioon vastaks järgmistele tingimustele: Õigusselgus: oluline on ennetada edasisi vaidluseid. See eeldab seaduses konkreetsete ja lihtsate säilitusnõuete fikseerimist ja seejärel põhjalikku põhiõiguste analüüsimist, mida antud juhul tehtud ei ole; Tehniliselt lihtsalt ja käesoleva aasta jooksul teostatav: tehnilise lihtsuse all mõtleme ka seda, et lahendus on selgete ja lihtsate andmekategooriate põhine ja automatiseeritult realiseeritav. Väga oluline on arvestada, et kõik nõuded sideettevõtja poolt sideandmete säilitamise (sh atribuutide loetelu) ja väljastamise osas peavad olema selgelt seaduses või äärmisel juhul seaduse rakendusaktides kirjeldatud. On mõeldamatu ja lubamatu panna sideettevõtjaid nõ kohtuniku rolli ehk olukorda, milles nad peaksid asuma hindama uurimis- või julgeolekuasutuste tegevuse ja taotluste õiguspärasust või proportsionaalsust. Põhjendamatut halduskoormust vältiv: lahenduse ellu viimine ja selle edasine haldamine ei tohi olla liiga keeruline ja ressursimahukas, olgu siis rahalises või ajalises plaanis. Sideettevõtja tegevuse eesmärk ei ole uurimis- ja jälitusasutustele andmete säilitamine või andmetöötlusteenuse pakkumine. Seetõttu ei tohi sideettevõtjatele pandavad kohustused olla ülemäära koormavad ega tehniliselt keerulised ning kulukad rakendada. Kui eelnõuga lisatakse koormavad kohustused, tuleb nende täitmine ettevõtetele riigi poolt hüvitada; Range kontroll uurimisasutuste tegevuste üle, kuna vajalik on taastada ühiskonna usaldus. Märkime, et ei saa tekitada ootust, et eraõiguslikud sideettevõtjad oleksid nõ kontrollorganiks uurimis- ja jälitusasutuste tegevuse osas. Vastavad ranged kontrollmehhanismid peab uurimis- ja jälitusasutuste suhtes nende poolt sideandmete pärimise ja kasutamise osas kehtestama ja ka seadusesse sõnaselgelt kirja panema riik. Hetkel neid selles eelnõus ei sisaldu ja juba ainuüksi seetõttu on see eelnõu poolik ja sellega ei saa edasi liikuda.	ANTUD SELGITUS Eelnõu näeb ette senisest erinevad sideandmete säilitamise alused, mis vastavad kohtupraktikale. Seeläbi tagatakse ühelt poolt andmete säilitamise õiguspärasus ning teiselt poolt pädevate asutuste juurdepääs ning võimalus andmeid kasutada, sealhulgas süüteo menetluse eesmärkidel. Seaduses nähakse ette selged alused andmete säilitamiseks ning detailsed andmekategooriad täpsustatakse hiljem Vabariigi Valitsuse määrusega. Samuti nähakse ette senisest tõhusam järelevalve sideandmete päringute üle. Eelnõuga nähakse ette erinevad alused sideandmete säilitamiseks. Sihistatud säilitamise kui senisega võrreldes uue ja keerukama lahenduse puhul näeb eelnõu ette ka kulude hüvitamise.
3.	Leida lahendus, kus seadus sätestab konkreetse kohustuse menetluste jaoks sideandmeid säilitada koos konkreetse tähtaja või tähtaegadega ning näeb ette erineva andmete väljastamise korra erinevateks menetlusteks ehk reguleeritakse peamiselt sideandmete väljastamist ja kasutamist.	ANTUD SELGITUS Eelnõus nähakse ette võimalus andmete kiirsäilitamiseks juhuks, kui on alust arvata, et vastasel juhul võidakse need kustutada. Muuhulgas on selline meede nähtud ette nii Euroopa Nõukogu küberkuritegevusvastases konventsioonis kui ka EL e-tõendite määruhes.
4.	Kui punktis 2.1 pakutud lahendus tõesti mitte kuidagi teostatav ei ole, siis on alternatiiviks minna tagasi eelnõu versiooni	ANTUD SELGITUS

	juurde, kus tunnistatakse kehtetuks ainult elektroonilise side seadise § 111¹ lg 2 ehk kriminaalmenetluste jaoks jäävad selles lõikes nimetatud andmed kättesaadavaks ainult juhul, kui need on sideettevõtja poolt äriliselt säilitatud.	Eelnõu autorite hinnangul ei pruugi üksnes ärilisel eesmärgil säilitatud andmed olla piisavad, sealhulgas riigi julgeoleku tagamisel ning raske kuritegevuse vastu võitlemisel. Sellel põhjusel nähakse eelnõus ette ka eraldi täiendavad alused sideandmete säilitamiseks.
5.	ESS § 111¹ - Andmete säilitamine konkreetse menetluse tarbeks (nn quick freeze) Meile jääb eelnõus välja pakutud kiirsäilitamise ehk quick freeze lahenduse vajadus arusaamatuks. Arutelude käigus on meile teadaolevalt ka ilmnunud, et see ei ole ühegi osapoole päris vajadus, kuna see leiaks kasutust vaid üksikutel juhtudel. Pakutud lahendus ei ole mõistlik. See tekitab peamiselt käsitööna lahendatava protsessi, mis ei ole proportsionaalne sellise säilitusviisi puhul saadava kasuga. Leiame, et sideettevõtted ei pea osutama riigile jälitusandmete säilitamise teenust. Paralleelselt säilitatud andmed (just sellise kohustuse see nõue tekitab) võivad suurendada andmekaitse ja andmeturbe riske ja sellise kohustuse kehtestamine ei oleks kooskõlas andmekaitse minimaalsuse põhimõttega. Säte tekitab palju küsimusi, mis muudavad sellise kohustuse kehtestamise enam kui küsitavaks: Näiteks kuidas saab vahetut ohtu tõrjuda 6 kuud hiljem? Miks on vaja julgeoleku jaoks seda alust ka, kui julgeoleku jaoks andmed säilitatakse teiste sätete alusel niigi? Lisaks tekib küsimus, kuidas saab quick freeze aidata ohtude ennetamisel ja tõrjumisel, kuivõrd sündmused, mis sellise säilitusviisi praktikas käivitaks, pole veel esinenud. Praktikas oleks selline sideandmete säilitamine võimalik meie hinnangul üksnes kriminaalmenetluses tagantjärele tõendite kogumiseks ja kuriteo uurimiseks (§ 111¹ lg 1 p 1). Säte on ebamõistlik ka seetõttu, et eelnõuga jääb alles mitmeid teisi sideandmete säilitamise aluseid. Selline erandkorras kiirsäilitamise alus võiks ehk olla põhjendatud olukorras, kus seaduses pole ühtegi kohustust sideandmeid säilitada ning uurimis- ja julgeolekuasutuste ainuke võimalus menetluses sideandmeid kasutada oleks juhul, kui sideettevõtetel on need muudel õiguslikel alustel olemas. Eelnõuga on kavandatud mitu muud alust ehk sellist erakorralist vajadust, mille puhul kiirsäilitamisest päriselt abi oleks, ei paista. Ka Euroopa Liidu teiste riikide praktika kinnitab, et kiirsäilitamise nõue on praktikas kasutusel üksnes siis, kui kõik muud seadusest tulenevad sideandmete säilitamisalused on kehtetuks tunnistatud. Eestis me ei näe, et selline olukord saaks lähiaastatel tekkida, sest meie julgeolekuolukorras ei oleks	ANTUD SELGITUS Eelnõus nähakse ette võimalus andmete kiirsäilitamiseks juhuks, kui on alust arvata, et vastasel juhul võidakse need kustutada. Tegemist on täiendava võimaluse tagamaks ärilisel eesmärgil säilitatavate andmete olemasolu ning vältida nende kustutamist sideettevõtjate poolt. Tegemist on tõendite tagamise meetmega, mille eesmärk on kindlustada andmete olemasolu vastava hilisema päringu tegemise hetkel. Lisaks märgime, et käesolev andmete kiirsäilitamine puudutab üksnes säilitamise hetkel olemasolevaid andmeid ning see ei tähenda tulevikus tekkida võivate andmete kogumist ja säilitamist. Muuhulgas on selline meede nähtud ette nii Euroopa Nõukogu küberkuritegevusvastases konventsioonis kui ka EL e-tõendite määruses.

	mõistlik loobuda julgeolekuotstarbelisest konkreetse tähtajaga säilitamismõudest. Kui selline kohustus kehtestatakse, siis tuleb hüvitada sideettevõtjatele selle uue nõudega kaasnevad kulud. Tegemist oleks praktikas käsitööna elluviidava lahendusega. See tähendab, et sideettevõttes peavad olema töötajad, kes on valmis reageerima kiirsäilitamise korralduse saamisel ning korraldama taotletud andmete säilitamise. Kuna korraldus võib tulla 24/7 eeldab see vahetustega tööd või valveaega. Tuleb märkida, et kuna etteulatuvalt ei oska keegi hinnata, kui palju neid päringuid oleks, ei tule kõne alla ka kohene automaatse lahenduse arendamine. Pigem oleks vähemalt mõnda aega tegu käsitööga ning alles mõne aasta pärast saaks praktika põhjal kaaluda, kas on mõistlik ja tehniliselt võimalik midagi automatiseerida ja millised kulud ses osas tekivad. Kui selline kohustus kehtestaks, siis on oluline, et säilitatavate sideandmete kategooriad ehk andmete kataloog on ette teada. Iga asutus ei saa pöörduda sideettevõtte poole erineva nimekirjaga, milliseid andmeid tal vaja on. Samuti ei ole andmekaitsemõuetega (minimaalsusprintsip, eesmärgipärasus jt) kooskõlas see, et sideettevõtja säilitab kõik, mis tal on, vaid säilitama peaks seda, mida uurimisasutusel uurimiseks vaja on. Vastasel juhul võib osutuda, et soovitu on tehniliselt teostamatu. Oluline on eelnõus ka rõhutada, et säilitatakse vaid neid andmeid, mis on olemas ehk andmeid juurde ei tekitata. See tähendab ka, et kiirsäilitamine saab olla vaid olukorra fikseerimine mingil kindlal ajahetkel. Näiteks et palutakse säilitada ühe tugimasti viimase ööpäeva andmed kuueks kuuks ehk tõsta need n-ö eraldi riiulile. See tähendab, et anda ei saa korraldust säilitada ühe tugimasti andmeid järgnevat kuus kuud ehk kõik andmed mis kuue kuu jooksul korralduse andmisest alates tekivad. Seega ükski selles osas antav korraldus ei saa olla tulevikku vaatav, vaid ainult korralduse väljastamise hetkel olemasolevate andmete säilitamine. Ettepanek: kustutada eelnõust ESS § 111¹	
6.	ESS § 111⁴ lg 4 julgeoleku tagamise eesmärgil andmete säilitamine Sättes sisalduv 6 kuud on väga lühike tähtaeg ja jääb arusaamatuks: Seletuskirja kohaselt põhineb antud sätte alusel antav korraldus 4 aasta vältel uuendataval ohuhinnangul. On ilmselge, et agressorriigi kõrval paiknedes ei muutu ohuolukord nii lühikese aja nagu 6 kuu jooksul. Nii lühike tähtaeg põhjustab sideettevõtetele halduskoormust ja kulusid. Kuuekuulise etteteatamisega muudatused (nt geograafiliste piirangute muutumine, hüpoteetiliselt mitte-säilitamise perioodil uuesti säilitama hakkamine vms) tekitaks olulist koormust, mis ei ole selgelt ettenähtavad (nt arendusvajadus ja ettevõtte enda arendusprioriteedid, inimressursi küsimused). Samas ei näe eelnõu selleks ette leevendavaid meetmeid sideettevõtjatele (nt kulude hüvitamist). Halduskoormus on märksa väiksem juhul,	ANTUD SELGITUS Eelnõud on täpsustatud ning välja on jäetud sihistatud säilitamine geograafiliste piirkondade kaupa. Arvestades asjaolu, et tegemist on nõ ajutise meetmega andmete säilitamiseks, siis ei ole võimalik ette näha Vabariigi Valitsuse korralduse kehtivust väga pika aja jooksul. Leiame, et optimaalne tähtaeg võiks siin olla 1 aasta.

	kui algselt anda pikem tähtaeg koos võimalusega seda lühendada olukorras, kui julgeolekuolukord ootamatult paraneb ja langeb ära vajadus julgeoleku huvides vastavaid andmeid säilitada. Leiame, et Eesti Vabariigi väiksust arvesse võttes on julgeolekuolukord ja ohuhinnang kogu riigis ühesugune, mistõttu pole asukohapõhine sideandmete säilitamine julgeoleku eesmärkidel kuidagi põhjendatud ega asjakohane ja vajab välistamist. Ettepanek: sätestada julgeoleku tagamise eesmärgil andmete säilitamise korralduse ülevaatamine 2 aasta tagant ning jätta sättest välja geograafiline sihistamine ehk võtta välja § 111³ lg 5 punktis 3 hõlmatud isikute ring ning piirkond.	
7.	Siseministeeriumi ettepanek: lisada eelnõusse andmete säilitamine raske kuritegevuse vastase võitluse eesmärgil ITL ei toeta eraldi aluse lisamist andmete säilitamiseks raske kuritegevuse vastase võitluse eesmärgil pakutud kujul. Mitme eraldi aluse lisamine on väga keeruline ja aeganõudev lahenduses olukorras, mis vajab kiiret ja lihtsat lahendust. Juhul, kui Justiits- ja Digiministeerium otsustab Siseministeeriumi palutud eraldi aluse lisada, siis teeme järgmised ettepanekud: Jätta eelnõust välja nn kiirsäilitamise alus. Neid mõlemaid koos pole vaja. Täpsustada Vabariigi Valitsuse korraldusega kõik piirkonnad, kus tuleb sideandmeid säilitada, s.h kaugus riigipiirist. Määratleda geograafilised alad maakonna täpsusega. Geograafiliselt sihistatud säilitamine on tehniliselt võimalik vaid tugijaama aadressi põhisel. Seega õigusnormiga saab öelda ette, millises geograafilises piirkonnas (nt maakonnas) asuvate tugijaamade andmed tuleb säilitada. Geograafiliselt sihistatud säilitamisel tuleb arvestada, et tugijaamades tekib vaid kärjeinfo ehk muid andmeid (nt kõneeristust) nii ei teki. Jätta eelnõust välja eraldi sideandmete säilitamine anonüümse ettemakstud kõnekaardi mobiiltelefoniteenuse ja välisriigi abonendi rändlusteenuse kasutaja mobiiltelefoniteenuse puhul: Ettemakstud kõnekaardi andmete säilitamine ei ole tehniliselt täna teostatav, kuna tugijaamade mõttes on tegu mobiiltelefoniteenuse kasutajaga. Tugijaamas ei eristata, kas tegemist on ettemakstud kõnekaardi või lepingulise kliendiga. Selline eristamine eeldaks täiendavaid andmetöötlustegevusi puhtalt kriminaalmenetluse jaoks andmete säilitamiseks ehk lisatööd. Samuti on tegemist praktikas muutuva teguriga, kuna kõnekaardilt minnakse üle lepingule ja vastupidi, kuid number jääb samaks. Tehniliselt probleemne on ka välisriigi rändlusteenuse kasutajate sideliikluse eristamine selle säilitamiseks.	ANTUD SELGITUS Sideandmete säilitamine raske kuritegevuse vastu võitlemise eesmärgil on eelnõusse lisatud. Eelnõu kohaselt nähakse ette sihistatud säilitamine geograafiliste piirkondade alusel, mis määratletakse osaliselt seaduse ning osaliselt määruse tasandil. Lisaks on meie hinnangul põhjendatud ja vajalik säilitada andmeid anonüümsete ettemakstud kõnekaartide ning Eestis rändlusteenuse kasutajate kohta. Oleme kursis, et nimetatud lahenduse teostamisega kaasnevad kulud ning eelnõu kohaselt need hüvitatakse.

	Peame neid mõlemaid aluseid ka andmekaitse reeglite vaatest põhjendamatuteks ja kasutajaid alusetult diskrimineerivateks, kuna meie hinnangul ei ole õige eeldada, et nimetatud teenuseid kasutavad isikud on teistest kriminaalsemad. Selle kohta puudub meie teada igasugune statistika. Jätta eelnõust välja ka konkreetsete objektide põhine sideandmete säilitamine, kuna see on liiga keeruline. Oluline on arvestada, et tugijaamade asukohad on muutumises. Seega meie hinnangul on geograafiline sihistamine teostatav vaid tugijaamade aadresside põhisel maakondade lõikes (lisaks vajadusel riigipiiri lähistel). Lisada eelnõusse kulude hüvitamine sideettevõtetele, kuna raske kuritegevuse vastase võitlus eesmärgil eraldi geograafiliselt sihistatult andmete säilitamine eeldab tehnilist arendust ning hilisemaid jooksvaid kulusid.	
8.	ESS § 111² lg 3 ja § 111⁴ lg 3 sisalduvad andmekaitse lisanõuded sideettevõtetele. Leiame, et need nõuded on põhjendamatud. Näiteks ei ole õigustatud piirata seadusega eesmärki, milleks sideettevõtte ise võib sideandmeid kasutada. Sideettevõtja säilitab ja töötleb andmeid enda lõppkasutaja tuvastamiseks oma ärielistel eesmärkidel vastavalt EL-i andmekaitse üldmääruses ja e-privatsuse direktiivis toodud nõuetele. Sellised piirangud saavad kõne alla tulla ja peavad olema seaduses sees hoopis uurimisasutuste tegevuse suhtes. Hetkel uurimisasutuste suhtes vastavaid piiranguid eelnõus pole ja see on antud eelnõu olemuslik ning oluline puudus. Juhul, kui sellised piirangud seada, peaksid need paiknema kriminaalmenetluse seadustikus, kuna reguleerivad üldiselt uurimisasutuste tegevusi, mitte sideettevõtja omi. Ei ole arusaadav ega õiguspärane põhjendatud, miks peaks elektroonilise side seaduses lisama sideettevõtjale sellise piirangu ja kitsendama ettevõtja kui vastutava töötaja enda õigust otsustada, millisel viisil teenuse käigus tekkinud andmed on vajalikud. Sellise piirangu lisamist ei ole selgitatud ka seletuskirjas. Samuti on arusaamatu ja põhjendamatult § 111⁴ lg 3 p 2 sisalduv kohustus. Ka selle kohustuse kehtestamist ei ole seletuskirjas käsitletud. Ettepanek: Kustutada ESS § 111² lg 3 ja § 111⁴ lg 3 p 2. Tegemist on kriitiliselt tähtsa muudatusega ja ilma selleta on eelnõuga edasi liikumine mõeldamatu.	ANTUD SELGITUS Eelnõu ei piira sideettevõtja andmete kasutamist, mida ta on säilitanud oma ärielistel eesmärkidel. Eelnõu piirab nende sideandmete kasutamist, mida ta on säilitanud tulenevalt riigi poolt pandud kohustusest.
9.	ESS § 111² lg 1 p 7 - Anonüümsete kõnekaartide isikuandmed jääb arusaamatuks, miks nõutakse anonüümsete ettemakstud kõnekaartide puhul teenuse lõppkasutaja isikuandmeid. Kui tegu on anonüümse kõnekaardiga, siis selliseid andmeid sideettevõtjal ei ole.	ANTUD SELGITUS Eelnõus lähtutakse andmete säilitamise kohustuse panemisel põhimõttest, et säilitada saab andmeid, mis sideettevõtjal on olemas ehk mis tekivad või

	Lisaks on see säte vastuolus põhimõttega, mille kohaselt tuleb andmeid väljastada siis, kui need on teenuse osutamisel tekkinud ehk sideettevõttel olemas. Ettepanek: kustutada ESS § 111² lg 1 punktist 7 lõppkasutaja isikuandmed.	luuakse sideteenuse osutamise käigus. Juhul, kui sideettevõtjal on olemas andmeid, mis aitab tuvastada ettemakstud kõnekaardi kasutajat, siis neid andmeid on ta kohustatud säilitama.
10.	Sideandmete väljastamist täpsustav säte ESS-is EL e-privaatsuse direktiiv (EPD) on eriseadus võrreldes muude isikuandmete kaitse normidega ning on näinud ette sideandmetele kõrgendatud kaitse. Täpsemini loetleb EPD artikkel 15 ka, millistel alustel /eesmärkidel on liikmesriigil õigus seaduses sätestada sideandmete konfidentsiaalsuse rikkumise lubamine. Seetõttu on vajalik ESS'is sätestada lisaks muudes seadustes sätestatud üldisele andmete nõudmise õigusele konkreetne alus sideettevõtjatele andmete väljastamiseks (antud küsimuses siis julgeoleku, kriminaalmenetluse ja väärteomenetluse, maksumenetluse ja kohtumenetluse juhtudel). Kui sellist piirangut ei ole, siis võiksid sideandmeid nõuda ka kõik kohtutäiturid, pankrotihaldurid, kindlustusandjad jt, kellel on nende ülesannete täitmiseks seaduses antud üldine õigus andmeid kolmandalt isikult nõuda, kuid kelle tegevus kindlasti ei eelda sideandmete kasutamist (sh võttes arvesse ka sideandmete säilitamist ja kasutamist puudutavaid kohtulahendeid). Taolistel eesmärkidel ja menetlustes oleks sideandmete töötlemine päringu esitaja poolt meie hinnangul ebaproportsionaalne riive isikute põhiõigustele. Need juhtumid on ka praegu praktikas olemas ja sideettevõtja peab selgitama, et sideandmete väljastamisele kehtivad erireeglid. Ettepanek: sätestada samasugune loetelu asutustest, kellele sideettevõtja on kohustatud andmeid väljastama, nagu see on kirjas täna kehtivas ESS § 111' lõikes 11. Tulevikku vaatavalt peame oluliseks, et see loetelu vaadatakse üle ning seda isikute ringi kitsendatakse, et tagada sideandmete väljastamise kooskõla Euroopa Kohtu praktikaga.	ARVESTATUD
11.	Eelnõu jõustumisaeg Eelnõu jõustumisaeg 1.11.26 oli sobiv lahendus üksnes eeldusel, kui eelnõu oleks vastu võetud enne käesoleva aasta suve ning eelmises eelnõu versioonis sätestatud vormis, mis eeldas sideettevõtjatelt oluliselt vähem muudatusi. ITL-i ettepanek on jõustada väiksemad muudatused 9 kuu möödumisel alates eelnõu vastuvõtmisest ja Riigi Teatajas avaldamisest. Suuremate muudatuste puhul on vaja ülemineku aega vähemalt 1,5 aastat, kuna muudatused eeldavad analüüsimist ja arendamist. Ei saa tekitada olukorda, kus lühikese seaduse jõustumisaja tõttu on sideettevõtjad sunnitud peatama enda põhitegevusega seotud kriitilised arendused, et	ARVESTATUD Eelnõu jõustumistähtaegu on korrigeeritud. Vajadusel tuleb need hiljem Riigikogu menetluses üle vaadata.

	ellu viia uute säilitamismõuete rakendamine ja seda seejuures olukorras, milles riik on vastavate seadusemuudatuste tegemist seni aastaid edasi lükanud. Üldkorras võib jõustuda üksnes nn julgeolekuerandit puudutav säte, mis annaks võimaluse ka selle muudatuse rakendamist ette valmistada.	
12.	Ettepanekud seletuskirja osas Lisada kiirsäilitamise osas on eelnõu seletuskirja põhiseadusele vastavuse analüüs. Eemaldada eelnõu seletuskirjast ekslikud väited, nagu ei tooks kiirsäilitamise aluse lisamine kaasa olulist halduskoormuse kasvu. Oluliselt on vajalik täiendada seletuskirjas ka muus osas mõju sideettevõtjatele. Hetkel ei kajastu seletuskirjas kõikide eelnõus sisalduvate säilitamise aluste mõjud ja neid ei ole isegi analüüsitud. Kui need uued täiendavad alused ja koormavad lisakohustused peaksid sideettevõtjate suhtes sisse jääma kas või osaliselt, siis ei ole õige ja on olulises ulatuses eksitav seletuskirja lk 2 sisalduv väide: „Sideettevõtjate jaoks halduskoormus andmete säilitamise osas oluliselt ei suurene. Kaasneb ühekordne halduskoormus seoses uue regulatsiooni jõustamiseks vajalike muudatuste teostamisega. Kui eeldada, et iga-aastane päringute maht jääb samasse suurusjärku võrreldes senisega ja võrreldes senisega ei muutu koormavamaks ka päringutele vastamise ja nende tegemise viis, on vastav halduskoormuse kasv ajutine.“ Halduskoormus ei ole sel juhul ajutiselt suurem, vaid püsivalt.	ARVESTATUD Eelnõu seletuskirja on täiendatud. Antud selgitused andmete kiirsäilitamise, samuti kulude tekkimise ning kulude hüvitamise osas.
Eesti Advokatuur		
1.	Eelnõu on võrreldes varasemate versioonidega küll paranenud, kuid tekitab jätkuvalt mitmeid olulisi õiguslikke ja sisulisi küsimusi. Need puudutavad eelkõige säilitamiskohustuste ulatust, kohaldamise lävendeid, sõltumatu kontrolli olemasolu ning regulatsiooni kooskõla Euroopa Liidu õigusega. Positiivsena tuleb esile tõsta loobumist varasemast üldisest sideandmete säilitamiskohustusest ning liikumist lahenduse poole, kus riik kasutab eelkõige andmeid, mida sideettevõtjad juba oma tegevuse käigus töötlevad ja säilitavad. See lähenemine vähendab võrreldes varasema regulatsiooniga põhiõiguste riive ulatust ning arvestab paremini Euroopa Kohtu praktikast tulenevaid nõudeid. Samas jääb eelnõu mitmes keskse tähtsusega küsimuses probleemseks. Esiteks on mitmed säilitamiskohustuste ja andmete kasutamise aluseks olevad lävendid liiga madalad ega piirdu piisavalt selgelt raske kuritegevuse või tõsiste julgeolekuohtudega. Teiseks on korrakaitsetelised eesmärgid määratletud liiga laialt, võimaldades meetmete kohaldamist ka olukordades, mis ei õigusta nii intensiivset põhiõiguste riivet.	ANTUD SELGITUS Eelnõu vastab EL Kohtu praktikale, sealhulgas säilitamise aluste ja tagatiste osas. Eelnõu teksti on täpsustatud.

	Kolmandaks ei taga eelnõu piisavat sõltumatut eelkontrolli ning riigi julgeoleku erand ei ole piisavalt selgelt piiritletud. Nende puuduste tõttu tekivad tõsised küsimused regulatsiooni vastavuse kohta Euroopa Kohtu väljakujunenud praktikale.	
2.	Rõhutame, et Euroopa Kohtu praktikast tulenevad väga selged piirid sideandmete säilitamisele ja kasutamisele. Üldine ja vahet tegemata säilitamine on lubatav üksnes erandina riigi julgeoleku kaitseks olukorras, kus esineb tõeline, tõsine ja ettearvatav oht, ning sedagi ajutiselt ja rangete tingimuste alusel (vt liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18, La Quadrature du Net jt.). Lisaks peab selline meede alluma kohtu või sellega võrdsustatud sõltumatu asutuse eelkontrollile. Samuti on Euroopa Kohus rõhutanud, et liiklus- ja asukohaandmetele juurdepääsu saab õigustada üksnes võitluses raskete kuritegude vastu või avalikku julgeolekut ähvardava suure ohu ennetamisel ning see peab üldjuhul puudutama konkreetseid isikuid (C-746/18, H.K vs Prokuratuur). Sellest lähtuvalt on problemaatiline eelnõus sisalduv lahendus, mille kohaselt saab riigi julgeoleku huvides lausalise sideandmete kogumise otsustada Vabariigi Valitsus. Euroopa Kohtu praktika kohaselt (liidetud kohtuasjad C-511/18, C-512/18 ja C-520/18, La Quadrature du Net jt) peab sellise otsuse tegema kohus või sõltumatu haldusorgan, milleks Vabariigi Valitsus kui täidesaatva võimu organ ei kvalifitseeru. Samuti on küsitav eelnõus sätestatud madal lävend („ohu ennetamine“) ning võimalus pikendada meetmete kohaldamist, mis võib viia erandi muutumiseni sisuliselt reegliks. Ka kuuekuuline periood on ebaproportsionaalselt pikk, eriti arvestades, et kriminaalmenetluses, kus uuritakse juba konkreetseid kahtlustusi, on jälituslubade kestus märkimisväärselt lühem. Sihistatud säilitamise regulatsioon ESS § 111¹ alusel tekitab täiendavaid probleeme. Eelnõu võimaldab andmete säilitamist mitte ainult kriminaalmenetluse, vaid ka korrakaitselistel eesmärkidel, sealhulgas „korrarikkumise kõrvaldamiseks“. Selline lähenemine on jällegi vastuolus Euroopa Kohtu praktikaga, mis lubab andmete säilitamist ja kasutamist üksnes raskete kuritegude või tõsiste julgeolekuohtude korral. Korrakaitse ohuennetamine hõlmab oma olemuselt ka väga madala kaaluga rikkumisi ning ei saa õigustada ulatuslikku põhiõiguste riivet. Sama probleem puudutab ka julgeolekualast lävendit, kus kasutatakse „ohu“ mõistet üldises tähenduses, mis ei vasta Euroopa Kohtu nõudele käsitleda üksnes eriti tõsiseid ohte riigi julgeolekule. Lisaks ei ole eelnõus ette nähtud piisavat sõltumatut eelkontrolli. Säilitamiskohustust saab kehtestada prokuratuuri, PPA või julgeolekuasutuse otsusega, mis ei vasta Euroopa Kohtu praktikas nõutud sõltumatu kontrolli standardile. Ka kohtuloo olemasolu ei lahenda iseenesest probleemi, kui materiaalõiguslikud lävendid on liiga madalad või ebaselged.	ANTUD SELGITUS EL Kohus võimaldab liikmesriikidel võtta seadusandlikke meetmeid, et näha ette võimalus sideandmete üldiseks ja ühetaoliseks ning ajutiseks säilitamiseks riigi julgeolekut ähvardava ohu korra. EL Kohus ei nõua eelkontrolli, vaid ütleb, et vastav säilitamise ettekirjutus peab olema kontrollitav kohtu või sõltumatu haldusasutuse poolt. Vabariigi Valitsuse korraldus kui haldusakt peab vastama haldusmenetluse reeglitele ning see on vaidlustatav ning halduskohtu poolt kontrollitav. Konkreetsed isikuid puudutavatele andmetele juurdepääsuks näeb juba kehtiv KrMS ette kohtu loa nõude. Oluline on siin lisaks eristada andmete säilitamist, sealhulgas konkreetse menetluse raames ning nendele andmetele hilisemat juurdepääsu, kus kehtivad kõrgemad menetluslikud garantiid. Eelnõu teksti on täpsustatud.

	Euroopa Kohtu praktika kohaselt peab ka kohtulik kontroll olema sisuline, mitte pelgalt formaalne, ning luba saab anda üksnes piisava raskusastmega juhtudel.	
3.	Eelnõu kõige haavatavamaks kohaks on mõiste „äri­lilisel eesmärgil säilitatavad andmed“, millele kogu regulatsioon üles on ehitatud. Kuigi eristus äri­lilistel ja seadusest tulenevatel põhjustel säilitatavate andmete vahel on kontseptuaalselt arusaadav, tunnistab ka seletuskiri, et praktikas ei pruugi nende kahe kategooria vahel alati selget piiri olla. Kui tulevikus ei ole võimalik usaldusväärselt kindlaks teha ega tõendada, millisel alusel konkreetseid andmeid säilitati, muutub kogu regulatsiooni keskne eeldus küsitavaks ning järelevalve selle üle oluliselt raskendatuks. Sellest tulenevalt võiks kaaluda, kas süsteem ei peaks veelgi selgemalt lähtuma põhimõttest, et lisaandmete kogumine ja säilitamine on lubatud üksnes erandjuhtudel ning selgelt määratletud ja põhjendatud õigusliku aluse olemasolul, mitte üldiseks ettenägemiseks või võimaliku tulevase vajaduse katmiseks. Oluline on rõhutada ka seda, et kohtu loa olemasolu ei lahenda iseenesest kõiki Euroopa Kohtu praktikast tulenevaid probleeme. Euroopa Kohus ei ole keskendunud üksnes sellele, kes loa annab, vaid ka sellele, millistel sisulistel tingimustel tohib luba anda. Kohtulik kontroll ei tohi taanduda formaalseks kinnituseks. Juurdepääs liiklus- ja asukohaandmetele eeldab materiaalõiguslikult piisavalt kõrget lävendit. Euroopa Kohus on kohtuasjas C 746/18 rõhutanud, et kuritegevuse vastu võitlemise eesmärgil peaks juurdepääs põhimõtteliselt piirduma nende isikute andmetega, keda kahtlustatakse raske kuriteo kavandamises, toimepanemises või sellega seotud olemises. Sellest tulenevalt peaks kohtul olema võimalik luba anda üksnes olukorras, kus tegemist on piisava raskusastmega kuritegevuse või sellega võrreldava ohuga. Vastasel juhul muutub kohtulik kontroll olemuslikult formaalseks. Just samast lähtepunktist vaadatuna tekitab tõsisemaid küsimusi sideandmete kasutamine väärtemenetluses ning korra­kaitselistel eesmärkidel. Euroopa Kohtu praktikast ei nähtu, et liiklus- ja asukohaandmete kasutamist oleks võimalik põhjendada pelgalt üldise ohuennetuse, korra­rikkumise kõrvaldamise või tavapärase haldusjärevalve vajadusega. Sellised eesmärgid ei vasta sellele raskusastmele, mida Euroopa Kohus peab vajalikuks sellise intensiivse põhiõiguste riive õigustamiseks.	ANTUD SELGITUS Eelnõus nähakse ette üldine ja ühetaoline säilitamiskohustus ette lõppkasutaja tuvastamiseks vajalike andmete ja IP-aadresside osas. Senine säilitamiskohustus liiklus- ja asukohaandmete osas (ESS § 111¹ lg 2) kaotatakse ning üldjuhul jääb edaspidi pädevatele asutustele võimalus kasutada neid andmeid juhul, kui need on säilitatud äri­lilistel eesmärkidel. EL Kohus on oma otsustes korduvalt öelnud, et sideettevõtjal olemasolevaid andmeid võib kasutada ka muudel eesmärkidel, sh menetlustes, kus seda nõuab EL õigus (C-339/20, C-397/20). Samuti lubab EL Kohus säilitada lõppkasutaja tuvastamiseks vajalikke andmeid ja IP-aadresse ning kasutada neid ka muudel eesmärkidel kui raske kuritegevuse vastane võitlus (C-470/21).
4.	Sarnased küsimused tekivad ka ESS § 111² alusel nimetatud seadmetunnuste puhul. IMSI, IMEI, SUPI, SUCI ning muud võrguidentifikaatorid võivad praktikas võimaldada väga detailset seadmepõhist ja kaudselt ka isikupõhist profileerimist. Kuigi neid käsitletakse tehniliste andmetena, ei kõrvalda see nende potentsiaalset mõju isiku eraelu puutumatusele.	ANTUD SELGITUS Tegemist on lõppkasutaja tuvastamist võimaldavate andmetega ning üksnes nende andmete põhjal ei ole võimalik kasutaja detailne profileerimine.

	Seetõttu vajab täiendavat põhjendamist nii sellise andmekoosseisu vajalikkus kui ka see, milliste konkreetsete meetmetega välditakse nende andmete kasutamist isiku käitumise, liikumismustrite ja suhtlusvõrgustiku detailseks profileerimiseks. Eraldi tähelepanu väärib ka reaalajas asukoha tuvastamise regulatsioon. Liiklus- ja asukohaandmete põhjal on võimalik teha väga ulatuslikke ja täpseid järeldusi inimese eraelu, harjumuste, liikumiste, suhtlusvõrgustiku ja elustiili kohta. Mida lähemale liigub meede reaalajas jälgimisele, seda intensiivsem on põhiõiguste riive ning seda tugevamad peavad olema nii meetme põhjendus kui ka selle kohaldamise tingimused ja lävend. Sama tähelepanek kehtib ka Vabariigi Valitsuse määruse kavandis loetletud andmekoosseisu kohta. Kärjetunnused, tugijaamade asukohad, roaminguandmed, IP-aadressid ning sideansside algus- ja lõpuaeg võimaldavad koos analüüsituna koostada inimese liikumisest ja suhtlusmustri äärmiselt detailse ja tervikliku pildi. Seetõttu ei ole küsimus üksnes selles, kas andmeid säilitatakse, vaid ka selles, kui ulatuslikku isikuprofiili on nende andmete põhjal võimalik hiljem rekonstrueerida. Just see aspekt nõuab regulatsioonis eriti selget põhjendust ja ranget piiritlemist.	Selleks on vajalik oluliselt suurem andmemaht ning lisaks ka liiklusandmed. Terminalseadme reaalajas tuvastamise regulatsioon võrreldes kehtiva õigusega sisuliselt ei muutu. Õigusselguse huvides on eelnõus tõstetud see regulatsioon eraldi paragrahvi. Vabariigi Valitsuse määrusega nähakse ette detailsed andmekategooriad, mis on seotud eelnõus sätestatud säilitamiskohustusega. Tegemist on liiklus- ja asukohaandmetega ning nende osas on ette nähtud eraldi reeglid nende säilitamise ja juurdepääsu osas.
5.	ESS § 112 regulatsioon tekitab olulisi küsimusi ka isikuandmete kaitse üldmääruse (IKÜM) valguses. Sideettevõtjad peavad tagama, et andmete töötlemine, sealhulgas edastamine, oleks seaduslik ja läbipaistev. Eelnõu võib aga panna nad olukorda, kus nad on sunnitud oma kohustusi rikkuma. Lisaks puudub piisav logimiskohustus sideettevõtja poolel, mistõttu ei ole hiljem võimalik kontrollida, milliseid andmeid, kellele ja millisel alusel edastati. See omakorda muudab andmesubjekti õiguste teostamise praktikas äärmiselt keeruliseks. Seetõttu võiks kaaluda, kas ka sideettevõtjal peaks olema kohustus säilitada teave selle kohta, milliseid andmeid, kellele ja millisel õiguslikul alusel väljastati. Lisaks on lahendamata andmesubjekti hilisema teavitamise küsimus. Kui inimene ei saa kunagi teada, et tema andmeid kasutati, muutub ka õigusvastase kasutamise vaidlustamine suuresti teoreetiliseks. Teavitamine peaks vajadusel olema küll edasilükatav, kuid põhimõtteliselt automaatne. Teavitamata jätmine peaks olema põhjendatud erand, mis allub sõltumatule kontrollile.	ANTUD SELGITUS Päringute tegemine fikseeritakse ning elektrooniliselt tehtud päringutest jääb alati maha logi. Vastav kohustus logifaile säilitada on päringu tegijal ning seadus näeb ette ka järelevalve teostamise päringute tegemise üle. Isikute teavitamise regulatsioon ei ole ESS kohaldamisala küsimus, vaid pigem eriseaduste reguleerimisala. Leiame, et andmete päringutest teavitamine on oluliselt laiem kui sideandmete päringud ning seetõttu tuleks see küsimus lahendada hiljem eraldi eelnõuga.
6.	Oluline probleem on andmete hilisema kasutamise võimalus. Eelnõus tuleb selgelt välistada olukord, kus julgeoleku eesmärgil kogutud andmeid kasutatakse hiljem kriminaalmenetluses nn tagaukse kaudu. Kui sideandmeid kogutakse ja säilitatakse JAS-i alusel, tuleb välistada ka olukord, kus nende andmete kasutamiseks kriminaalmenetluses koostatakse teabehanke kokkuvõte, mida seejärel KrMS § 63	ANTUD SELGITUS EL Kohtu praktika kohaselt ei ole lubatud kriminaalmenetluses kasutada andmeid, mis säilitati riigi julgeoleku tagamise eesmärgil.

	lõike 1¹ alusel riigi peaprokuröri loal käsitatakse kriminaalmenetluses tõendina. Samuti ei nähtu Euroopa Kohtu praktikast, et sideandmete kasutamine väärtemenetluses või tavapäraste korrakaitsete ülesannete täitmisel oleks lubatav.	Lõppkasutaja tuvastamist võimaldavate andmete, samuti ärilisel eesmärgil säilitatud andmete kasutamist ei ole EL Kohus keelanud muudel eesmärkidel. (C-339/20, C-397/20 ja C-470/21).
7.	Tähelepanu väärrib ka asjaolu, et väga erinevatele andmekategooriatele nähakse eelnõus ette ühesugune säilitamistähtaeg (ESS § 111¹ lg 5). Eelnõust ei nähtu seejuures selgelt, millistel objektiivsetel kriteeriumidel põhineb selline ühtne lähenemine ega miks peaksid eri laadi ja erineva tundlikkusega andmeliigid alluma samale säilitusperioodile. Arvestades, et andmekategooriate olemus ja nendest tulenev põhiõiguste riive intensiivsus võivad oluliselt erineda, eeldaks selline lahendus selget ja veenvat põhjendust.	ANTUD SELGITUS Eelnõu näeb ette erinevad andmete säilitamise tähtajad. Eelnõu üheks eesmärgiks on muuhulgas luua sideettevõtjate jaoks selge ja lihtne raamistik, sealhulgas säilitamistähtaegade osas, et tagada pakutud regulatsiooni lihtne rakendamine praktikas.
8.	Eelnõu eesmärk on saavutada sideandmete küsimuses õigusselgus ja õigusrahu. Seda ei saavuta lihtsalt laussäilitamise teise sätte all jätkamisega. Liiklus- ja asukohaandmete säilitamine ja kasutamine riivab intensiivselt eraelu puutumatust ning vajab seetõttu selgeid seaduslikke lävendeid, sõltumatut kontrolli ja muid tasakaalustavaid meetmeid. Euroopa Kohus on seda lähtekohta järjekindlalt kinnitanud. Kohtuasjas Digital Rights Ireland (C-293/12 ja C-594/12, 8.04.2014, p-d 51, 59) rõhutas kohus, et liiklus- ja asukohaandmete põhjal saab teha väga täpseid järeldusi isiku eraelu kohta ning tegemist on ulatusliku põhiõiguste riivega. Kohtuasjas SpaceNet (C-793/19 ja C-794/19, 20.09.2022, p 61) kinnitas kohus, et nende andmete põhjal saab koostada isiku igapäevaelust, liikumistest ja sotsiaalsetest suhetest üksikasjaliku pildi. Samades lahendites selgitati neid põhimõtteid just nimelt säilitamise, mitte üksnes edastamise kontekstis.	ANTUD SELGITUS Eelnõuga nähakse ette selge raamistik, mis vastab kohtupraktikale.
9.	Peame jätkuvalt vajalikuks juhtida tähelepanu probleemile, millele saavad üksnes sideettevõtjad vastuseid anda - kuidas sideettevõtjad saavad praktikas eristada ärilisel eesmärgil säilitatavaid andmeid nendest, mida säilitatakse riigi kohustuse alusel. Kui see eristus ei ole kontrollitav, muutub eelnõu üks keskseid eeldusi ebakindlaks. Hiljem ei saa usaldusväärselt kontrollida, millisel alusel konkreetseid andmeid säilitati ja kas nende väljastamiseks oli piisav õiguslik alus.	ANTUD SELGITUS Eelnõuga nähakse lõppkasutaja tuvastamist võimaldavate osas ette üldine ja ühetaoline säilitamiskohustus ning liiklus- ja asukohaandmete puhul lähtutakse reeglina edaspidi andmetest, mis on säilitatud ärilisel eesmärgil.

		Kuigi eelnõuga nähakse ette ka täiendavad säilitamiskohustused, siis need andmed on kasutatavad üksnes seaduses loetletud juhtudel ja eesmärkidel.
10.	Advokatuur ei pea põhjendatuks Kaitsepolitseiameti lisamist ESS § 111¹ lg 1 p 2 juurde korrakaitseliste volituste kontekstis. Kaitsepolitseiameti ülesanded on sätestatud JAS §-s 6, millest punktid 1-22 langevad ESS § 111¹ lg 1 p 3 kohaldamisalasse ning JAS § 6 p 4 langeb ESS § 111¹ lg 1 p 1 kohaldamisalasse. Kuivõrd Kaitsepolitseiameti uurimisalluvuses on üksnes kuriteod, mis on otseselt või kaudselt seotud JAS §-s 6 nimetatud ülesannetega, on JAS § 6 p 3 alusel nende tõkestamine samuti hõlmatud ESS § 111¹ lg 1 punktidega 1 ja 3. Seetõttu ei näe advokatuur vajadust anda KaPo-le õigust andmete säilitamiseks nendes olukordades, kus oht ei tulene KaPo JAS-is sätestatud ülesannetest. Kiirsäilitamine peab olema seotud konkreetse menetluse, konkreetse ohu või piisava raskusastmega kuriteoga, mitte üldise korrakaitse vajadusega. Toetame seda, et rakendusaktis sätestatakse täpne andmekataloog ning seaduses selgitatakse, et nõuda saab üksnes andmeid, mis on sideettevõtjal olemas ja mille säilitamine on konkreetse eesmärgi saavutamiseks vältimatult vajalik. Samaaegselt ei tohi sideettevõtjad sellist andmekataloogi ise säilitada üksnes selleks, et olla kooskõlas uue ESS-iga. Seetõttu tuleb seadusemuudatusega tühistada ka ESS § 184¹ lg 1 vähemalt ärilisel eesmärgil kogutud andmete osas. Lisaks on Euroopa Kohtu praktika kohaselt kiirsäilitamine lubatav üksnes pädevate asutuste ettekirjutusel (C-511/18, C-512/18, C-520/18, p 163). Siinkohal tuleb arvestada ka kohtuasja H.K. vs Prokuratuur (C-746/18, p-d 51–57), kus Euroopa Kohus leidis, et prokuratuur kui eeluurimismenetluse juht ei saa sõltumatult kaaluda isiku põhiõiguste rikkumise kaalu, kui tema huvi on ise esitada riiklikku süüdistust. See järeldus ei erine kiirsäilitamise puhul, kuivõrd kiirsäilitamise mõte on üksnes andmete täiendav säilitamine juhuks, kui neid on vaja hiljem prokuratuuri tööülesannete täitmiseks. Sama kehtib ilmselgelt ka teistele uurimisasutustele. Euroopa Kohtu praktikaga kooskõla saavutamiseks tuleb see otsustus anda üle kellelegi teisele, päriselt sõltumatule asutusele või kohtule, või luua kriminaalmenetluses oleva läbiotsimise regulatsioonile sarnane regulatsioon, kus edasilükkamatu juhu puhul võib uurimisasutus ise teha kiirsäilitamise korralduse, kuid seda peab hiljemalt 24 tunni jooksul kontrollima sõltumatu haldusorgan või kohus.	ANTUD SELGITUS Arvestades Kaitsepolitseiameti ülesandeid ja kohustusi on otstarbekas näha ette võimalus andmete kiirsäilitamiseks konkreetsetes menetluses ka korrakaitse eesmärkidel. Rõhutame siinkohal, et oluline on eristada andmete säilitamist ja juurdepääsu. Lisaks puudutab see meede ainult olemasolevaid andmeid ja tagab selle, et ärilisel eesmärgil säilitatud andmed on olemas kui neile taotletakse juurdepääsu. Ärilisel eesmärgil andmete säilitamist hindab iga sideettevõtja ise, sealhulgas nii andmete kategooriate kui ka tähtaegade osas. ESS kohaselt on vastutus ette nähtud üksnes juhtudel, kui rikutud on seadusega kehtestatud säilitamiskohustust. EL Kohus ei nõua andmete kiirsäilitamise puhul kohtu luba. Kohtu luba on vajalik andmetele juurdepääsu taotlemisel. Sarnane regulatsioon on ette nähtud ka EL e-tõendite määrusega, kus andmete säilitamise taotlemiseks on piisav prokuröri luba või valideerimine.
11.	Esmalt soovib advokatuur rõhutada Euroopa Kohtu järgnevat seisukohta – liikmesriigid ei saa teha erandist reeglit,	ANTUD SELGITUS

kehtestades sellega liiklus- ja asukohaandmete üldise ja vahet tegemata säilitamise (C-140/20, p 84). Riigi julgeoleku eesmärgil laussäilitamine on juba eos väga intensiivne põhiõiguste riive. Euroopa Kohus on expressis verbis selgitanud, et laussäilitamine, olgu see ka riigi julgeoleku jaoks, on siiski äärmiselt intensiivne põhiõiguste riive (nt C-793/19, C-794/19, p-d 60-62). Seega ei seisne riive ainult hilisemas andmetele juurdepääsus – ulatuslik andmekogu sideettevõtja juures suurendab ka väärkasutuse, lekke ja küberrünnaku riski. Teisisõnu - eelnõu tahab lubada sideandmete säilitamise ja kasutamise Eesti Vabariigi kaitseks, kuid kui lubada sideettevõtjatel koostada massiivseid ning äärmiselt detailseid andmekogusid kõigi elanike kohta, tuleb täiendavalt kaaluda ka riski, et Eesti Vabariigile vaenulikud jõud kasutavad sedasama andmebaasi Eesti Vabariigi ja tema elanike vastu. Eelneva tõttu on väär ning Euroopa Kohtu praktikaga vastuolus ka 12.06.2026 kõlanud argumentatsioon, et justkui andmete massiivse säilitamise riive ei ole suur. Lisaks, seaduse säte ise peab sisaldama selget ja kontrollitavat lävendit, millest nähtub tõeline, tõsine ja vahetu või ettearvatav oht riigi julgeolekule. Pelk viide põhiseaduslikku korda ohustavale ohule ei ole piisav. Kohtuasjas La Quadrature du Net (C-511/18, C-512/18, C-520/18, p-d 135–139, 168) selgitas Euroopa Kohus, et üldine ja vahet tegemata liiklus- ja asukohaandmete säilitamine võib tulla kõne alla üksnes erandina riigi julgeoleku kaitseks, kui esineb tõeline, vahetu või ettearvatav ja piisavalt tõsine oht, ning meede peab olema ajaliselt piiratud. Kohtuasjas SpaceNet (C-793/19 ja C-794/19, 20.09.2022, p-d 66–74) kinnitas kohus sama põhimõtet ning rõhutas, et selline säilitamine ei ole lubatav kuritegevuse vastu võitlemise tavapärase meetmena. Samuti ei ole Euroopa Kohtu praktikaga kooskõlas 12.06.2026 kõlama jäänud plaan, et justkui ohu lävendiga seotud kohtupraktikale võib lihtsalt viidata seaduse seletuskirjas. Euroopa Kohus on rõhutanud, et proportsionaalsuse tagamiseks peavad kõik asjakohased piirangud ja tagatised olema sätestatud riigisisises õigusaktis endas, mitte seletuskirjas või muudes mitteõiguslikes dokumentides. Kohtuasjas SpaceNet (C-793/19 ja C-794/19, 20.09.2022, p-d 69–70) kinnitas kohus, et õigusaktis peavad olema selged ja täpsed reeglid meetme ulatuse ja kohaldamise kohta ning selles tuleb märkida, millistel asjaoludel ja tingimustel võib meetme võtta. Ainult nii on tagatud, et riive piirdub vältimatult vajalikuga. Pelk seletuskirjas Euroopa Kohtu praktikale viitamine ei taga regulatsiooni kooskõla selle praktikaga. Samuti toetame võimalikult lühikest säilitamiskohustuse kestust. Euroopa Kohus on selgitanud (C-140/20, p 82), et eesmärgipärase säilitamise meetmete kestus ei või ületada seda, mis on taotletava eesmärgi ja meetmeid põhjendavate asjaolude seisukohast tingimata vajalik, ilma et see piiraks meetmete	EL Kohus näeb ette võimaluse riigi julgeolekut ähvardava ohu korral võtta meetmeid sideandmete ajutiseks säilitamiseks. Eelnõu kohaselt nähakse säilitamiskohustus ette Vabariigi Valitsuse korraldusega, mille kehtivus on ajaliselt piiratud ja mis on kohtulikult kontrollitav. EL Kohus ei nõua sellise säilitamiskohustuse puhul kohtulikku eelkontrolli.
--	---

	võimalikku pikendamist, kui püsib vajadus andmete säilitamise järele. Kui eelnõus nähakse ette kahest kuust pikem tähtaeg, peab seadusandja seda eraldi ja veenvalt põhjendama – miks võib Vabariigi Valitsus äärmiselt intensiivselt riivata kõigi Eesti Vabariigi elanike põhiõigusi kordades rohkem kui jälitustegevusega KrMS või JAS alusel. Haldusmugavus, bürokraatia vältimine või partnerasutuste ootused ei õigusta riive kestuse pikendamist. Ka võimalus korraldust hiljem lühendada ei muuda riive esialgset iseloomu. Meie hinnangul peaks riigi julgeoleku eesmärgil kehtestatavale säilitamiskohustusele eelnema kohtulik kontroll. Euroopa Kohus on andmetele juurdepääsu andmise kontekstis selgitanud, et sõltumatu kontroll peab toimuma enne mis tahes juurdepääsu andmist, välja arvatud nõuetekohaselt põhjendatud kiireloomulistel juhtudel, mil kontroll peab toimuma lühikese aja jooksul, ning seda ei asenda kohtulik järelkontroll (nt C-746/18, p 58). Kuivõrd Euroopa Kohus on leidnud, et nii riigi julgeoleku erandi kui juurdepääsu andmise puhul on vajalik kohtulik kontroll, tuleb seda kohaldada mõlemal juhul samasuguselt – kohtuliku eelkontrolliga. Alternatiivina saab kaaluda üksnes sõltumatut kontrollimehhanismi, mille otsus on täitevvõimule siduv ning mis vastab Euroopa Kohtu praktikast tulenevatele nõuetele. Õiguskantsleri siduv arvamus oleks kaalutav juhul, kui seadus tagab selle menetluse sisulise ja sõltumatu iseloomu. Õiguskantsler on sisuliselt ainus põhiõiguslik institutsioon, kes kvalifitseeruks Vabariigi Valitsusest sõltumatuks asutuseks Euroopa Kohtu praktika mõttes (nt C-746/18, p 53). Viimaks, Vabariigi Valitsuse korraldus ei tohiks olla salajane, vaid avalikult kättesaadav. Vastasel puhul puudub isikul tegelik võimalus kontrollida meetme õiguspärasust ja pöörduda kohtusse. Seega on ka igasugune kohtulik kontroll üksnes näilik ning mitte tõhus, nagu Euroopa Kohus seda nõuab (nt C-511/18, C-512/18, C-520/18, p 168).	
12.	Raskete kuritegude menetlemise eesmärgil andmete säilitamisel tuleb lähtuda proportsionaalsuse ja minimaalsuse põhimõtetest. Euroopa Kohus on selgitanud, et ka eesmärgipärase säilitamise meetmete puhul on seaduslikkuse eeltingimuseks proportsionaalsuse põhimõtte järgimine ning meetmete kestus ei või ületada seda, mis on taotletava eesmärgi ja meetmeid põhjendavate asjaolude seisukohast tingimata vajalik, ilma et see piiraks meetmete võimalikku pikendamist, kui püsib vajadus andmete säilitamise järele (C-140/20, p 82). Seega tuleb eelnõus võimalikult selgelt põhjendada kõik geograafilised alad või tugijaamad, mille suhtes säilitamiskohustust kohaldatakse. Täpsemalt peavad need liikmesriigi õigusnormid ette nägema, millistel asjaoludel ja milliste tingimuste kohaselt võib andmete säilitamise meetme ennetavalt võtta, tagades seeläbi, et niisugune meede	ANTUD SELGITUS Eelnõu näeb ette sihistatud säilitamise geograafilise tunnuse alusel raske kuritegevuse vastu võitlemise eesmärgil. EL Kohus on korduvalt oma otsustes öelnud, et selline sihistatud säilitamine ei ole vastuolus EL õigusega. Eelnõus nähakse ette kriteeriumid ja tingimused, millal on andmete säilitamine kohustuslik. Lisaks nähakse ette võimalus Vabariigi Valitsuse korraldusega

piirduks rangelt vajalikuga (C-203/15 ja C-698/15, p 109). Peame vajalikuks vältida lahendust, kus tihedama asustusega piirkondades elavad inimesed peavad püsivalt arvestama oma sideandmete kogumisega üksnes seetõttu, et piirkonnas on rohkem inimesi ning seega ka kuriteoteateid. Kõrgema kuritegevusega piirkonna määratlemise alus peab olema objektiivne, kontrollitav ja ajakohane. Kohtuasjas Tele2 Sverige (C-203/15 ja C-698/15, 21.12.2016, p-d 106–111) selgitas Euroopa Kohus, et liiklus- ja asukohaandmete sihitatud säilitamine peab olema piiratud rangelt vajalikuga ning piiritlemine võib põhineda isikute kategoorial, geograafilisel kriteeriumil või ajavahemikul, kuid kriteeriumid peavad olema objektiivsed ja proportsionaalsed. Sama otsuse punktis 119 rõhutati, et juurdepääs peab olema piiratud raske kuritegevuse vastu võitlemisega. Euroopa Kohtu kohtupraktika kohaselt tuleb selliseid piiranguid otsustada pädeval asutusel. Nagu ülal selgitatud, ei ole uurimisasutused selliseks asutuseks, kes suudaks erapooletult omavahel kaaluda isikute põhiõiguste riivet ning taotletava eesmärgi olulisust (C-746/18, p-d 54-55). Seega ka see otsustus tuleb teha Vabariigi Valitsusel, juhindudes kas kohtu või õiguskantsleri siduvast seisukohast. Juhime tähelepanu, et igasugune säilitatud andmete kasutamine, sh riikliku julgeoleku tagamise eesmärgil säilitatud andmete kasutamine, peab olema allutatud eelnevale kohtulikule kontrollile (C-746/18, p-d 51-52). Julgeolekuasutuste puhul ei sätesta JAS sellist kohtulikku kontrolli. Seetõttu näeb advokatuur hädavajaliku muudatusena muudatust JAS § 27 lg 1 ja 2 muuta viisil, et see hõlmab ka JAS § 26 lg 3 p 4 alusel teostatut. Vastasel juhul on julgeolekuasutuste poolt teostatud andmete kasutamine automaatselt vastuolus EL õigusega. Meie hinnangul ei ole riigi sunnil säilitatavate liiklus- ja asukohaandmete kasutamine väärtemenetluses Euroopa Kohtu praktikaga kooskõlas. Äriline eesmärgil juba kogutud andmete kasutamine võib teoreetiliselt tulla kõne alla üksnes kitsalt piiritletud juhtudel, kui tagatud on kohtulik kontroll, selgelt kõrge lävend ja proportsionaalsus. Eelnõus tuleb vältida lahendust, mis võimaldab sideandmete kasutamist üldise ohuennetuse, tavapärase haldusjärelvalve või korrarikkumise kõrvaldamise eesmärgil. Kohtuasjas Prokuratuur (C-746/18, p-d 45, 50) rõhutas Euroopa Kohus, et ulatuslik juurdepääs liiklus- ja asukohaandmetele on kuritegevuse vastu võitlemise eesmärgil põhjendatud üksnes raskete kuritegude puhul. Kohtuasjas Tele2 Sverige (C-203/15 ja C-698/15, p-d 115–119) rõhutas kohus samuti, et juurdepääs peab olema piiratud rangelt vajaliku ja raske kuritegevuse vastu võitlemise eesmärgiga. Sellest ei nähtu alust laiendada sideandmete kasutamist väärtemenetlusele või üldistele korrakaitselistele	säilitamiskohustuse ulatust täpsustada. Ka see korraldus peab vastava haldusmenetluse nõuetele, olema põhjendatud ning on kohtulikult kontrollitav. Lõppkasutaja tuvastamist võimaldavate andmete, samuti ärilisel eesmärgil säilitatud andmete kasutamist ei ole EL Kohus keelanud muudel eesmärkidel. (C-339/20, C-397/20 ja C-470/21).
--	---

	eesmärkidele. Lugesdes viidatud kohtulahendeid, ei ole üheselt selge, et Euroopa Kohtu seisukohad rakenduksid üksnes riiklikul sunnil kogutavatele andmetele, vaid kõigile sideettevõtjate poolt kogutud sideandmetele.	
13.	Peame andmesubjekti hilisemat teavitamist väga oluliseks riive tasakaalustamise meetmeks. Kui teavitamise regulatsiooni praegusesse eelnõusse ei lisata, tuleb riive intensiivsust muude meetmetega oluliselt vähendada. Muidu jääb risk, et andmesubjekti õiguskaitsevahendid jäävad üksnes teoreetiliseks, sest isik ei saa kunagi teada, et tema andmeid on kasutatud. Teavitamine võib olla edasilükatav üksnes siis, kui see on konkreetse menetluse või julgeolekuhuvi kaitseks vältimatult vajalik. Kohtuasjas Tele2 Sverige (C-203/15 ja C-698/15, 21.12.2016, p 121) rõhutas Euroopa Kohus, et pädevad asutused peavad teavitama puudutatud isikuid andmetele juurdepääsust niipea, kui teavitamine ei kahjusta enam uurimist, sest teavitamine on vajalik tõhusate õiguskaitsevahendite kasutamiseks. See põhimõte seondub põhiõiguste harta artikliga 47 ning nõuab, et teavitamata jätmine ei muutuks reegliks.	ANTUD SELGITUS Teavitamise regulatsioon ei kuulu ESS kohaldamisalasse ning see on reguleeritud eriseadustes. Kuna tegemist on horisontaalse teemaga, mis puudutab mis tahes andmete päringuid, siis peame vajalikuks seda teemat käsitleda eraldi eelnõus.
14.	Palume eelnõu edasisel menetlemisel tagada, et sideandmete säilitamise ja kasutamise regulatsioon sisaldaks selgeid seaduse tasandil sätestatud lävendeid, võimalikult lühikesi ja andmekategooriate kaupa põhjendatud säilitamistähtaegu, sõltumatut eel- või järelkontrolli, andmesubjekti hilisema teavitamise regulatsiooni ning selgeid piiranguid andmete hilisemale kasutamisele muudes menetlustes. Ilma nende tagatisteta ei pruugi regulatsioon saavutada soovitud õigusselgust ning võib kaasa tuua uued vaidlused andmete säilitamise ja kasutamise lubatavuse üle ning kõigi osaliste jaoks kõige halvema tagajärje – igasuguse õigusliku aluse kadumise sideandmete säilitamiseks ja kasutamiseks.	ANTUD SELGITUS Eelnõu väljatöötamisel on lähtutud EL Kohtu ja Riigikohtu lahenditest ning nendega kehtestatud tingimustest. Eelnõuga nähakse ette säilitamiskohustus ulatuses, kus see on lubatud kohtupraktikaga.